38. 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 2015. Redaktionsschluss für die Beiträge war der 31. Dezember 2015.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Die europäische Grundrechtecharta als internetvertrauensbildende Maßnahme in Bremen und Europa

Auch wenn es beim Umgang mit den flüchtenden Menschen leider nicht immer den Anschein hat, ist der eingebaute Antriebsmechanismus der Europäischen Union das Einreißen von Grenzen. Bei dem Ziel, Verkehrshemmnisse abzubauen, geht es nicht nur darum, dass sich Personen von nationalstaatlichen Grenzen ungehindert in Europa bewegen können. Auch Waren, Dienstleistungen und Beschäftigte sollen Grenzen überschreiten können, ohne dass hierfür Nachteile erwartet werden müssen. Der von der Europäischen Union eingeschlagene Weg ist dabei regelmäßig der, in allen Staaten durch den Erlass von Rechtsnormen einheitliche Verhältnisse herzustellen. Dadurch, dass überall in der Europäischen Union dasselbe Recht gilt, soll verhindert werden, dass Menschen, aber vor allem auch Unternehmen aus anderen Staaten der Europäischen Union schlechter oder besser behandelt werden als inländische Personen oder Unternehmen. Auch bei der Diskussion um den Datenschutz in Europa geht es um den Abbau von Verkehrshindernissen. Die Datenschutzgrundverordnung ist daher in Wirklichkeit keine "Datenschutz"-Grundverordnung, wie es die auch hier verwendete amtliche Abkürzung nahelegt. Der korrekte Titel lautet: "Verordnung (…) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten **und zum freien Datenverkehr**".

Sofern die betreffenden Grundrechtsbereiche wirtschaftliche Reflexe aufwiesen, konnte die primäre Wirtschaftsgetriebenheit der Europäischen Union in der Vergangenheit positive Nebeneffekte für Grundrechte erzeugen. So hängt das Außerkrafttreten von deutschen Gesetzen, die Frauen bezüglich ihres Arbeitsentgeltes diskriminierten, eng damit zusammen, dass Frankreich bereits auf die Frauendiskriminierung in diesem Bereich verzichtet hatte. Dies wurde jedoch als wirtschaftlicher Nachteil im Vergleich zu der Situation in anderen Staaten erlebt. Deshalb wirkte Frankreich darauf hin, dass die damalige Europäische Wirtschaftsgemeinschaft in Artikel 119 des Vertrages über die Europäischen Gemeinschaften den Grundsatz des gleichen Entgelts für Männer und Frauen bei gleicher Arbeit formulierte. Das ökonomische Ziel, in der Europäischen Gemeinschaft einen einheitlichen Frauendiskriminierungsgrad beziehungsweise Frauengleichstellungsgrad beim Entgelt zu erreichen, hätte auch erreicht werden können, indem Frankreich auf die Regelungen verzichtet hätte, die die Entgeltdiskriminierung von Frauen sanktionierten. Dass dieser Weg nicht beschritten wurde, sondern die anderen europäischen Länder verpflichtet wurden, Regelungen wie in Frankreich zu erlassen, zeigt, dass es zwei Voraussetzungen für grundrechtserweiternde Effekte von Entwicklungen auf europäischer Ebene gibt: Ein grundrechtsfreundlicher europäischer Konsens muss auf rechtliche Verpflichtungen treffen. In den 1970er Jahren sorgte der europäische Konsens, Frauendiskriminierungen in allen

Lebensbereichen abbauen zu wollen, dafür, dass europäische Regelungsverpflichtungen dafür genutzt wurden, das Niveau der Frauengleichstellung überall in Europa anzuheben.

Die Lage beim Datenschutz ist vergleichbar: Unternehmen, die die als besonders streng geltenden deutschen Datenschutzgesetze beachten müssen, betrachten dies als wirtschaftlichen Nachteil. Die Datenschutzgrundverordnung hat daher in der europäischen Logik vor allem das Ziel, alle Unternehmen, die in Europa agieren, gleich (aus Sicht der Lobby des freien Datenverkehrs: gleich schlecht) zu behandeln. Die wirtschaftsgetriebene europäische Diskussion um den Datenschutz, die im Frühjahr 2016 mit der Verabschiedung der Datenschutzgrundverordnung ihren vorläufigen Höhepunkt erreichen wird, wird also dann positive Nebeneffekte für die Datenschutzgrundrechte haben, wenn die beiden Voraussetzungen des flankierenden grundrechtsfreundlichen Diskurses und der bindenden rechtlichen Verpflichtung für die Verabschiedung von Regelungen mit einem hohen Datenschutzniveau gegeben sind.

1.1 Das gestiegene Bedürfnis nach internetvertrauensbildenden Maßnahmen

Die Menschen in Europa schätzen ihr Grundrecht auf informationelle Selbstbestimmung und beklagen den mangelnden Schutz personenbezogener Daten im Internet. 2015 ergab eine Umfrage des Deutschen Instituts für Vertrauen und Sicherheit im Internet, dass zwar fast alle Internetnutzerinnen und Internetnutzer in Deutschland zumindest gelegentlich im Netz einkaufen. Doch die Mehrheit von ihnen (54 Prozent) hat solche Einkäufe bereits aufgrund von Sicherheitsbedenken abgebrochen. Die meisten Befragten nennen die mangelnde Sicherheit persönlicher Daten sowie den unsicheren Online-Zahlungsverkehr als größte Probleme. Dabei liegt es am Fehlen alternativer Angebote, dass trotz der vorhandenen Sicherheitsbedenken online bestellt wird. Nach einer im November 2015 veröffentlichten Umfrage des Bundesverbandes der Verbraucherzentralen ist die Bereitschaft der Verbraucherinnen und Verbraucher, für Datenschutz zu zahlen, dabei von 35 Prozent im Jahr 2013 auf 51 Prozent gestiegen. Von ihnen würden 87 Prozent bis zu fünf Euro im Monat oder mehr zahlen. Der Mangel an Vertrauen der Menschen in die Sicherheit wirtschaftlicher Interaktionen im Internet kann nicht im Interesse der digitalen Wirtschaft Europas liegen und war nach Aussage der Europäischen Kommission sogar Motivation für den Entwurf für die Datenschutzgrundverordnung.

Die dem Grundrecht auf Datenschutz gewogene Stimmung in der europäischen Öffentlichkeit wurde durch die Enthüllungen von Edward Snowden über die anlasslosen und umfassenden Überwachungsmaßnahmen US-amerikanischer Geheimdienste seit Juni 2013 noch verstärkt. So kritisierten 47 Prozent der Befragten ein Jahr nach den ersten Enthüllungen in einer repräsentativen Umfrage des Deutschen Instituts für Vertrauen und

Sicherheit im Internet, dass zu wenig für den Datenschutz in Deutschland unternommen werde. 52 Prozent hielten ein starkes, gemeinsames Auftreten der Europäischen Union (EU) beim Thema Datenschutz gegenüber den Vereinigten Staaten von Amerika (USA) für wichtig. Die große Mehrheit lehnte den Zugriff auf private Daten im Netz durch Außenstehende ab, wobei 56 Prozent glaubten, jeder werde abgehört. In Bezug auf Datenzugriffe von Nachrichtendiensten meinten 48 Prozent, dass dadurch unsere Grundrechte verletzt werden. 83 Prozent wollten einen Datenzugriff ausländischer Sicherheitsbehörden nicht erlauben. Nur 39 Prozent der Befragten wollten dies deutschen Sicherheitsorganen erlauben. 23 Prozent der Befragten gaben an, wegen der Snowden-Enthüllungen beim Telefonieren, Mailen und Surfen im Internet vorsichtiger geworden zu sein. Auch wenn hier möglicherweise das tatsächliche Handeln dem Wollen hinterherhinkt, ist soziologisch gesehen eine Verhaltensänderung bei fast einem Viertel der Menschen eine beachtliche Größe.

Von einem dem Grundrecht auf informationelle Selbstbestimmung gewogenen Klima in Europa kann also ausgegangen werden. Wie aber sieht es mit der bindenden rechtlichen Verpflichtung für die Verabschiedung von Regelungen mit einem hohen Datenschutzniveau aus? Im Januar 2012 legte die Europäische Kommission den genannten Entwurf der "Verordnung (…) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" vor. Nach Auffassung von Datenschützerinnen und Datenschützern erreichte dieser Entwurf das von der Europäischen Kommission selbst formulierte Ziel nicht, das Vertrauen der Menschen in die Sicherheit ihrer Daten durch die Schaffung eines hohen Datenschutzniveaus nicht nur zu erschleichen, sondern zu rechtfertigen. Siehe hierzu die Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Datenschutzgrundverordnung[1] sowie mein Gutachten für den Innenausschuss des Deutschen Bundestages zur EU-Datenschutzgrundverordnung[2]. Obwohl es im Interesse der Wirtschaft gelegen hätte, das Vertrauen der Menschen in wirtschaftliche Aktionen im Internet durch die Gewährleistung eines hohen Datenschutzniveaus zu begründen, gab es im Zusammenhang mit der Diskussion über die europäischen Datenschutzregelungen von Seiten der Wirtschaft massive Versuche, darauf hinzuwirken, das Datenschutzniveau der von der Europäischen Kommission vorgeschlagenen Regelungen abzusenken, die ja ihrerseits bereits der Kritik von Seiten der Datenschützerinnen und Datenschützern ausgesetzt waren. Der Erfolg der Einflussnahmeversuche der Lobby des freien Datenverkehrs (siehe hierzu 36. Jahresbericht, Ziffer 1.) zeigt sich beim Vergleich des vom federführenden Berichterstatter verfassten Entwurfes der Fassung des Europäischen Parlamentes mit der letztlich im Oktober 2013

[1] https://ssl.bremen.de/datenschutz/sixcms/media.php/13/DSK_Stellungnahme_Grundverordnung.pdf
[2] https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Datenschutzverordnung%20Kommissionsentwurf.pdf

vorgelegten Version des Europäischen Parlamentes. Vor allem aber findet sich der Einfluss datenschutzkritischer Argumente in den Vorschlägen des Rates der Europäischen Union zur Datenschutzgrundverordnung, die erst im Juni 2015 veröffentlicht wurden. Die datenschutzrechtlichen Kernpunkte der Datenschutzkonferenz für die Trilogverhandlungen[3] bestanden daher im Wesentlichen darin, die Forderungen des Rates zurückzuweisen.

Insgesamt ist zu konstatieren, dass die Versuche von Datenschützerinnen und Datenschützern, auf die Formulierungen der Datenschutzgrundverordnung Einfluss zu nehmen, trotz des genannten datenschutzfreundlichen Klimas und trotz des Umstandes, dass es eigentlich im Interesse der Internetwirtschaft gelegen hätte, durch die Formulierung eines verbindlichen und hohen Datenschutzniveaus das Vertrauen der Menschen in Internettransaktionen zu erhöhen, deutlich weniger erfolgreich blieben als das auf Absenkung des Datenschutzniveaus gerichtete Lobbying. Insofern wird die Datenschutzgrundverordnung ihrer Funktion als internetvertrauensbildende Maßnahme nicht allein gerecht werden können.

1.2 Der Europäische Gerichtshof als oberster Internetvertrauensbildner in Europa

Dies alles könnte Anlass zu Pessimismus bezüglich des Datenschutzniveaus in Europa sein. Ein solcher Pessimismus würde aber die Bedeutung der Europäischen Grundrechtecharta, die für alle Staaten, ausgenommen das Vereinigte Königreich und Polen, seit Dezember 2009 bindend ist, und die Rolle des vierten Akteurs auf europäischer Ebene verkennen. Neben den drei Trilogpartnern Europäische Kommission, Europäisches Parlament und Rat der Europäischen Union gibt es im Europäischen Gerichtshof einen Akteur, der uns in der letzten Zeit mit starken grundrechtlichen Pflöcken erfreut hat, die er gestützt auf die Europäische Grundrechtecharta einrammte. Das europäische internetvertrauensbildende Regelwerk ist also nicht erst die Datenschutzgrundverordnung, sondern schon die Europäische Grundrechtecharta. In ihrem Artikel 8 ist festgelegt, dass jeder Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten zusteht. Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Artikel 7 der Europäischen Grundrechtecharta gewährt jeder Person das Recht auf Achtung ihres Privatlebens und ihrer Kommunikation.

Diese starke grundrechtliche Verankerung von Sachverhalten mit Internetbezug hat der Europäische Gerichtshof vor allem in den drei wegweisenden Entscheidungen zur Nichtigkeit der europäischen Vorratsdatenspeicherungsrichtlinie, zu Google Spain und zur Nichtigkeit der Safe-Harbor-Entscheidung der Europäischen Kommission noch einmal gestärkt. Mit

[3] https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Kernpunktepapier+DE.pdf

Urteil vom 8. April 2014 erklärte der Europäische Gerichtshof die Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten für ungültig und erteilte der undifferenzierten und automatischen Totalerfassung dieser Daten unter Hinweis auf die in der Europäischen Grundrechtecharta garantierten Rechte auf Privatleben und Datenschutz eine Absage (siehe hierzu 37. Jahresbericht, Ziffer 19.6). In seinem "Google Spain"-Urteil vom 13. Mai 2014 entwickelte der Europäische Gerichtshof das gegen die Betreiber von Suchmaschinen gerichtete Recht, nicht in jedem Fall leicht im Internet gefunden zu werden. Das Urteil stellt klar, dass Anbieter von Suchmaschinen keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen sind, die die Grundrechte der Betroffenen zu berücksichtigen haben (siehe hierzu 37. Jahresbericht, Ziffer 19.10). Am 6. Oktober 2015 erklärte der Europäische Gerichtshof die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig, die als Rechtsgrundlage für die Übermittlung personenbezogener Daten von Bürgerinnen und Bürgern der Europäischen Union in die USA auch über das Internet gedient hatte (siehe hierzu Ziffer 15.2 und Ziffer 17.8 dieses Berichts). Der Gerichtshof verweist dabei darauf, dass die Kommissionsentscheidung den Wesensgehalt des durch Artikel 7 der Europäischen Grundrechtecharta garantierten Grundrechts auf Achtung des Privatlebens verletze.

1.3 Profiling als besonders internetvertrauensbedürftiger Bereich

Die Datenschutzgrundverordung wird aller Voraussicht nach im Frühjahr 2016 verabschiedet werden, nachdem der Trilog im Dezember 2015 abgeschlossen worden war. Soweit die Datenschutzgrundverordnung die starken Hinweise des Europäischen Gerichthofes nicht beachtet, ist es nicht unwahrscheinlich, dass der Gerichtshof, der durch die genannte Rechtsprechung zum unverzichtbaren Garanten eines hohen Datenschutzniveaus in Europa geworden ist, bestimmte Regelungen der Datenschutzgrundverordnung wegen Verstoßes gegen die Europäische Grundrechtecharta zurückweisen, beziehungsweise die Rechtsanwendenden zur Grundrechtcharta-konformen Auslegung der Datenschutzgrundverordnung verpflichten wird.

Einer dieser Fälle könnte das Profiling sein. Von keinem der Trilogpartner wurde hierzu ein aus Sicht des Datenschutzgrundrechtes akzeptabler Regelungsvorschlag gemacht, der eine wirksame Begrenzung von Profilbildungen ermöglicht. Im zum Redaktionsschluss vorliegenden Text der Datenschutzgrundverordnung hat sich der Rat der Europäischen Union durchgesetzt. Nicht bereits die Profilbildung selbst, sondern erst die Nutzung von Profilen wird rechtlichen Beschränkungen unterworfen, wenn es in Artikel 20 heißt, die Menschen sollten das Recht haben, keiner Entscheidung ausgesetzt zu sein, die allein auf automatischer Datenverarbeitung inklusive Profilbildung beruhe und rechtliche Auswirkungen habe oder sie in ähnlich bedeutsamer Weise beträfe. ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling,

which produces legal effects concerning him or her or similarly significantly affects him or her.") Dieses bereits sehr schmale Recht der Menschen auf Schutz vor Entscheidungen, die nur auf Profilbildungen beruhen, soll zusätzlich dann nicht bestehen, wenn die Profilbildung auf der ausdrücklichen Einwilligung der oder des Betroffenen beruht, erforderlich für den Abschluss oder die Durchführung eines Vertrages mit dem Datennutzer ist oder durch nationalstaatliche Gesetze erlaubt ist, die ausreichend die Rechte und Freiheiten und legitimen Interessen der Grundrechtsträgerinnen und Grundrechtsträger beachten.

Alle genannten Urteile des Europäischen Gerichtshofes enthalten wichtige Aussagen, die darauf hindeuten, dass schon die Profilbildungen selbst grundrechtlichen Beschränkungen unterworfen werden müssten. Im Urteil zu Google Spain stellt der Europäische Gerichtshof grundlegende Erwägungen zur Rolle des Internets, von Suchmaschinen und mit ihnen möglichen Profilbildungen in der modernen Gesellschaft an. Allen, die diese Möglichkeiten nutzten, sei ein strukturierter Überblick über die zu Personen im Internet zu findenden Informationen möglich, die potenziell zahlreiche Aspekte von deren Privatleben betreffen könnten und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden könnten. Hieraus schließt der Europäische Gerichtshof, wegen seiner potenziellen Schwere könne ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse an der Datenverarbeitung gerechtfertigt werden. Im Urteil zur Ungültigkeit der Vorratsdatenspeicherungsrichtlinie wird deutlich, dass der Europäische Gerichtshof dem Grundsatz der Erforderlichkeit eine hohe Bedeutung beimisst. Auch die Aussagen zu technischen Anforderungen können auf Profilbildungen übertragen werden. Es sei entscheidend, dass es hinreichende Garantien gebe, dass die Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung geschützt seien. Im Urteil zur Ungültigkeit der Safe-Harbor-Entscheidung formuliert der Europäische Gerichtshof eine strikte Zweckbindung von Datenverarbeitungen, die verletzt sei, wenn eine Regelung generell die Speicherung aller personenbezogenen Daten sämtlicher Personen gestatte. In Randnummer 91 bringt der Europäische Gerichtshofs seine ständige Rechtsprechung folgendermaßen auf den Punkt: Eine Unionsregelung, die einen Eingriff in die durch die Artikel 7 und 8 der Charta garantierten Grundrechte enthalte, müsse klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen, sodass die Personen, deren personenbezogene Daten betroffen seien, über ausreichende Garantien verfügten, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichten.

Die Anforderungen des Europäischen Gerichtshofes sprechen also dafür, auch die Profilbildungen selbst rechtlichen Beschränkungen zu unterwerfen. Es hätte daher nahe gelegen, in der Datenschutzgrundverordnung eng begrenzte klare Erlaubnistatbestände für Profilbildungen zu formulieren, Transparenz und Informiertheit der Betroffenen ausdrücklich

zu gewährleisten und etwa eine Verpflichtung zu frühestmöglicher Anonymisierung oder Pseudonymisierung der für die Profilbildung und Auswertung verwendeten Daten festzuschreiben. Die Formulierung eines solchen verbindlichen und hohen Datenschutzniveaus hätte auch im Interesse der Internetwirtschaft gelegen, weil sie das Vertrauen der Menschen in Internettransaktionen erhöht hätte. Insofern werden sich die Lobbyisten der Datenschutzrechte gemeinsam mit den Lobbyistinnen des freien Datenverkehres über die zu erwartenden Entscheidungen des Europäischen Gerichtshofes freuen!

1.4 Da kommt was auf uns zu. Oder: Was der Landesgesetzgeber nach Erlass der Datenschutzgrundverordnung entscheiden muss

Eines steht fest: Nach Verabschiedung der Datenschutzgrundverordnung werden auf die nationalstaatlichen Gesetzgeber sehr viele Entscheidungen über die Beurteilung des jetzt geltenden Rechts zukommen. Auch der bremische Landesgesetzgeber muss für alle Normen, die gegenwärtig Datenverarbeitungsregelungen enthalten, prüfen, ob das Landesrecht durch die Datenschutzgrundverordnung **ersetzt** wird, die Datenschutzgrundverordnung also direkt gilt, ob das Landesrecht **beibehalten** bleiben kann und soll, oder ob das Landesrecht unter Beachtung der Datenschutzgrundverordnung **geändert** werden soll. Das gilt beispielsweise für das Bremisches Datenschutzgesetz, das Bremische Schuldatenschutzgesetz, das Bremische Krankenhausdatenschutzgesetz, das Bremische Archivgesetz, das bremische Pressegesetz, das Bremische Polizeigesetz, das Bremische Hilfeleistungsgesetz, das Gesetz über das Krebsregister der Freien Hansestadt Bremen, das Bremische Naturschutzgesetz, das bremische Vergabegesetz, das Bremische Beamtengesetz und das Bremische Hafenbetriebsgesetz. Über den Bundesrat ist Bremen daneben auch an der Bundesgesetzgebung beteiligt, die ebenfalls weitreichende Aufgaben bei der Konkretisierung der Datenschutzgrundverordnung zu erfüllen hat.

Dies alles gibt dem bremischen Gesetzgeber die Chance, den durch die Datenschutzgrundverordnung eröffneten gesetzgeberischen Spielraum im Sinne des durch die Europäische Grundrechtecharta geforderten höchstmöglichen Grundrechtsschutzes zu nutzen. Das Pochen auf die demokratisierende Funktion von Grundrechtsschutz wäre jetzt genau die richtige Reaktion auf die im Berichtsjahr verübten offenbar zutiefst antidemokratisch motivierten Attentate.

Dr. Imke Sommer

2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 37. Jahresberichts

Der Bericht und Antrag des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zum 37. Jahresbericht der Landesbeauftragten für Datenschutz vom 20. März 2015 (Drucksache 18/1795) und zur Stellungnahme des Senats vom 11. August 2015 (Drucksache 19/44) lag zum Redaktionsschluss noch nicht vor.

3. Behördliche und betriebliche Beauftragte für den Datenschutz

3.1 Bestellung betrieblicher Datenschutzbeauftragter durch Verbundunternehmen

Von einem Bremer Kreditinstitut wurden wir unterrichtet, dass der bisherige betriebliche Datenschutzbeauftragte mit diesem Amt nicht länger betraut sei, weil er in den Ruhestand trete. Die Funktion des betrieblichen Datenschutzbeauftragten werde künftig von einem Mitarbeiter der Muttergesellschaft der Bank als externem Beauftragten wahrgenommen. Das Bremer Kreditinstitut schlösse sich somit der Linie zahlreicher Konzernverbünde an, bei denen von den einzelnen zum Verbund gehörenden Unternehmen eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter bestellt worden sei.

Bei der Bestellung des betrieblichen Datenschutzbeauftragten durch das Bremer Kreditinstitut war zu beachten, dass gemäß § 4f Absatz 1 Satz 1 Bundesdatenschutzgesetz jede nicht öffentliche Stelle, die personenbezogene Daten automatisiert verarbeitet, eine Beauftragte beziehungsweise einen Beauftragten für den Datenschutz zu bestellen hat. Grundsätzlich sind somit alle verantwortlichen Stellen zur Bestellung einer oder eines Beauftragten für den Datenschutz verpflichtet. Die zur Bestellung verpflichtete Stelle bestimmt selbstständig und eigenverantwortlich, wer für ihren Tätigkeitsbereich die von den Datenschutzgesetzen näher genannten Aufgaben wahrnehmen soll. Auch einzelne zu einem Konzernverbund gehörende Stellen, die für die Verarbeitung personenbezogener Daten Verantwortung tragen, müssen jeweils für sich betriebliche Datenschutzbeauftragte bestellen.

Außerdem muss bei der gemeinsamen Bestellung beachtet werden, dass es jeweils gegenläufige Unternehmensinteressen geben kann, die die Datenschutzbeauftragten Konflikten aussetzen können, die mit ihrer Funktion unvereinbar sind. Zu solchen Konflikten kann es zum Beispiel kommen, wenn innerhalb eines Konzernverbunds die eine Stelle Auftraggeberin und die andere Stelle Auftragnehmerin ist. Mit den datenschutzrechtlichen Anforderungen wäre es darüber hinaus nicht zu vereinbaren, wenn die zum Verbund

gehörenden Unternehmen Datenschutzbeauftragte nach Vorgabe der Konzernmutter bestellten.

Im vorliegenden Fall wurden zwischen dem Bremer Kreditinstitut und der Konzernmutter feste Regelungen zur Ausgestaltung der Tätigkeit des neuen Datenschutzbeauftragten getroffen. Diese Regelungen sehen unter anderem vor, dass der betreffende Mitarbeiter von der Konzernmutter für die Tätigkeit des Datenschutzbeauftragten freizustellen ist, die Konzernmutter nicht berechtigt ist, dem Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben für das Bremer Kreditinstitut Weisungen zu erteilen. Daneben wurde festgelegt, dass der Datenschutzbeauftragte unmittelbar der Geschäftsleitung des Bremer Kreditinstituts unterstellt ist, er nur dieser berichtspflichtig ist und bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei und eigenverantwortlich tätig ist. Auch wurde der Datenschutzbeauftragte vom Bremer Kreditinstitut zum Datenschutzbeauftragten bestellt.

3.2 Unvereinbarkeiten bei der Bestellung behördlicher Datenschutzbeauftragter

Wiederholt waren wir im Berichtsjahr mit der Unvereinbarkeit von anderen dienstlichen Tätigkeiten mit der Funktion der oder des behördlichen Datenschutzbeauftragten befasst.

Um ihren Aufgaben gerecht zu werden und diesen effektiv nachkommen zu können, müssen behördliche Datenschutzbeauftragte über die für ihr Amt notwendige Fachkunde und Zuverlässigkeit verfügen. Die Zuverlässigkeit untergliedert sich in die objektive und subjektive Zuverlässigkeit. Die objektive Zuverlässigkeit ist insbesondere beeinträchtigt und nicht ausreichend gegeben, wenn die Beauftragtenfunktion von der Amtsinhaberin oder dem Amtsinhaber gemeinsam mit anderen Tätigkeiten, die auch Entscheidungen hinsichtlich der personenbezogenen Datenverarbeitung einer Stelle umfassen, wahrgenommen wird. Die beziehungsweise der behördliche Datenschutzbeauftragte würden dann die Rechtmäßigkeit der eigenen Entscheidung überwachen, was mit dem Bremischen Datenschutzgesetz nicht zu vereinbaren ist. Daher dürfen insbesondere die folgenden Funktionsträgerinnen und Funktionsträger nicht zu behördlichen Datenschutzbeauftragten bestellt werden: Amtsleiterinnen und Amtsleiter, Vorstände, Geschäftsführerinnen und Geschäftsführer, sonstige gesetzlich oder verfassungsmäßig berufene Leiterinnen und Leiter sowie Datenverarbeitungsleiterinnen und Datenverarbeitungsleiter, Personalverantwortliche, leitende Mitarbeiterinnen und Mitarbeiter von Organisationseinheiten mit besonders umfangreicher oder sensitiver Datenverarbeitung.

Der behördliche Datenschutzbeauftragte der Staatsanwaltschaft Bremen war dort gleichzeitig auch als IT-Leiter und stellvertretender Geschäftsleiter tätig. Bei beiden Tätigkeiten hatte er im Hinblick auf die personenbezogene Datenverarbeitung seiner Behörde umfangreiche Entscheidungsbefugnisse. Wie vorstehend erläutert war dies mit den

Bestimmungen des Bremischen Datenschutzgesetzes nicht zu vereinbaren, worauf wir die Staatsanwaltschaft hinwiesen. Der Leitende Oberstaatsanwalt teilte unsere Rechtsauffassung. Mit dem Einverständnis des bisherigen behördlichen Datenschutzbeauftragten wurde dieser abberufen und ein neuer Datenschutzbeauftragter bestellt.

Auch bei der Feuerwehr Bremerhaven erfolgte eine Neubesetzung des Amtes der beziehungsweise des behördlichen Datenschutzbeauftragten, nachdem wir die gleichzeitige Wahrnehmung der Aufgaben des behördlichen Datenschutzbeauftragten und Aufgaben mit erheblichen Entscheidungsbefugnissen im IT-Bereich und im Personalbereich durch den bisherigen Beauftragten kritisiert hatten. Da es möglich ist, dass es entsprechende Unvereinbarkeiten auch bei anderen Stellen der Stadt Bremerhaven gibt, baten wir die Magistratskanzlei, die Ämter und Einrichtungen der Stadt auf die zu beachtende Rechtslage hinzuweisen, was diese durch eine entsprechende Mitteilung an alle Verwaltungsstellen der Stadt umsetzte.

3.3 Bestellung behördlicher Datenschutzbeauftragter durch die Ortsämter

Die Ortsämter der Stadt Bremen haben die Aufgabe, die bei ihnen wirkenden Beiräte bei der Erfüllung ihrer Aufgaben zu unterstützen und ihre Beschlüsse bei den Behörden und anderen zuständigen Stellen zu vertreten. Sie sind verpflichtet, den gegenseitigen Kontakt zwischen den Einwohnerinnen und Einwohnern, Beiräten und Behörden zu fördern. Sie müssen bei allen Angelegenheiten, die von öffentlichem Interesse sind und ihren örtlichen Zuständigkeitsbereich betreffen, tätig werden, zudem Wünschen, Hinweisen und Beschwerden aus der Bevölkerung nachgehen.

Nach dem Ausscheiden des früheren Amtsinhabers, den die bremischen Ortsämter gemeinsam bestellt hatten, ist die Funktion der oder des behördlichen Datenschutzbeauftragten der Ortsämter seit langem unbesetzt. Da die einzelnen Ortsämter aber zur Bestellung einer oder eines behördlichen Datenschutzbeauftragten verpflichtet sind, schrieben wir sie mittels eines Rundschreibens an und baten um Mitteilung, ob eine Neubestellung erfolgt sei. Falls dies nicht der Fall sei, baten wir, die Bestellung kurzfristig nachzuholen. Die Ortsämter teilten uns hierzu mit, dass wir eine Stellungnahme auf unser Rundschreiben von der ihnen vorgesetzten Senatskanzlei erhalten würden. Trotz mehrmaliger Erinnerung haben wir diese von dort bislang nicht erhalten.

3.4 Bestellung behördlicher Datenschutzbeauftragter durch die Regionalen Beratungs- und Unterstützungszentren

Bereits im Jahr 2010 wurden in Bremen und Bremerhaven schulbezogene Regionale Beratungs- und Unterstützungszentren (ReBUz) gegründet, die unter anderem für die Bereiche Diagnostik, Prävention und Intervention bei Krisen, Notfällen und Gewaltvorkommnissen zuständig sind. Bei der Wahrnehmung ihrer Aufgaben werden von den ReBUz auch äußerst sensible personenbezogene Daten, insbesondere von Schülerinnen und Schülern, verarbeitet.

Die ReBUz sind eigenständige öffentliche Stellen, die gemäß § 7a Absatz 1 Bremisches Datenschutzgesetz eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten zu bestellen haben. Deshalb schrieben wir im August des Berichtsjahrs alle ReBUz an und baten um Mitteilung, wer dort die Aufgaben der beziehungsweise des behördlichen Datenschutzbeauftragten wahrnimmt. Für den Fall, dass eine Bestellung nicht erfolgt war, baten wir alle Zentren, diese kurzfristig nachzuholen. Antworten auf unser Rundschreiben erhielten wir von den ReBUz selbst nicht. Die Senatorin für Kinder und Bildung bat uns, gemeinsam die Pflicht zur Bestellung einer oder eines behördlichen Datenschutzbeauftragten durch die ReBUz in Bremen näher zu erörtern. Dazu sind wir im Stadium der Terminabsprachen. In Bremerhaven wurde dem behördlichen Datenschutzbeauftragten des Schulamtes und der Schulen die Funktion des Datenschutzbeauftragten für das dortige ReBUz mitübertragen.

3.5 Treffen der behördlichen Datenschutzbeauftragten

Auch im Berichtsjahr trafen sich die behördlichen Datenschutzbeauftragten aus Bremen und Bremerhaven zu gemeinsamen Veranstaltungen, bei denen schwerpunktmäßig ein bestimmtes Thema behandelt wurde, bei denen sie aber auch Gelegenheit zum gegenseitigen Erfahrungsaustausch hatten.

Bei dem ersten Treffen im Frühjahr wurde schwerpunktmäßig das Thema "Einsatz von Aktenverwaltungssystemen in der Verwaltung und die damit verbundenen datenschutzrechtlichen Probleme" behandelt. Als zentrales Dokumentenmanagementsystem gelangt in der bremischen Verwaltung in vielen Dienststellen VISkompakt zum Einsatz. Bei der Präsentation dieses Themas konnten die mit dem Einsatz eines solchen Systems verbundenen Fragestellungen detailliert, auch in Bezug auf die Nutzung anderer Systeme angesprochen werden. Das zweite Treffen im Herbst befasste sich schwerpunktmäßig mit dem Thema "Datensicherheit unter Beachtung der Entscheidung des Europäischen Gerichtshofs zu Safe Harbor"(siehe hierzu Ziffer 15.2 dieses Berichts).

Beide Veranstaltungen stießen bei den behördlichen Datenschutzbeauftragten auf große Resonanz. Sie nutzten die Gelegenheit, über ihre Tätigkeit, ihre Erfahrungen und ihre Probleme bei der Amtswahrnehmung zu berichten und darüber mit den anderen Teilnehmerinnen und Teilnehmern sehr engagiert zu diskutieren. Insbesondere die den Datenschutzbeauftragten neben ihren sonstigen Tätigkeiten fehlende Zeit für die Wahrnehmung ihrer Aufgaben wurde oft als problematisch geschildert. Die Vertreter der Landesbeauftragten für Datenschutz und Informationsfreiheit erneuerten ihr Angebot, die behördlichen Datenschutzbeauftragten bei der Lösung ihrer Probleme zu unterstützen. Für das Jahr 2016 sind weitere Treffen der behördlichen Datenschutzbeauftragten geplant.

4. Verwaltungsübergreifende Verfahren

4.1 BASIS.bremen – datenschutzgerechter Betrieb

Am 29. November 2011 beschloss der Bremer Senat die Standardisierung des Supports (Unterstützung) und des Betriebs der Informationstechnologie zur Verbesserung der Qualität und Sicherheit. Er schuf damit auch die Grundlage für die Umsetzung unserer zum damaligen Zeitpunkt formulierten Sicherheitsanforderungen (siehe 33. Jahresbericht, Ziffer 4.4.1). Damals hatte die Senatorin für Finanzen zugesichert, die noch offenen Sicherheitsfragen während des Projektverlaufs zu klären und unsere Anforderungen umzusetzen. Der seit dem Jahr 2012 laufende Migrationsprozess (Umstellung auf eine andere Technologie) zum standardisierten Betrieb von Verwaltungsarbeitsplätzen (BASIS.bremen) erfolgte entgegen der Zusage ohne die Umsetzung der von uns gestellten Anforderungen. Bis zum Berichtsjahr 2013 lieferte die Projektarbeitsgruppe Datenschutz und Datensicherheit, in der unsere Anforderungen bearbeitet werden sollten, keine Ergebnisse. Deshalb bündelten wir (siehe 36. Jahresbericht, Ziffer 4.4) unsere Anforderungen und übergaben den entsprechenden Katalog der Senatorin für Finanzen mit der Forderung, bis März 2014 einen Umsetzungsplan vorzulegen. Hierzu initiierte die Senatorin für Finanzen bereits im vergangenen Berichtsjahr einen Workshop mit einer durch das IfIB (Institut für Informationsmanagement Bremen GmbH) durchgeführten Moderation, der in diesem Jahr seine Arbeit fortsetzte. Am Workshop nahmen Vertreterinnen und Vertreter der Senatorin für Finanzen, des Gesundheitsamtes Bremen und der Senatorin für Soziales, Kinder, Jugend und Frauen teil. Wir beteiligten uns an diesem Workshop beratend.

Im Ergebnis wurde eine Reihe von dokumentarischen Grundlagen erarbeitet, die insbesondere eine systematische Erfassung der Geschäftsprozesse für die verarbeiteten Daten ermöglichen. Das Gesundheitsamt Bremen nahm die besonders hohe Schutzbedürftigkeit seiner Daten zum Anlass, für sich eine Analyse nach dem IT-Grundschutzmodell des Bundesamtes für Sicherheit in der Informationstechnik (eine Methode zur Durchführung des Sicherheitsmanagements einer Institution) vorzunehmen. In

diesem Rahmen wurden eine IT-Strukturanalyse, eine Schutzbedarfsfeststellung und eine Risikoanalyse durchgeführt mit der daraus abgeleiteten Beschreibung der einzusetzenden besonderen Maßnahmen, die den hohen Schutzbedarf gewährleisten sollen. Die systematische Durchführung der Analysen ist in dieser Form für alle Dienststellen übertragbar und durchführbar. Sie sind auch erforderlich, um aufgrund des daraus resultierenden Schutzbedarfs die notwendigen Sicherheitsmaßnahmen definieren und umsetzen zu können.

In diesem Berichtsjahr wurde intensiv an der Einführung eines zentralen Sicherheitsmoduls gearbeitet. Zusammen mit der Anstalt öffentlichen Rechts Dataport, der IT-Dienstleisterin der Freien Hansestadt Bremen, wurde ein Betriebskonzept für eine Dateiverschlüsselung und Netzwerkverschlüsselung erstellt. Die Integration einer File (Datei) Service Verschlüsselung in den BASIS.bremen Betrieb ist ein wesentlicher Baustein zur Gewährleistung eines der Schutzstufe hoch entsprechenden Sicherheitsstandards. Neben grundsätzlichen Fragen zur Betriebssicherheit von Sicherheitsprodukten wie der Verschlüsselungssoftware wurden einzelne Verfahrensschritte, wie beispielsweise die Beantragung eines Schlüssels und deren Durchführung, behandelt. Wir begrüßen ausdrücklich die Bereitstellung des Verschlüsselungsmoduls im Rahmen des BASIS.bremen Betriebs, halten es aber für erforderlich, dass der Betrieb des Sicherheitsproduktes dem Schutzbedarf der Daten, also hoch, entspricht. Deshalb forderten wir vor Inbetriebnahme des Produktes Verbesserungen, wie etwa einen revisionssicheren Beantragungsvorgang, einen Sicherheitsnachweis für die Verschlüsselungsinfrastruktur und ein sicheres Schlüsselmanagement.

Des Weiteren steht nun ein mit uns abgestimmtes Muster zum Abschluss von SSLAs (security service level agreements/Sicherheitsdienstleistungsvereinbarungen) zur Verfügung, das eine vertragliche Sicherstellung des von den für die Daten verantwortlichen Dienststellen geforderten Schutzniveaus ermöglicht. Diese Vereinbarungen zur Gewährleistung der Sicherheit bei Dataport sollten für alle wesentlichen Infrastrukturkomponenten, wie den Verzeichnisdienst (Active directory), die elektronische Post, die Administrationsplattform und die Grundschutzkonformität des Netzes, erfolgen. Ziel ist es, sicherheitstechnisch und dokumentarisch die Bereiche der Arbeitsplatzrechner (Clients), die die lokale Verantwortung vom Arbeitsplatzrechner bis zum Router (Vermittlungsknoten) des Hauses umfasst, der Netze und der Infrastruktur im Rechenzentrum zu erfassen. Unabhängig vom Abschluss einer Sicherheitsdienstleistungsvereinbarung ist jedoch weiterhin die Verpflichtung Dataports als Auftragnehmerin, die Durchführung der gesetzlich vorgeschriebenen Auftragskontrolle (§ 9 Bremisches Datenschutzgesetz) zu gewährleisten.

Bisher sind die konzeptionellen Weichen gestellt und das erste Modul zur Gewährleistung eines hohen Schutzbedarfs, die Möglichkeit der Verschlüsselung, steht kurz vor der

Einführung. Erst die komplette Umsetzung unserer Anforderungen liefert allerdings die Basis für die Etablierung eines dynamischen und notwendigen Sicherheitsprozesses. Da die konzeptionellen Grundlagen weitgehend geschaffen sind, erwarten wir, dass die datenschutzrechtlich erforderlichen Implementierungen technischer Maßnahmen zeitnah erfolgen werden.

4.2 Länderübergreifende Zusammenarbeit im IT-Bereich

Die von sechs Bundesländern getragene Körperschaft öffentlichen Rechts Dataport ist auch zentrale IT-Dienstleisterin der Freien Hansestadt Bremen. Laut Staatsvertrag werden durch den Zusammenschluss für die an Dataport beteiligten Trägerländer Synergieeffekte erwartet.

Über den zentralen länderübergreifenden Verzeichnisdienst, das Active Directory (AD) als technische Lösung, die länderübergreifend genutzt werden kann, berichteten wir zuletzt in unserem 36. Jahresbericht unter Ziffer 4.6. Dort wiesen wir darauf hin, dass bislang in Bremen eine Rechtsgrundlage für den Betrieb länderübergreifender Verfahren, wie beispielsweise eines zentralen AD, fehlt. Im Berichtsjahr wurde uns eine technische Lösung vorgestellt, mit der dem Problem der fehlenden Rechtsgrundlage begegnet werden sollte. Dazu wurde bei Dataport ein zentrales AD errichtet, das den jeweiligen Landes-AD vertraut, und in dem jedes Konto aus den vertrauten Landes-AD ein entsprechendes Konto hat. Zwischen den Konten im zentralen AD und den zugehörigen Konten in den Länder-AD besteht also eine Eins-zu-Eins-Beziehung. Die Konten im zentralen AD wurden deaktiviert. Wir wiesen im Rahmen von Gesprächen darauf hin, dass deaktivierte Konten nach wie vor Personenbezug haben, weil sie eindeutig Benutzerkonten einzelner Personen und damit den Personen direkt zuzuordnen sind. Nach unserer Auffassung stellt das zentrale AD damit in der beschriebenen Form ein zentrales Verfahren dar, in dem personenbezogene Daten länderübergreifend gespeichert und verarbeitet werden, sodass wir weiterhin der Auffassung sind, dass es an einer Rechtsgrundlage fehlt.

Eine ähnliche grundsätzliche Konstellation besteht bei einem weiteren länderübergreifenden und zentral bei Dataport betriebenen Projekt. Das Projekt trägt den Namen "Community Cloud Mail Service" (CCMS) und steht für eine durch die Trägerländer gemeinsam genutzte Infrastruktur zur Nutzung des elektronischen E-Mail-Verkehrs, zur Terminverwaltung und Aufgabenplanung. Die bisher in den Ländern bestehenden Infrastrukturen werden durch CCMS abgelöst. Technische Basis für das CCMS ist Microsoft Exchange und ein, wie oben beschriebenes, zentrales länderübergreifendes AD. Das Projekt befindet sich seit Sommer 2015 in der Realisierung, zunächst in Hamburg, dann in Bremen und zuletzt ab Anfang 2016 auch in Schleswig-Holstein.

Zunächst vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit erhielten wir einen Hinweis auf dieses bevorstehende Projekt und wurden kurz danach auch

durch die Senatorin für Finanzen informiert. Da das Projekt länderübergreifend installiert wird, bemühen sich die Datenschutzbeauftragten der Dataport-Trägerländer, wie bei anderen gemeinsamen IT-Verfahren und gemeinsam genutzter IT-Infrastruktur, um eine enge inhaltliche Abstimmung untereinander. Basis hierfür ist zumindest eine einheitliche Dokumentenlage in allen betroffenen Bundesländern. Die Dokumentenlage war unbefriedigend. Viele Dokumente mit zentraler Bedeutung für eine Einschätzung der Einhaltung der gesetzlich geforderten technischen und rechtlichen Maßnahmen waren unvollständig. Trotzdem wurde im Sommer 2015 für Hamburg die Migration von Echtdaten in die CCMS-Anwendung begonnen. Die bis dahin vorliegenden Unterlagen wiesen aus, dass drei Ländermandanten geplant sind. Das Mandantenkonzept hatte einen Stand von Dezember 2014 und beschrieb keine hinreichenden Maßnahmen, um die Anforderungen der Prüfschritte gemäß der "Orientierungshilfe Mandantenfähigkeit"[4] des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu erfüllen und damit eine effektive Mandantentrennung zu realisieren.

Problematisch ist aus unserer Sicht, dass das CCMS-Konzept eine Öffnung der Kalender und Postfächer der einzelnen Teilnehmerinnen und Teilnehmer sowohl landesintern als auch länderübergreifend ermöglicht. Länderübergreifende Freigaben müssen einmal in den jeweils beiden beteiligten Ländern freigegeben werden. Das geschieht immer landesweit. Eine technische Hürde, die es ermöglichen würde, dass die Nutzerinnen und Nutzer aus einem Land etwa individuell entscheiden können, ob der Kalender oder das Postfach für die Nutzer aus einem anderen Land prinzipiell freigegeben werden kann, besteht nicht. Die Öffnung der Kalenderdaten führt gleichzeitig dazu, dass auch E-Mail-Inhalte für Nutzerinnen und Nutzer des anderen Mandanten sichtbar geschaltet werden können. Diese Einstellung kann benutzerindividuell vorgenommen werden, sobald landesweit die Möglichkeit der gegenseitigen, länderübergreifenden Einsichtnahme für Kalenderdaten freigeschaltet wurde. Weder die Freischaltung der Outlook-Postfächer noch ein Zugriff auf diese aus einem anderen Mandanten wird protokolliert. Durch die Öffnung der Kalender werden somit auf Nutzerebene lesende Zugriffe auf Kalenderinhalte und E-Mail-Inhalte eines anderen Mandanten möglich. Dies steht den Anforderungen der "Orientierungshilfe Mandantenfähigkeit" der Datenschutzbeauftragten des Bundes und der Länder entgegen. In der Orientierungshilfe ist eindeutig festgelegt, dass Inhaltsdaten nur in genau einem Mandanten verarbeitet werden dürfen und Zugriffe auf Inhaltsdaten eines anderen Mandanten nicht zulässig sind. Da die Möglichkeit besteht, ohne großen technischen Aufwand die Mandantengrenzen für das CCMS aufzuheben, gehen wir nach derzeitigem Kenntnisstand davon aus, dass das CCMS prinzipiell keine Mandantenfähigkeit im Sinne der Orientierungshilfe aufweist.

[4] https://ssl.bremen.de/datenschutz/sixcms/media.php/13/TOP08_20121011_OH_Mandantenfaehigkeit_v10_b.pdf

Die Annahme "Mandant = Bundesland" halten wir im Übrigen für eine zu grobe Einteilung. So erfordert das Bremische Datenschutzgesetz, dass die jeweils datenschutzrechtlich verantwortlichen Stellen in die Lage versetzt werden, durch Konfigurationsvorgaben Zugriffsmöglichkeiten auf Kalender oder E-Mail-Inhalte ausschließlich auf ihren Teilnehmerkreis beschränken zu können.

Unabhängig von der fehlenden vollständigen Mandantenfähigkeit handelt es sich bei dem CCMS wie bei dem oben beschriebenen AD, um ein gemeinsames länderübergreifendes Verfahren, für dessen Betrieb in Bremen bislang eine Rechtsgrundlage fehlt.

4.3 SAP-Verfahren in Bremen

In der bremischen Kernverwaltung wird das Softwarepaket SAP flächendeckend und auch in diversen Eigenbetrieben, sonstigen Sondervermögen, Gesellschaften, Anstalten sowie in der Universität Bremen und in den Hochschulen eingesetzt. Wir berichteten in der Vergangenheit von der Überarbeitung der konzeptionellen Verankerung des Systems (vergleiche 37. Jahresbericht, Ziffer 4.4) und stellten auch in diesem Berichtsjahr fest, dass die diversen Konzepte weiterhin einer grundsätzlichen Überarbeitung bedürfen. Die konkrete Umsetzung der erarbeiteten Anforderungen aus den Konzepten zur Reorganisation der Berechtigungen und vor allem die Implementierung der Berechtigungen wurden uns leider noch nicht berichtet. Die Erstellung der Berechtigungen und der Funktionstest für diese Reorganisation sollten ohne personenbezogene Echtdaten ausgeführt werden. Für den darauf folgenden Integrationstest erwarten wir die Erstellung eines Sicherheitskonzepts, dessen Umsetzung den Zugriff auf personenbezogene Daten effektiv verhindert. Im Projekt Ticketmanagement der fachlichen Leitstelle für SAP wurden uns im Berichtsjahr für den Prozess "Passwort-Selfservice", mit dem eine Nutzerin oder ein Nutzer des Systems elektronisch das eigene Kennwort zurücksetzen kann, Dokumente vorgelegt, die für eine Bewertung ausreichend waren. Die von uns identifizierten Schwachstellen in der Prozessbeschreibung wurden im Konzept überarbeitet. Der Prozess ist Teil eines Konzeptes für die Bearbeitung von Fehlermeldungen sowie für das Berechtigungsmanagement, für das der "fachlichen Leitstelle SAP" der Senatorin für Finanzen eine Stellungnahme unsererseits vorliegt. Eine Benachrichtigung, dass das von uns im letzten Berichtsjahr geforderte Projekt zur kontinuierlichen Anpassung der Dokumentenlage und deren Umsetzung gestartet wurde, haben wir leider nicht erhalten. Dieses Projekt sollte die technischen und organisatorischen Maßnahmen zur Umsetzung des Datenschutzes bei dem Betrieb von SAP kontinuierlich auf dem neuesten Stand halten.

5. Inneres

5.1 Allgemeines zu den Polizeiverfahren

Aktuell unterliegen die polizeilichen Informationssysteme @rtus und PIER (Polizeiliches Informationssystem Ermittlung und Recherche) unserer datenschutzrechtlichen Bewertung.

Der Fokus in Bezug auf das polizeiliche Informationssystem @rtus liegt neben der Ausgestaltung der Protokollierung, des Zugriffskonzepts und des Berechtigungskonzepts auf der Anbindung bei der Anstalt öffentlichen Rechts Dataport im Rahmen des Data Center Polizeien (vergleiche 37. Jahresbericht, Ziffer 5.4). In der letzten Zeit ist die Zahl datenschutzrechtlicher Auskunftsanträge zu @rtus erheblich gestiegen. Der Zeitraum zwischen Antragstellung und Erteilung der entsprechenden Auskünfte hat sich ebenfalls auf derzeit etwa vier bis sechs Wochen verlängert. Hier könnte überlegt werden, eine Softwarelösung anzustreben, um Auskunftsersuchen schneller und damit effektiver zu bearbeiten.

Gegenstand der datenschutzrechtlichen und datenschutztechnischen Auseinandersetzung im Rahmen von PIER sind die Schnittstelle XPolizei, die Protokollierung (insbesondere die Möglichkeit der Abschaltung der Protokollierung), die Auftragsdatenverarbeitung, das Berechtigungskonzept sowie Funktionen wie Volltextrecherche im Mandanten und nicht im Verfahren selbst, die Änderung der Treffermengenbegrenzung sowie das Telekommunikationsüberwachungsmodul.

Die offenen Themen einer Besprechung mit der Polizei Bremen im Oktober 2015 waren neben den oben genannten Polizeiverfahren @rtus und PIER auch noch das Rahmendatenschutzkonzept, die elektronische Akte mit VISkompakt, das Rechen- und Dienstleistungszentrum für die Telekommunikationsüberwachung sowie das Datenschutzkonzept für die Telekommunikationsüberwachung mit dem Landeskriminalamt Niedersachsen (vergleiche 37. Jahresbericht, Ziffer 5.2), das fehlende Datenschutzkonzept für das Verfahren INPOL-Land und die noch ausstehende Mitteilung des behördlichen Datenschutzbeauftragten über die Ergebnisse der Vorabkontrollen betreffend Intrapol (vergleiche 37. Jahresbericht, Ziffer 5.3).

5.2 Einsatz der BodyCam bei der Polizei Bremen

Im Berichtsjahr haben wir das Konzept zum Einsatz der BodyCam, namentlich der Schulterkamera, vom Senator für Inneres datenschutzrechtlich bewertet. Unsere Stellungnahme zieht das Fazit, dass das beschriebene Konzept zum Einsatz der BodyCam mit § 29 Bremisches Polizeigesetz (BremPolG) in seiner gegenwärtigen Gestalt unvereinbar ist. § 29 BremPolG enthält historisch bedingt Regelungen zu fest installierten Videokameras

und erlaubt nicht den tiefer in das Grundrecht auf informationelle Selbstbestimmung eingreifenden polizeilichen Einsatz der BodyCam.

Als mobile Videotechnik greift die BodyCam in das informationelle Selbstbestimmungsrecht der erfassten Personen anders ein als eine fest installierte Videokamera, welche durch die Funktionen Schwenken oder Zoomen geprägt ist. Historisch hat der Gesetzgeber bei Schaffung von § 29 BremPolG an fest verankerte Videoinstallationen gedacht, die einen klar definierten Bereich, also im öffentlichen Verkehrsraum oder öffentlich zugängliche Orte, erfasst. Das Erfüllen dieser grundsätzlichen Tatbestandsmerkmale ist bei dem polizeilichen Einsatz der BodyCam nicht möglich. Beim Aufzeichnen mit einer Schulterkamera kann nicht ausgeschlossen werden, dass private oder nicht öffentlich zugängliche Orte wie Fenster oder Türen von Wohnungen oder ein Geschäftsbereich, der den Zutritt nur für Betriebsangehörige vorsieht, ein Parkhaus außerhalb der Öffnungszeiten oder eine Tankstelle außerhalb der Öffnungszeiten versehentlich (eventuell auch nur im Hintergrund) mitgefilmt werden. Bei einer festinstallierten Kamera kann dies durch Schwärzen oder Verpixeln dieser festen Bereiche ausgeschlossen werden. Dies kann bei dem Einsatz mobiler Videotechnik wie der Schulterkamera nur durch organisatorische Maßnahmen erreicht werden. Rein faktisch ist eine solche Aufzeichnung nicht ausgeschlossen.

Bei einer mobilen Videotechnik wie zum Beispiel bei der Schulterkamera können sich die Bürgerinnen und Bürger auch nicht im Vorfeld überlegen, ob sie diesen Bereich der Videoüberwachung meiden. Diese Wahl haben sie aber bei einer festinstallierten Videoanlage durch die Hinweisschilder auf den überwachten Bereich. Der Aufnahmebereich der mobilen Videotechnik ist deutlich flexibler und eher zufällig. Diese Flexibilität ist abzuwägen mit den schutzwürdigen Belangen von Betroffenen, Dritten sowie Polizeibeamtinnen und Polizeibeamten selbst. Auch sind für die Bürgerinnen und Bürger weder die Reichweite der mobilen Videotechnik wie zum Beispiel der Schulterkamera noch die Qualität (beispielsweise durch mögliches Zoomen in den Hintergrund) erkennbar. Der Einsatz einer BodyCam birgt damit eine höhere Gefahr für den Eingriff in das informationelle Selbstbestimmungsrecht als eine fest installierte Videokamera.

Der Einsatz mobiler Videotechnik ist von neuer, eingriffsintensiverer Qualität und erfordert deshalb eine eigene Rechtsgrundlage im Bremischen Polizeigesetz. Neben der Schaffung einer klaren rechtlichen Regelung ist im Zusammenhang mit dem Einsatz von Schulterkameras wichtig, dass die mobile Videotechnik nur als eine ergänzende Maßnahme der polizeilichen Eigensicherung zur Reduzierung von Übergriffen auf Polizeibeamtinnen und Polizeibeamte betrachtet werden kann und weiterhin mit den klassischen, deeskalierenden Maßnahmen gegen mögliche Störer im öffentlichen Raum vorzugehen ist.

Im November 2015 legte uns der Senator für Inneres einen Entwurf zur Änderung von § 29 Absatz 5 BremPolG zur Stellungnahme vor. In unserer Stellungnahme äußerten wir

wegen der Weite des Entwurfs verfassungsrechtliche Zweifel daran, dass der Entwurf den kompetenzrechtlichen Maßgaben des Artikel 74 Absatz 1 Nummer 1 Grundgesetz entspricht, weil die Videoüberwachung auch Strafverfolgungszwecken dienen sollte, deren Regelung in der Strafprozessordnung dem Bundesgesetzgeber zuzuordnen ist. In dem Entwurf kam auch nicht zum Ausdruck, dass die Polizei die BodyCam nur in Kontrollsituationen, die eine Identitätsfeststellung ermöglichen sollen, einsetzen möchte. Wir betonten, dass durch das flexible Anfertigen von Tonaufnahmen und Videoaufnahmen ein sehr tief gehender, intensiver Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt. Außerdem forderten wir Maßnahmen im Hinblick auf Artikel 10 und Artikel 13 Grundgesetz: Es sollten Überlegungen angestellt werden, wie damit umgegangen wird, wenn beispielsweise zufällig ein Telefonat einer beziehungsweise eines Unbeteiligten oder auch eine Unbeteiligte beziehungsweise ein Unbeteiligter, die oder der in einem Wohnungsfenster zu sehen ist, mit aufgezeichnet werden. Wir unterbreiteten einen Textvorschlag für § 29 Absatz 5 BremPolG, wobei wir uns am neu gefassten § 14 Absatz 6 des Hessischen Sicherheits- und Ordnungsgesetzes orientierten, der am 1. November 2015 in Kraft trat. Seit Dezember 2015 befinden wir uns mit dem Senator für Inneres im konstruktiven Gespräch über die Ausgestaltung von § 29 Absatz 5 BremPolG.

5.3 Prüfung der Antiterrordatei

In diesem Berichtsjahr war die Prüfung der Antiterrordatei beim Landeskriminalamt Bremen und beim Landesamt für Verfassungsschutz weiterhin Gegenstand unserer datenschutzrechtlichen Prüfung (vergleiche 37. Jahresbericht, Ziffer 5.7). Im Wesentlichen lässt sich zusammenfassen, dass die Auswertung der Protokolldaten eine Herausforderung darstellte und dass Änderungen größtenteils nicht nachvollziehbar waren, weil die Protokollierung diese nicht kennzeichnete.

Die Unterarbeitsgruppe "Antiterrordatei" des Arbeitskreises Sicherheit der Datenschutzbeauftragten des Bundes und der Länder hatte vereinbart, entsprechend der Aussagen im Urteil des Bundesverfassungsgerichts vom 24. April 2013 zum Gesetz über die Antiterrordatei den Fokus auf die inhaltliche Prüfung zu legen, also vorrangig zu prüfen, ob die betreffenden Personen rechtmäßig in der Antiterrordatei gespeichert sind. Dieser Anforderung kamen wir bei dem Landeskriminalamt Bremen nach. Die Speicherung in der Antiterrordatei war rechtmäßig. Die inhaltliche Prüfung beim Landesamt für Verfassungsschutz steht derzeit noch aus.

5.4 Prüfung der Falldatei Rauschgift

Prüfgegenstand war in diesem Berichtsjahr die Speicherung von Personen in der Falldatei Rauschgift gemäß dem Bundeskriminalamtgesetz. Die Falldatei Rauschgift ist eine

Verbunddatei, das heißt, dass die Sicherheitsbehörden der Bundesländer und des Bundes personenbezogene Daten in diese Anwendung eingeben, speichern, verändern und nutzen. In der Falldatei Rauschgift werden Personen erfasst, die beschuldigt oder verdächtigt wurden, Straftaten nach dem Arzneimittelgesetz, nach dem Betäubungsmittelgesetz, nach dem Gesetz zur Überwachung des Verkehrs mit Grundstoffen, die für die unerlaubte Herstellung von Betäubungsmitteln missbraucht werden können, und bestimmte andere Straftaten nach dem Strafgesetzbuch in Zusammenhang mit Betäubungsmitteln begangen zu haben.

Exemplarisch wählten wir uns zur stichprobenartigen Überprüfung Speicherungen unter der Rubrik "Verschaffen einer Gelegenheit" gemäß § 29 Absatz 1 Nummer 10 und Nummer 11 Betäubungsmittelgesetz zum Prüfgegenstand. Nach § 29 Absatz 1 Nummer 10 Betäubungsmittelgesetz ist strafbar, wer einem anderen eine Gelegenheit zum unbefugten Erwerb oder zur unbefugten Abgabe von Betäubungsmitteln verschafft oder gewährt, eine solche Gelegenheit öffentlich oder eigennützig mitteilt oder einen anderen zum unbefugten Verbrauch von Betäubungsmitteln verleitet. Nach § 29 Absatz 1 Nummer 11 Betäubungsmittelgesetz ist strafbar, wer ohne Erlaubnis nach dem Betäubungsmittelgesetz einem anderen eine Gelegenheit zum unbefugten Verbrauch von Betäubungsmitteln verschafft oder gewährt oder wer eine außerhalb einer Einrichtung nach dem Betäubungsmittelgesetz bestehende Gelegenheit zu einem solchen Verbrauch eigennützig oder öffentlich mitteilt.

Im Prüfgespräch wurde uns mitgeteilt, dass weder die nach dem Bundeskriminalamtgesetz erforderliche Filterung noch die Prognose vorgenommen wurden beziehungsweise werden. Nach dem Bundeskriminalamtgesetz sind nur solche Straftaten in der Falldatei Rauschgift zu erfassen, die von länderübergreifender, internationaler oder erheblicher Bedeutung sind. Außerdem dürfen Personendaten nur in die Falldatei Rauschgift eingegeben, gespeichert, verändert und genutzt werden, soweit dies erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der oder des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass Strafverfahren gegen die Beschuldigte oder den Beschuldigten oder Tatverdächtigen zu führen sind (sogenannte Negativprognose).

In der Prüfung fiel auf, dass neben der Erfassung von Bagatelldelikten bei einigen Personen die Aussonderungsprüffrist abgelaufen war, was eine Löschung in der Falldatei Rauschgift normalerweise am auf das Aussonderungsprüfdatum folgenden Tag nach sich ziehen muss. Wir bemängelten deshalb gleich vor Ort die organisatorische, manuelle Löschroutine des Landeskriminalamts. Außerdem war auffällig, dass das Aussonderungsprüfdatum bei einigen Personen die Höchstfrist von zehn Jahren nach dem Bundeskriminalamtgesetz überschritt. Dies wurde uns gegenüber damit begründet, dass andere, in dem polizeilichen Informationssystem, nicht jedoch in der Falldatei Rauschgift gespeicherte

Betäubungsmitteldelikte zu einer Verlängerung der Höchstspeicherfrist geführt hätten. An dieser Stelle wurde aus unserer Sicht folgendes verkannt: Die Speicherung eines Delikts im polizeilichen Informationssystem @rtus darf nicht zu einer Verlängerung der Speicherfrist der Person in der Falldatei Rauschgift führen, wenn das Delikt selbst nicht in der Falldatei Rauschgift erfasst wird. Außerdem unterliegen die Deliktsspeicherungen einer absoluten Höchstspeicherdauer. Einen Mitzieheffekt, wie ihn das polizeiliche Informationssystem @rtus kennt, gibt es im Verbundsystem nach dem Bundeskriminalamtgesetz nicht. Unterschiedliche Verfahren haben unterschiedliche gesetzliche Voraussetzungen und damit verschiedene datenschutzrechtliche technische und organisatorische Maßnahmen umzusetzen. Es ist Aufgabe des Landeskriminalamtes dafür zu sorgen, dass die nach dem Bundeskriminalamtgesetz anzuwendenden Verfahren entsprechend angewandt werden. Das Landeskriminalamt plant, uns ein Konzept vorzulegen, wie es insbesondere die organisatorischen Mängel in der manuellen Löschroutine abstellen und die oben genannte Filterung und Negativprognose umsetzen wird.

5.5 facebook-"Fanseiten" der Polizeien

Im 37. Jahresbericht (siehe Ziffer 11.3) berichteten wir, dass der Arbeitskreis I der Konferenz der Innenminister des Bundes und der Länder plante, Gespräche mit facebook zum Thema des Datenschutzes bei facebook-"Fanseiten" zu führen und die Konferenz der Datenschutzbeauftragten hierzu um Unterstützung gebeten hatte. Wir begleiteten die Aufnahme dieser Gespräche, die sich insbesondere mit dem datr-Cookies beschäftigten. Der datr-Cookie ist eine Datei, die facebook im Browser der Nutzerinnen und Nutzer speichert und damit Informationen über das Nutzungsverhalten auf Seiten mit dem "gefällt mir"-Button sammeln kann. Den Schlüssen, die die Innenministerkonferenz aus dem Gespräch ziehen wird, sehen wir gespannt entgegen. Wir rechnen damit, dass die Innenministerkonferenz deutlich machen wird, welche Rechtmäßigkeitsanforderungen die Anwendung "Fanseite" erfüllen muss.

Während die Anzahl der Anfragen zur Nutzung von facebook aus den Verwaltungsbereichen im vergangenen Berichtsjahr zurückging, übermittelten uns die Polizeien Bremen und Bremerhaven ihr gemeinsames Umsetzungskonzept für ihre facebook-"Fanseiten" und baten uns um eine Bewertung hinsichtlich der Kritikpunkte des Datenschutzes und der Wahrung des Rechts auf informationelle Selbstbestimmung.

In unserer Stellungnahme machten wir deutlich, dass die Polizeien eine facebook-"Fanseite" nicht datenschutzkonform betreiben können, da diese als Diensteanbieter auftreten würden und die datenschutzrechtlichen Grundsätze nach dem Telemediengesetz dabei nicht eingehalten werden könnten. Die Bindung der öffentlichen Verwaltung und damit auch der Polizeien an das Rechtsstaatsprinzip und das Prinzip der Rechtmäßigkeit der Verwaltung

führt dazu, dass Anwendungen, die nicht erwiesenermaßen rechtmäßig sind, nicht genutzt werden dürfen. Deshalb baten wir auch die Polizeien, die Ergebnisse der Gespräche zwischen facebook und der Innenministerkonferenz abzuwarten. Die per Senatsbeschluss zu diesem Thema geforderte sorgfältige Abwägung des Informationsinteresses und Veröffentlichungsinteresses mit dem Recht auf informationelle Selbstbestimmung konnten wir in dem Konzept zudem nicht erkennen. Auch vermissten wir die Beschreibung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Anforderungen des Datenschutzes, die laut § 7 Bremisches Datenschutzgesetz erforderlich sind.

Zum 1. Juni 2015 gingen die facebook-"Fanseiten" der beiden Polizeien online. Ob und wie staatliche Stellen aufgrund der Entscheidung des Europäischen Gerichtshofs in Sachen Safe Harbor ihr Vorgehen bezüglich facebook-"Fanseiten" ändern werden, bleibt im nächsten Jahr ein spannendes Thema, zumal auch der Bundesjustizminister Gespräche mit facebook führt, um darauf zu dringen, dass facebook die Pflichten aus dem Telemediengesetz umsetzt und rechtswidrige Inhalte, wie zum Beispiel Hasskommentare, unverzüglich aus dem Netzwerk entfernt.

5.6 Versendung von Radarmessungsdaten an den falschen Adressaten

Ein Petent berichtete uns, dass er in Bremerhaven von einer Radarfalle erfasst worden sei. Neben den Unterlagen zu seiner Geschwindigkeitsüberschreitung habe er von der Bußgeldstelle personenbezogene Daten einschließlich Fotos einer ihm unbekannten Bürgerin erhalten. Wir wurden gebeten, der Angelegenheit nachzugehen. Der Magistrat der Stadt Bremerhaven teilte uns auf Anfrage mit, dass der tägliche Postversand der Bußgeldstelle größtenteils maschinell erfolge. Im vorliegenden Fall habe der Petent telefonisch bei der Sachbearbeitung ein Foto als Beweismittel angefordert. Dieses Fotoprotokoll sei dann zusammen mit einem Formvordruck als Anschreiben ausgedruckt worden. Die gesamte tägliche Ausgangspost werde nach der Bearbeitung der Posteingänge kuvertiert. Der Magistrat geht davon aus, dass sich die beiden Schreiben an den Heftklammern miteinander verhakt hätten und dann in einem Umschlag an den Petenten versandt worden seien. Uns wurde zugesagt, dass man sich bemühen werde, derartige Fehler zukünftig auszuschließen. Da uns bisher keine ähnlichen Versehen bekannt geworden sind, haben wir auf weitere Maßnahmen verzichtet.

5.7 Datenweitergabe an die Tochter durch die Kfz-Zulassungsstelle

Eine Petentin berichtete uns, dass ihre Tochter ihr Kraftfahrzeug veräußern wollte. Da sie sich mitten in einem Umzug befunden habe, sei ihr kein Zugriff auf den Fahrzeugschein möglich gewesen. Von der Zulassungsstelle sei ihr deshalb vorgeschlagen worden, Ersatzpapiere zu beantragen. Eine neue Adresse habe sie zu dem Zeitpunkt noch nicht

gehabt. Deshalb sei sie nach Verwandten gefragt worden, an die die Unterlagen gesendet werden könnten. Daraufhin habe die Tochter ihre Mutter erwähnt, habe aber deren Adresse nicht angeben können. Die Behördenmitarbeiterin habe deshalb die Daten der Petentin im Computer recherchiert, ausgedruckt und der Tochter zur Unterschrift vorgelegt.

Wir baten die Zulassungsstelle dazu um Stellungnahme. Von dort wurde uns mitgeteilt, dass der Tochter bei der Bearbeitung ihres Anliegens ein Auszug aus dem Melderegister zur kurzen Einsichtnahme zur Verfügung gestellt worden sei. Eine Rechtsgrundlage bestehe dafür nicht. Der Auszug habe die benötigten Meldedaten der Petentin enthalten. Weitere Daten wie Einzugsdaten und Auszugsdaten seien daraus nicht hervorgegangen. Man habe der Kundin eine Lösung anbieten wollen, damit diese ihr Anliegen zügig und ohne weiteren Aufwand abschließend erledigen könne. Die datenschutzrechtlichen Vorschriften seien dabei vernachlässigt worden. Die entsprechende Sachbearbeiterin sei von der Behördenleitung noch einmal ausführlich über die datenschutzrechtlichen Bestimmungen belehrt worden. Zudem sei der Vorfall zum Anlass genommen worden, dass Thema Datenschutz in den kommenden Dienstbesprechungen nochmals aufzugreifen und die Mitarbeiterinnen und Mitarbeiter erneut für die Thematik zu sensibilisieren.

5.8 Erhebung von personenbezogenen Daten durch Fischereiaufseher

Ein Angler wandte sich mit der Frage an uns, ob Fischereiaufseher, sofern es nichts zu beanstanden gebe, seine personenbezogenen Daten erheben dürften. Er sei Mitglied einer Pachtgemeinschaft, die aus mehreren Vereinen bestehe. Alle darin organisierten Anglerinnen und Angler dürften in der Weser angeln und würden von den zuständigen Fischereiaufsehern kontrolliert. Wir teilten dem Petenten mit, dass das Bremische Fischereigesetz es der Fischereibehörde erlaubt, ehrenamtliche Fischereiaufseher zu bestellen, soweit es zur Wahrnehmung der Fischereiaufsicht erforderlich ist. Die Kontrolleurinnen und Kontrolleure dürfen von den bei der Fischerei angetroffenen Personen jederzeit verlangen, die Personalien anzugeben und den Fischereischein sowie den Fischereierlaubnisschein vorzuweisen. Das Notieren der Personalien, also das Speichern, ist nicht explizit im Gesetz geregelt. Insofern vertreten wir die Auffassung, dass die Personalien nach dem Grundsatz der Datensparsamkeit nur dann gespeichert werden dürfen, wenn dies zur Aufgabenerfüllung der Fischereiaufseher erforderlich ist. Sofern keine Beanstandungen vorliegen, ist für uns kein Grund ersichtlich, der eine Datenspeicherung erfordern würde. Insofern halten wir in diesen Fällen das Notieren der Daten für unzulässig.

5.9 Wahlen in Bremen

Auch hinsichtlich der Wahl der Bremischen Bürgerschaft im Jahr 2015 wurden einige datenschutzrechtliche Fragen an uns herangetragen. So sorgten sich Bürgerinnen und

Bürger darüber, dass im Wahllokal ihre Namen auf einer Liste abgehakt und die Wahlbenachrichtigungskarten einbehalten wurden. Sie wollten wissen, was mit den Daten passiert. Wir teilten den Anfragenden mit, dass die Bremische Landeswahlordnung die Kennzeichnung der Personen im Wählerverzeichnis, die gewählt haben, zwingend vorsieht. Insofern bestehen dagegen keine datenschutzrechtlichen Bedenken. Nach den Vorschriften der Bremischen Landeswahlordnung sind die Wählerverzeichnisse so zu verwahren, dass sie gegen Einsichtnahme durch Unbefugte geschützt sind. Auskünfte daraus dürfen nur Behörden, Gerichten und sonstigen amtlichen Stellen innerhalb des Landes erteilt werden. Weitere Voraussetzung ist, dass die Auskünfte für den Empfänger im Zusammenhang mit der Wahl erforderlich sind. Ein solcher Anlass liegt insbesondere beim Verdacht von Wahlstraftaten, bei Wahlprüfungsangelegenheiten und bei wahltaktischen Arbeiten vor. Die Bremische Landeswahlordnung schreibt zudem vor, dass einbehaltene Wahlbenachrichtigungen unverzüglich zu vernichten sind. Wählerverzeichnisse, Wahlscheinverzeichnisse, weitere Verzeichnisse und Formblätter sind nach Ablauf von sechs Monaten nach der Wahl zu vernichten, wenn nicht die Landeswahlleitung mit Rücksicht auf ein schwebendes Wahlprüfungsverfahren etwas anderes anordnet oder sie für die Strafverfolgungsbehörde zur Ermittlung einer Wahlstraftat von Bedeutung sein können. Die übrigen Wahlunterlagen können 60 Tage vor der Neuwahl vernichtet werden, soweit sie nicht für ein schwebendes Wahlprüfungsverfahren oder für die Strafverfolgungsbehörde zur Ermittlung einer Wahlstraftat von Bedeutung sein können.

Aus der Bürgerschaft wurde an das Wahlamt der Wunsch gerichtet, zusätzlich zu den bereits bestehenden Wahlmöglichkeiten der unmittelbaren Wahl am Wahlsonntag und der Briefwahl auch noch in einigen Einkaufszentren für den Zeitraum von zwei Wochen vor der Wahl die Möglichkeit der Stimmabgabe zu schaffen. Hierzu bat uns das Wahlamt um Stellungnahme. In diesem Zusammenhang ist zu beachten, dass ohne Verletzung datenschutzrechtlicher Grundsätze bei der Ausgabe der Wahlunterlagen sichergestellt werden muss, dass nicht Unberechtigte wählen oder mehrfach gewählt wird. In einem Termin legte uns das Wahlamt die bisherigen Überlegungen zur technischen Umsetzung dar. Letztlich wurde das Vorhaben im Rahmen der Bürgerschaftswahl im Jahr 2015 nicht weiter verfolgt. Es ist aber durchaus denkbar, dass das Projekt für spätere Wahlen wieder aufgegriffen wird.

5.10 Behördlicher Datenschutzbeauftragter und Verfahren im Stadtamt

In der Vergangenheit berichteten wir über die Situation im Stadtamt (vergleiche 34. Jahresbericht, Ziffer 5.11, 35. Jahresbericht, Ziffer 5.5 und 36. Jahresbericht, Ziffer 5.6). Nachdem wir in den jeweiligen Berichtsteilen bemängelten, dass keine behördliche Datenschutzbeauftragte beziehungsweise kein behördlicher Datenschutzbeauftragter vom Stadtamt bestellt worden war, hat dieses mittlerweile einen solchen bestellt. In der Zeit ohne Beauftragte oder Beauftragten und während der im Stadtamt stattfindenden umfassenden

Reorganisationsprozesse wurden die bis dahin nicht bewertbaren Datenschutzkonzepte nach unserem Wissen nicht weiterentwickelt, sodass, auch dies berichteten wir, weiterhin eine große Anzahl von Verfahren mit denen teilweise sensible Daten verarbeitet werden, ohne ausreichende Datenschutzkonzepte, und nicht bewertbare technische und organisatorische Maßnahmen im Echtbetrieb sind.

Wie mit dem Stadtamt besprochen, sollen im nächsten Berichtsjahr wieder regelmäßige Gespräche zwischen uns und dem Datenschutzbeauftragten des Stadtamts stattfinden. Wir gehen davon aus, dass den zuständigen Stellen im Stadtamt ausreichende Kapazitäten zur Erstellung der erforderlichen Verfahrensbeschreibungen zur Verfügung gestellt werden.

5.11 Zuverlässigkeitsprüfung der Gewerbebehörde bei Bewachungspersonal

Die Gewerbeordnung und die ausführende Bewachungsverordnung schreiben mit gutem Grund vor, dass Bewachungsaufgaben lediglich von Personen übernommen werden dürfen, welche die hierfür erforderliche Zuverlässigkeit besitzen. Daher müssen sich Personen, welche im Bewachungsgewerbe tätig werden wollen, vor ihrer Tätigkeitsaufnahme durch die zuständige Gewerbebehörde auf ihre Zuverlässigkeit hin überprüfen lassen. Damit die Gewerbebehörde alle für die Zuverlässigkeitsüberprüfung notwendigen Informationen zu der (potentiellen) Wachperson zusammentragen und sich so ein Bild von ihrer Zuverlässigkeit oder gegebenenfalls Unzuverlässigkeit machen kann, hat der Gesetzgeber eine Reihe von Datenerhebungsbefugnissen für die Gewerbebehörde normiert. Soweit hierbei Spielräume belassen sind, kann es eine schwierige Gratwanderung sein, zwischen einerseits tiefgehendem Informationsbedarf zur Person zwecks Zuverlässigkeitsbeurteilung und andererseits geschuldetem Respekt der Privatsphäre und Nichtausforschung sämtlicher Lebensumstände.

Unter anderem durch einen Pressebericht sowie eine stadtparlamentarische Drucksache wurden wir im Herbst 2014 auf eine Datenerhebungspraxis der Gewerbebehörde bei der Überprüfung der Zuverlässigkeit von (potentiellem) Bewachungspersonal aufmerksam, die aus unserer Sicht in mehrerlei Hinsicht datenschutzrechtliche Bedenken aufwarf. So stellten wir beispielsweise fest, dass die Gewerbebehörde trotz der bereits durch das Gesetz eingeräumten Datenerhebungsbefugnisse von den potentiellen Wachleuten stets eine Einwilligung in die Zuverlässigkeitsprüfung und die Erhebung von Daten einholte. Da zugleich feststand, dass bei einer Verweigerung der Einwilligungsabgabe letztlich keine Beschäftigung als Wachperson zugelassen würde, waren die Bewerber letztlich zu einer Einwilligung gezwungen. Dies stand in offenkundigem Widerspruch zu der Rechtsvorgabe, dass Einwilligungen freiwillig erteilt sein müssen, nur rechtswirksam sind, wenn eine tatsächlich freie Entscheidung der oder des von der Datenerhebung Betroffenen vorliegt.

Zudem kann eine Behörde nicht ihre durch den Gesetzgeber eingeräumten Handlungsbefugnisse, hier also ihre gesetzlichen Datenerhebungsbefugnisse – welche implizit auch Datenerhebungsgrenzen ziehen – einfach durch ein Ausweichen (Einwilligung) umgehen.

Wir wandten uns daher an die Gewerbebehörde und legten ausführlich die datenschutzrechtlichen und zugleich auch staatsrechtlichen Bedenken gegenüber der Einwilligungseinholung dar. Zugleich benannten wir einige sonstige aus unserer Sicht klärungsbedürftigen Fragen zur Datenerhebungspraxis. Trotz mehrfacher Erinnerung an eine Stellungnahme zu unserem Schreiben erfolgte keinerlei Reaktion der Gewerbebehörde. Erst als wir schließlich eine förmliche Beanstandung wegen Verletzung unserer Untersuchungsbefugnisse androhten, ging im Herbst des Berichtsjahres, also fast ein Jahr nach unserem Anschreiben eine Stellungnahme ein. Uns wurde zugesagt, das Einwilligungsmodell bei der Zuverlässigkeitsprüfung nicht fortzuführen. Dies begrüßen wir ausdrücklich. Hinsichtlich der weiteren im Raum stehenden datenschutzrechtlichen Aspekte bei der Zuverlässigkeitsprüfung konnten wir die Prüfung im Berichtsjahr noch nicht abschließen. Wir werden gegebenenfalls im nächsten Jahresbericht über den Verfahrensabschluss und die Ergebnisse berichten.

5.12 Namensverwechselung beim Stadtamt

In diesem Berichtsjahr erhielten wir eine Beschwerde einer Bürgerin, die aufgrund einer Namensverwechselung mit einer Klage überzogen wurde, die sie fälschlicherweise als Beklagte nannte. Hier stellte sich das Problem, dass das Gericht die "falsche" Beklagte vom Rechtsanwalt benannt bekommen hatte und diese aufgrund des zivilrechtlichen Beibringungsgrundsatzes um erneute Prüfung bat. Der Rechtsanwalt hatte zuvor eine erweiterte Melderegisterauskunft beim Stadtamt beantragt, indem er sich nach der aktuellen Adresse der Beklagten unter Nennung des Namens und der alten Adresse erkundigte. Ein Geburtsdatum wurde seitens der Rechtsanwaltskanzlei bei der Anfrage an das Stadtamt Bremen nicht übermittelt.

Auf Nachfrage beim Stadtamt erhielten wir die Auskunft, dass es sich um einen Fehler gehandelt habe. Wie dieser Fehler entstanden sei, konnte dort nicht mehr ermittelt werden. Datenschutzrechtlich interessant ist an diesem Fall, dass das Gericht an eine dritte Person, nämlich die "falsche" Beklagte, personenbezogene Daten aus der Klageschrift über die "richtige" Beklagte offenbarte. In diesem Kontext stellten wir fest, dass für solche Fälle einer Namensverwechselung durch öffentliche Stellen eine Unterrichtung der oder des Betroffenen über die Weitergabe personenbezogener Daten gesetzlich nicht verankert ist. Diese Feststellung betrifft alle öffentlichen Stellen in der Freien Hansestadt Bremen, die das

Bremische Datenschutzgesetz anwenden. Aus unserer Sicht sollte eine solche Unterrichtungsverpflichtung in das Bremische Datenschutzgesetz aufgenommen werden.

6. Justiz

6.1 Auskunftsersuchen des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe

Der Europarat errichtete im Jahre 1987 einen Europäischen Ausschuss zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (im Folgenden Ausschuss), der durch Besuche unter anderem in Deutschland die Behandlung von Personen prüft, denen die Freiheit entzogen ist, um erforderlichenfalls den Schutz dieser Personen vor Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe zu verbessern (Artikel 1 des Europäischen Übereinkommens zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe).

Gegenstand unserer Prüfung war die Frage des Einsichtsrechts des Ausschusses in die Personalakten und Patientenakten von Gefangenen. Unsere datenschutzrechtliche Bewertung ergab, dass der Ausschuss Einsichtsrechte in die Personalakten von Gefangenen nach dem Bremischen Datenschutzgesetz hat, während ein Einsichtsrecht des Ausschusses in die Patientenakten von Gefangenen nicht besteht, sofern diese nicht einwilligen. Dieser Unterschied in der datenschutzrechtlichen Bewertung von Personalakte und Patientenakte liegt im Bremischen Datenschutzgesetz begründet, welches Gesundheitsdaten als besondere Arten von personenbezogenen Daten besonders schützt. Durch die zwischenzeitlich in Kraft getretene Änderung des Bremischen Strafvollzugsgesetzes wurde das von der Einwilligung der Gefangenen unabhängige Akteneinsichtsrecht des Ausschusses auch für Patientenakten von Gefangenen im Erwachsenenstrafvollzug geschaffen.

6.2 IT-Verfahren bei der Staatsanwaltschaft

Das IT-Verfahren "web.sta" bei der Staatsanwaltschaft Bremen unterstützt deren Arbeit bei der Registrierung und Verwaltung von Akten sowie bei der Schriftguterstellung. Mit "web.sta" steht ein Informationssystem zur Verfügung, das neben der gerichtlichen Terminierung den Stand des Ermittlungsverfahrens und der Vollstreckung wiedergibt. Das Automationsverfahren "web.sta" wird in einem Verbund von den Bundesländern Baden-Württemberg, Bayern, Bremen, Niedersachsen, Rheinland-Pfalz, Saarland, Sachsen, Thüringen und Sachsen-Anhalt betrieben. Auf "web.sta" können derzeit rund 180 Mitarbeiterinnen und Mitarbeiter der Staatsanwaltschaft Bremen lesend zugreifen.

In diesem Berichtsjahr führten wir anlässlich des Umstandes, dass in den anderen Bundesländern Berlin, Brandenburg, Hamburg, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen und Schleswig-Holstein die Anforderung einer Protokollierung lesender Zugriffe auf "MeStA" (Mehrländer-Staatsanwaltschafts-Automation) umgesetzt worden war, ein Gespräch mit dem leitenden Oberstaatsanwalt über die in Bremen bisher fehlende Protokollierung lesender Zugriffe auf "web.sta". "MeStA" und "web.sta" sind die führenden staatsanwaltschaftlichen Informationssysteme in der Bundesrepublik Deutschland. Ob eine Protokollierung lesender Zugriffe auf "web.sta" umgesetzt werden kann, wird derzeit geprüft. Die Staatsanwaltschaft Bremen erarbeitet gerade die Verfahrensbeschreibung für "web.sta" nach dem Bremischen Datenschutzgesetz, die uns dann zur Stellungnahme vorgelegt werden kann.

6.3 Veröffentlichung personenbezogener Daten durch Gerichte

Gemäß § 1 Absatz 4 Satz 1 Bremisches Datenschutzgesetz (BremDSG) unterliegen Gerichte nur insoweit unserer datenschutzrechtlichen Kontrollbefugnis, als sie Verwaltungsaufgaben erledigen und gemäß § 27 Absatz 1 Satz 2 BremDSG darüber hinaus beim Einsatz automatisierter Datenverarbeitung hinsichtlich der organisatorischen und technischen Maßnahmen der Datensicherung – unbeschadet der verfassungsrechtlich gewährleisteten Unabhängigkeit. Häufig beschweren sich Bürgerinnen und Bürger bei uns hinsichtlich des Datenumgangs in laufenden Gerichtsverfahren. Wir weisen dann die Bürgerinnen und Bürger auf unsere eingeschränkte Kontrollbefugnis gegenüber den Gerichten hin und führen aus, dass wir angesichts dieser richterlichen Unabhängigkeit in laufenden Gerichtsverfahren nicht tätig werden. Anders verhält es sich bei abgeschlossenen Gerichtsverfahren, also bei gerichtlichen Entscheidungen, die rechtskräftig sind.

Die Veröffentlichung rechtskräftiger Entscheidungen durch die Gerichte beschäftigte uns in diesem Berichtsjahr. Grundsätzlich werden rechtskräftige Entscheidungen nur in anonymer Form veröffentlicht. Unter Anonymisieren wird gemäß § 2 Absatz 4 BremDSG das Verändern personenbezogener Daten derart verstanden, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. In dem konkreten Fall stellte sich die Frage, ob die Zuordnung zu einem Beruf ein personenbezogenes Datum darstellt. Wir bejahten diese Frage in diesem Fall, da es sich bei dem diesen Beruf ausübenden Personenkreis um eine relativ kleine Berufsgruppe handelte und gemäß § 1 Absatz 1 BremDSG diese Einzelangabe über das Berufsverhältnis einer bestimmbaren natürlichen Person zugeordnet werden konnte. Die Zugehörigkeit zur Berufsgruppe musste beispielsweise auch durch das Schwärzen beziehungsweise Streichen der berufsspezifischen Altersversorgung in der Veröffentlichung

der gerichtlichen Entscheidung ausgeschlossen werden. Das verantwortliche Gericht teilte unsere Rechtsauffassung.

7. Gesundheit

7.1 Austausch sensibler Gesundheitsdaten zwischen Ärztin, Krankenkasse und kassenärztlicher Vereinigung

Ein Ehepaar aus Niedersachsen erlebte bei einem Hausarztbesuch in Bremen Folgendes: Trotz bereits circa zehnjähriger Behandlungsdauer und Vorlage von gültigen Gesundheitskarten wurde aufgrund eines mehrmonatigen Auslandsaufenthaltes der beiden von der Arztpraxis das Bestehen eines gültigen Versicherungsschutzes angezweifelt. Von Seiten der Praxis war deshalb diesbezüglich eine telefonische Anfrage bei der Krankenkasse erfolgt. Die Krankenkasse verneinte zunächst fälschlicherweise eine Versicherteneigenschaft der Beiden, woraufhin die Betroffenen der Praxis verwiesen wurden. Das Missverständnis konnte später von den Betroffenen aufgeklärt werden.

Die Nachfrage über den bestehenden Versicherungsschutz bei der Krankenkasse war im vorliegenden Fall nicht erforderlich und damit nicht zulässig, da gültige Versichertenkarten vorgelegt worden waren. Die Vorlage der Krankenversichertenkarte ist zum Nachweis des Versicherungsschutzes nach dem Sozialgesetzbuch V ausreichend. Bei Beendigung des Versicherungsschutzes oder bei einem Krankenkassenwechsel hätte die Karte von der bisherigen Krankenkasse eingezogen werden müssen. Damit lag für die Betroffenen also jeweils ein Nachweis eines bestehenden Krankenversicherungsschutzes bei der Krankenkasse vor. Die Ärztin sicherte uns zu, dies in Zukunft zu berücksichtigen und von entsprechenden Anfragen an Krankenkassen abzusehen.

Die Betroffenen wandten sich aufgrund der geschilderten Ereignisse darüber hinaus an die Krankenkasse, um sich über das Verhalten der Ärztin zu beschweren. Zum Zweck der Bearbeitung der Beschwerde unterzeichnete der Ehemann eine Erklärung, wonach die Ärztin gegenüber der Krankenkasse und der Kassenärztliche Vereinigung Niedersachsen von ihrer Schweigepflicht entbunden wurde. Die Krankenkasse wandte sich zur Klärung der Beschwerde an die Kassenärztliche Vereinigung Niedersachsen, die für die Hausarztpraxis in Bremen jedoch nicht zuständig ist. Im Folgenden gab die Hausärztin zum Zweck der Bearbeitung der Beschwerde sehr sensible Gesundheitsdaten an die Kassenärztliche Vereinigung Bremen und die Krankenkasse weiter. Es folgte ein reger Austausch der Unterlagen zu diesem Vorfall zwischen den drei Stellen, zum Teil in unverschlüsselter Form per E-Mail. In diesem Zusammenhang baten die Betroffenen die Kassenärztliche Vereinigung Bremen mehrfach um Information, welche Daten diese an welche Stellen weitergegeben hätten, erhielten dazu jedoch keine Auskunft.

Wir fragten die Ärztin und die Kassenärztliche Vereinigung Bremen nach den Rechtsgrundlagen für den Datenaustausch im Rahmen der Bearbeitung der Beschwerde. Von beiden Stellen wurde uns daraufhin mitgeteilt, dass eine Schweigepflichtentbindungserklärung der Betroffenen vorliege. Da uns von den Betroffenen mitgeteilt worden war, dass lediglich der Ehemann eine Schweigepflichtentbindungserklärung für die Ärztin gegenüber der Kassenärztlichen Vereinigung Niedersachsen und der Krankenkasse erteilt habe, baten wir die Ärztin und die Kassenärztliche Vereinigung Bremen um Übersendung von Ablichtungen der Schweigepflichtentbindungserklärungen der beiden Betroffenen.

Die Ärztin übersandte die Kopie eines Dokuments, aus dem hervorgeht, dass der Ehemann die Hausarztpraxis auch gegenüber der Kassenärztlichen Vereinigung Bremen von der Schweigepflicht entbunden habe. Auf unsere Nachfrage erklärte der Betroffene er habe eine solche Erklärung niemals abgegeben. Er erstattete Strafanzeige gegen die Hausärztin. Eine Einwilligungserklärung der Ehefrau legte die Ärztin nicht vor. Sofern es keine solche Erklärung gibt, war die Weitergabe der Daten der Ehefrau an die Kassenärztliche Vereinigung Bremen unzulässig. Aufgrund der Strafanzeige haben wir die Bearbeitung in Bezug auf diesen Aspekt vorläufig zurückgestellt.

Die Kassenärztliche Vereinigung Bremen legte ebenfalls keine Einwilligungserklärungen der beiden Ehepartner in die Verarbeitung ihrer Sozialdaten zum Zweck der Bearbeitung der Beschwerde vor. Sofern keine solchen Erklärungen vorlagen, war die Weitergabe der Daten an die Krankenkasse daher unzulässig. Dies teilten wir der Kassenärztlichen Vereinigung Bremen mit und baten um Berücksichtigung für die Zukunft. Eine Antwort steht noch aus. Zu der Frage, aus welchem Grund den Betroffenen die Auskunft über Art und Umfang des Datenaustauschs verweigert wurde, nahm die Kassenärztliche Vereinigung Bremen nicht Stellung. Sie wurde von uns auf die Verpflichtung zur Prüfung der gesetzlichen Auskunftsrechte und Einsichtsrechte hingewiesen.

Zusätzlich wiesen wir die Hausärztin und die Kassenärztliche Vereinigung Bremen darauf hin, dass die Übermittlung von personenbezogenen Daten in unverschlüsselter Form per E-Mail nicht zulässig ist. Nach den datenschutzrechtlichen Vorschriften sind bei der Verarbeitung oder Nutzung von personenbezogenen Daten die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die gesetzlichen Datenschutzregelungen zu gewährleisten. Bei der Weitergabe von personenbezogenen Daten muss gewährleistet sein, dass diese bei der elektronischen Übertragung oder während des Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Weitergabekontrolle), was bei der elektronischen Übertragung von personenbezogenen Daten per unverschlüsselter E-Mail nicht möglich ist, da eine Kenntnisnahme von unbefugten Dritten bei einer solchen Weitergabe nicht ausgeschlossen

werden kann. Wir baten die beiden Stellen darum, in Zukunft auf eine Versendung von personenbezogenen Daten in unverschlüsselter Form per E-Mail zu verzichten. Dies wurde sowohl von der Hausärztin also auch von der Kassenärztlichen Vereinigung Bremen zugesichert.

7.2 Anforderung von Einkommensnachweisen durch die Krankenkasse

Im Dezember 2014 wandte sich ein Bürger an uns, der als Beamter bei einer Bremer Krankenkasse freiwillig versichert ist. Er war von der Krankenkasse aufgefordert worden, einen Fragebogen zur Einkommenssituation auszufüllen und einen Einkommensnachweis, in jedem Fall aber die Bezügemitteilung für Dezember 2014, zu übersenden. Der Betroffene wandte sich gegen die Anforderdung des Einkommensnachweises durch die Krankenkasse, da er mit seinem Einkommen über der Beitragsbemessungsgrenze lag und aufgrund dessen bereits mit dem Höchstsatz veranschlagt wurde. Dies hatte er der Krankenkasse auch bereits mitgeteilt, die zunächst jedoch von der Anforderung der Bezügemitteilung für Dezember 2014 nicht absehen wollte, da in bestimmten Einzelfällen, nämlich wenn zusätzlich Rentenbezüge oder Versorgungsbezüge bestehen, zusätzliche Informationen aus der Bezügemitteilung für die Beitragsfestsetzung erforderlich sein könnten. Später räumte die Krankenkasse ein, dass diese pauschale Anforderung von Einkommensnachweisen datenschutzrechtlich unzulässig ist.

Die Erhebung von Einkommensdaten zum Zweck der Beitragsfestsetzung bei freiwillig versicherten Mitgliedern gesetzlicher Krankenkassen war bereits mehrfach Thema der Beratung der Datenschutzbeauftragten des Bundes und der Länder. Dabei bestand Einigkeit, dass Unterlagen zum Nachweis von Einkommen nur im erforderlichen Fall angefordert werden dürfen und dass die Versicherten in den Dokumenten die nicht notwendigen Daten schwärzen dürfen. Zu diesem Zweck ist es erforderlich, dass die Versicherten von Seiten der Krankenkasse bereits im Anforderungsschreiben unmissverständlich darüber informiert werden, in welchen Fällen die Übermittlung welcher Unterlagen zum Einkommen erforderlich ist und welche Daten darin geschwärzt werden dürfen (zum Beispiel Daten des Ehepartners, Steuerschuld).

Wir wandten uns an die Krankenkasse und baten um Umsetzung der datenschutzrechtlichen Anforderungen, was uns von der Krankenkasse auch bereits im Januar des Berichtsjahres zugesagt wurde. Die Krankenkasse übersandte uns neu gestaltete Formulare, die den Hinweis enthielten, dass bei einem Einkommen über der Beitragsbemessungsgrenze weitere Informationen und Nachweise nur erforderlich sind, wenn die beziehungsweise der Betroffene Rentenbezüge oder Versorgungsbezüge erhält. Die Unterlagen enthielten ebenfalls einen Hinweis auf die Möglichkeit zur Schwärzung der nicht erforderlichen Daten.

Bereits im Februar des Berichtsjahres meldete sich der Betroffene jedoch erneut bei uns und teilte mit, dass die Krankenkasse sich bei ihm in einem Informationsschreiben über die Beiträge der Krankenversicherung und Pflegeversicherung im Jahr 2015 für die Übersendung der Einkommensnachweise bedankte, die in seinem Fall bekanntlich nicht erforderlich war und auch nicht erfolgt ist. Zudem enthielt dieses Schreiben die Bitte, jede Änderung der Einnahmen umgehend unter Beifügung entsprechender Nachweise mitzuteilen und auch stets unmittelbar nach Erhalt den aktuellen Einkommenssteuerbescheid in Kopie zuzusenden. Ein Hinweis auf die Sachverhalte, in denen dies zum Zweck der Berechnung der Beiträge nicht erforderlich ist, und daher durch die Krankenkasse keine entsprechende Erhebung zulässig ist, erfolgte in diesem Schreiben nicht. Ebenfalls erfolgte kein Hinweis auf die Möglichkeit zur Schwärzung der zum Zweck der Beitragsberechnung nicht erforderlichen Daten.

Wir wandten uns daher erneut an die Krankenkasse und baten darum, alle Standardbriefe an freiwillig versicherte Mitglieder den datenschutzrechtlichen Anforderungen entsprechend umzugestalten.

Im Mai des Berichtsjahres erreichte uns dann ein Schreiben der Krankenkasse, in dem diese die neugefassten Unterlagen mit den geforderten Änderungen übersandte.

7.3 Verarbeitung von Patientendaten in einer kardiologischen Partnerschaftsgesellschaft

Im August 2014 wandte sich eine Patientin an uns, die in einer kardiologischen Arztpraxis, in der sie seit fast zwanzig Jahren behandelt wurde, kürzlich zur Abgabe einer datenschutzrechtlichen Einwilligungserklärung aufgefordert worden war. Inhalt dieser Erklärung war unter anderem die Erlaubnis des Zugriffs aller Mitarbeiterinnen und Mitarbeiter von allen vier Standorten der kardiologischen Partnerschaftsgesellschaft auf die Patientendaten der Betroffenen. Als die Betroffene die Abgabe dieser Einwilligung verweigerte, wurde ihr mitgeteilt, dass sie unter diesen Umständen nicht länger in der Praxis behandelt werden könnte.

Unsererseits bestanden erhebliche Bedenken im Hinblick auf die Erforderlichkeit einer derart umfassenden Ausgestaltung der Zugriffe auf die Patientendaten der Betroffenen. Zudem ergab unsere datenschutzrechtliche Prüfung des für die Einholung der Einwilligungserklärung und Schweigepflichtentbindungserklärung verwendeten Formulars, dass dieses nicht den gesetzlichen Wirksamkeitsanforderungen für eine datenschutzrechtliche Einwilligungserklärung im Bundesdatenschutzgesetz entsprach. Danach ist die Erklärung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen

der Verweigerung der Einwilligung hinzuweisen. Konkret fehlte es hier bereits an einer ausreichenden Erläuterung von Zweck und Umfang der Datenverarbeitung. Wir forderten die betroffene Praxis auf, uns die Erforderlichkeit von derart umfassenden Zugriffsmöglichkeiten in allen vier Standorten der Partnerschaftsgesellschaft zu erläutern und mitzuteilen, warum es erforderlich ist, die Behandlung von Patienten abzulehnen, die die Abgabe einer entsprechenden Einwilligungserklärung und Schweigepflichtentbindung ablehnen.

Daraufhin teilte uns die Praxis mit, dass sie die Weiterbehandlung der Betroffenen ablehne, da das Vertrauensverhältnis mit ihr nach mehreren Auseinandersetzungen nicht mehr gegeben sei. Zu unseren weiteren Fragen nahm die Praxis nicht Stellung.

Auf unseren Hinweis, dass eine Beendigung der Behandlung der Betroffenen sie nicht von der Pflicht zur Beantwortung unserer Fragen entbindet, meldete sich die Praxis erneut und teilte mit, dass sie die Einwilligung ihrer Patienten in die Datenverarbeitung mit ihrer Praxissoftware benötige, um ihre ärztlichen Pflichten im Zusammenhang mit dem Behandlungsvertrag zu erfüllen. Ein Zugriff auf die Patientendaten sei von allen Standorten der Partnerschaftsgesellschaft notwendig.

Wir wiesen darauf hin, dass nach dem Wortlaut des von der Praxis verwendeten Formulars eine Einwilligung in die Datenverarbeitung mit der standortübergreifenden Praxissoftware gar nicht Gegenstand der Einwilligungserklärung ist. Laut Formular sollen sich die Patienten damit einverstanden erklären, dass ihre Daten praxisintern allen Mitarbeitern der Praxis offengelegt werden, sofern dies zur Behandlung erforderlich ist. Da dieser Passus offensichtlich missverständlich und überdies auch zu unbestimmt ist, würden die Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligungserklärung im Bundesdatenschutzgesetz nicht erfüllt. Wir wiesen darauf hin, dass das Formular daher bereits einer Überarbeitung bedurfte. Darüber hinaus sei jedoch zu beachten, dass es einer Einwilligungserklärung und Schweigepflichtentbindungserklärung der Patienten nur in den Fällen bedarf, in denen für die Datenverarbeitung nicht bereits eine gesetzliche Rechtsgrundlage existiert. Da es für die Dokumentation der ärztlichen Behandlung eine gesetzliche Verpflichtung im Bürgerlichen Gesetzbuch und im Bundesdatenschutzgesetz gibt, ist die elektronische Verarbeitung von Patientendaten in einem Arztverwaltungssystem gesetzlich zulässig. Wir wiesen darauf hin, dass es einer Einwilligungserklärung und Schweigepflichtentbindungserklärung der Patienten jedoch gegebenenfalls für die Übermittlung von Patientendaten an andere Ärzte der Partnerschaftsgesellschaft bedarf. Eine solche Erklärung muss jedoch hinreichend konkret formuliert sein und sich zudem am Grundsatz der Erforderlichkeit orientieren. Demnach wird es nicht zulässig sein, den Patienten zu Beginn der Behandlung pauschal eine Einwilligung abzufordern, die die Übermittlung aller ihrer Daten an alle Ärzte und medizinischen Fachangestellten der vier Standorte der kardiologischen Partnerschaftsgesellschaft erlaubt. Die ärztliche

Schweigepflicht sei auch innerhalb einer Partnerschaftsgesellschaft zu wahren und darf nicht durch Einholung einer umfassenden Einwilligungserklärung und Schweigepflichtentbindungserklärung umgangen werden, ohne dass dies praktisch erforderlich ist. Für die Prüfung der Erforderlichkeit einzelner Zugriffe baten wir um Übersendung einer Verfahrensbeschreibung und einer Darstellung der Zugriffsberechtigungen einschließlich einer Erläuterung der Zwecke für die Zugriffe auf das Praxisverwaltungssystem.

Dazu wurde von der Praxis mitgeteilt, dass es sich bei der Partnerschaftsgesellschaft insgesamt um eine Gemeinschaftspraxis handelt, die verpflichtet sei, gegenüber der Kassenärztlichen Vereinigung eine gemeinsame Abrechnung abzugeben. Dafür sei eine Zusammenführung der Daten aller vier Standorte erforderlich. Das Einwilligungsformular sei zwischenzeitlich überarbeitet worden. Unserer Aufforderung nach Übersendung der Verfahrensbeschreibung und der Darstellung der Zugriffsberechtigungen kam die Praxis jedoch nicht nach.

Wir forderten die Praxis im Mai 2015 daher erneut auf, uns die angeforderten Dokumente sowie das überarbeitete Formular der Einwilligungserklärung und Schweigepflichtentbindungserklärung zum Zweck unserer datenschutzrechtlichen Prüfung zu übersenden und mitzuteilen, ob es zutrifft, dass im Praxisverwaltungssystem derzeit keinerlei Zugriffsbeschränkungen eingerichtet sind, somit also jeder Mitarbeiter Zugriff auf alle im Verfahren gespeicherten Patientendaten hat.

Als diese Anforderungen auch im Juli 2015 noch nicht erfüllt waren, setzten wir der Praxis eine Frist. Daraufhin meldete sich ein Anwalt für die Praxis und stellte eine umfassende Beantwortung in Aussicht, die jedoch bis November 2015 nicht erfolgte, sodass ein Zwangsmittelverfahren eingeleitet werden musste.

7.4 Änderung des Bremischen Krankenhausdatenschutzgesetzes

Die Senatorin für Gesundheit teilte uns mit, dass eine Novellierung des Bremischen Krankenhausdatenschutzes in dem Sinne beabsichtigt sei, dass dieses Gesetz außer Kraft gesetzt und Regelungen zum Datenschutz in Krankenhäusern in das Bremische Krankenhausgesetz integriert werden sollen. Ein entsprechender Entwurf wurde uns mit der Bitte um Stellungnahme übersandt. Begründet wurde dieses Vorhaben damit, dass das bestehende Gesetz die aktuelle Situation in den Krankenhäusern nicht mehr abbilde. Die Behandlungsstrukturen hätten sich in den letzten zehn Jahren drastisch verändert und es seien neue Versorgungsformen entstanden. Die Krankenhäuser seien nicht mehr nur auf die stationäre Behandlung ausgerichtet. Immer mehr Patientinnen und Patienten würden ambulant oder teilstationär behandelt, zudem komme es immer häufiger zu Kooperationen mit medizinischen Versorgungszentren und angegliederten Praxen. Für die Mitbehandlung

und Weiterbehandlung der Patientinnen und Patienten sei ein zügiger Datenaustausch notwendig. Die Regelungen zum Krankenhausdatenschutz bedürften insofern einer Novellierung, die dem technischen Fortschritt Rechnung trage. Außerdem enthalte das Bremische Krankenhausdatenschutzgesetz viele Regelungstatbestände, die in anderen Gesetzen bereits vorhanden seien. Es sei daher fraglich, ob man dieses Gesetz in seiner Ausführlichkeit überhaupt benötige.

Wir nahmen zu dem Gesetzentwurf Stellung. Dabei vertraten wir die Auffassung, dass sich das Bremische Krankenhausdatenschutzgesetz in der Praxis bewährt hat und gerade aufgrund seines speziellen Praxisbezugs ein sehr fortschrittliches Gesetzeswerk darstellt. Aus diesem Grund sollten Änderungen und Streichungen nur mit Bedacht vorgenommen werden, soweit sie in der Praxis auch tatsächlich erforderlich sind. Wir halten es aus diesen Gründen für die beste Lösung, dass das vorhandene Gesetzeswerk in seinem Regelungsgehalt weitestgehend erhalten wird und Änderungen nur an den Stellen vorgenommen werden, an denen es für die von der Senatorin für Gesundheit erwähnte Berücksichtigung neuer Versorgungsformen in der Praxis, beispielsweise einer vermehrten ambulanten und teilstationären Behandlung, tatsächlich erforderlich und unter Abwägung der Interessen der Patientinnen und Patienten und der anderen beteiligten Stellen angemessen ist. Den in der Gesetzesbegründung formulierten Anspruch, auf die neuen Entwicklungen in der Krankenhausbehandlung unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung zu reagieren, sehen wir mit dem vorliegenden Gesetzesentwurf gerade nicht erfüllt. Stattdessen werden bestehende spezielle Regelungen für die elektronische Datenverarbeitung im Krankenhaus ersatzlos gestrichen. Die pauschale Absenkung des Datenschutzniveaus lediglich zum Zweck der Vereinfachung von Verfahrensvorgängen ohne Abwägung der widerstreitenden Interessen genügt nicht dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Unsere praktischen Erfahrungen in der Anwendung des Bremischen Krankenhausgesetzes decken sich nicht mit den Ausführungen der Gesundheitssenatorin, wonach hier eine Überregulierung vorhanden ist, die abzubauen sei. Insbesondere die besondere Sensibilität der im Krankenhaus verarbeiteten Daten bedarf unter Berücksichtigung der potentiellen Gefahren einer elektronischen Verarbeitung differenzierter und praxisnaher Regelungen, wie sie seinerzeit in Zusammenarbeit der Akteure geschaffen worden sind. Insbesondere die Klarheit und Ausgewogenheit der gefundenen Regelungen hat zum Ergebnis, dass in Bremen mit dem Bremischen Krankenhausdatenschutzgesetz ein handwerklich gutes Gesetz geschaffen wurde, das die praktischen Anforderungen in besonderer Weise berücksichtigt und nach unserer Auffassung keiner wesentlichen Änderung bedarf.

8. Soziales

8.1 Datenbank Haaranalysen im Amt für Soziale Dienste

Im Juli 2012 erfuhren wir, dass es für die Datenbank, in der das Amt für Soziale Dienste (Jugendamt) Sozialdaten von drogenabhängigen Eltern und deren Kindern verarbeitet, von denen Gutachtenaufträge für Haaranalysen vergeben werden, kein Datenschutzkonzept beziehungsweise keine Verfahrensbeschreibung gibt. Gleichzeitig gab es begründete Zweifel an der Einhaltung der technischen und organisatorischen Maßnahmen zum Datenschutz nach dem Sozialgesetzbuch X. In dieser Datenbank sind sehr sensible Sozialdaten, wie Namen, Geburtsdaten, Ergebnisse der Gutachten sowie Informationen zu den in den betroffenen Familien vorgesehenen und durchgeführten Hilfemaßnahmen gespeichert.

Auf Nachfrage wurde uns mitgeteilt, dass diese Probleme im Amt für Soziale Dienste bereits aufgegriffen und die Einhaltung der datenschutzrechtlichen Anforderungen vom behördlichen Datenschutzbeauftragten angemahnt worden waren. Unsere Sachstandsanfragen aus den Monaten Mai, August, Oktober 2013 und Februar, April und Juli 2014 ergaben jedoch, dass die Anforderungen noch immer nicht erfüllt wurden. Daraufhin richteten wir im Juli 2014 eine schriftliche Anfrage an das Amt für Soziale Dienste, in der wir um Vorlage der Verfahrensbeschreibung sowie der Darstellung der Zugriffsberechtigungen für die Datenbank Haaranalysen baten. Daraufhin erhielten wir vom Jugendamt die Mitteilung, dass die von uns angeforderten Dokumente nicht existierten, die Datenbank jedoch aufgrund ihrer begrenzten Nutzungsmöglichkeiten in Kürze weiterentwickelt und in diesem Zusammenhang die von uns angeforderten Unterlagen erstellt würden. Zudem wurde mitgeteilt, dass zwei Mitarbeiterinnen eine Zugangsberechtigung zur Datenbank hätten und Auswertungen nur in anonymisierter Form erfolgen würden. Ohne die angeforderten Unterlagen waren noch nicht einmal diese Informationen durch uns überprüfbar. Für den Überarbeitungsprozess baten wir dem Jugendamt unsere Unterstützung an.

Als im März 2015 diesbezüglich noch immer keine weitere Entwicklung zu verzeichnen war, forderten wir das Amt für Soziale Dienste (Jugendamt) unter Hinweis auf den hohen Schutzbedarf der Daten auf, uns mitzuteilen, welche Maßnahmen getroffen worden seien, um einen datenschutzgerechten Einsatz der Datenbank zu gewährleisten. Wir wiesen erneut auf die Dringlichkeit der Umsetzung der datenschutzrechtlichen Anforderungen bei der seit nunmehr über drei Jahren betriebenen Datenbank hin und baten um Information über den Stand der Planungen für die Neukonzeption und die geplanten neuen Auswertungsmöglichkeiten. Im Mai 2015 erfuhren wir dann auf telefonische Nachfrage, dass das Amt für Soziale Dienste (Jugendamt) sich nicht in der Lage sehe, die von uns geforderten Maßnahmen zu treffen und zu beschreiben, obwohl dort bekannt war, dass die Datenbank erhebliche Mängel aufweist. Auf den Einsatz der Datenbank könne aus

fachlichen Gründen jedoch nicht verzichtet werden. Mit der erforderlichen Neukonzeption habe noch nicht begonnen werden können, da der entsprechende fachliche Bedarf noch nicht festgestellt worden sei. Dies solle in Kürze erfolgen. Wir baten um frühzeitige Beteiligung bei der Neukonzeption und erhielten die Zusage, dass uns der Konzeptentwurf bald übersandt werden würde. Später erhielten wir die Mitteilung, dass sich dieser Prozess bis in den Herbst 2015 hinziehen könnte. Im Juli 2015 teilten wir dem Amt für Soziale Dienste (Jugendamt) dann erneut mit, dass dieser Zustand inakzeptabel ist, da mit dem Betrieb der Datenbank mit sehr sensiblen Sozialdaten gegen Datenschutzrecht verstoßen wird, was seit Jahren bekannt ist, ohne dass eine Beseitigung der Mängel absehbar ist. Wir forderten erneut dazu auf, sich unverzüglich um die Beseitigung der datenschutzrechtlichen Mängel zu kümmern und erneuerten unser Angebot zur beratenden Unterstützung bei der Neukonzeptionierung einer Datenbank. Bis Redaktionsschluss gab es diesbezüglich keine weitere Entwicklung.

8.2 Bremerhavener Modell

Im März des Berichtsjahres informierte uns das Jobcenter Bremerhaven über ein gemeinsames Modellprojekt "Bremerhavener Modell – Perspektiven für Familien in Bremerhaven" mit dem Amt für Jugend, Familie und Frauen. In diesem mit Mitteln des Europäischen Sozialfonds (ESF) geförderten Projekt sollen Familien, insbesondere mit Migrationshintergrund oder Alleinerziehende mit unter-sechsjährigen Kindern, durch niedrigschwellige Hilfen erreicht und gefördert werden, um verfestigte Strukturen von Langzeitarbeitslosigkeit zu durchbrechen. Dafür sollen Familien, die bereits Hilfen der beiden beteiligten Stellen in Anspruch nehmen, auf freiwilliger Basis eine institutionalisierte Betreuung durch ein sogenanntes Tandem bestehend aus jeweils einer Mitarbeiterin beziehungsweise einem Mitarbeiter des Jugendamtes und des Jobcenters in einem neuen Familienzentrum erhalten. Ziel ist eine abgestimmte Arbeitsmarktunterstützung und Familienunterstützung aus einer Hand, die auf die individuellen Bedürfnisse der Betroffenen konkret eingeht, um die Erwerbschancen zu steigern und die sozioökonomische Situation der Familien und damit die Zukunftschancen der Kinder zu verbessern. In die Umsetzung ist je nach individueller Problemlage auch die Einbindung spezialisierter Angebote weiterer Stellen vorgesehen. Das Modellprojekt war zunächst für achtzehn Monate geplant mit einer Verlängerungsoption auf drei Jahre. Ziel ist eine langfristige Überleitung in den Regelbetrieb. Eine Evaluation ist ebenfalls vorgesehen. Um die für die Umsetzung des Projekts erforderliche Verwendung von Sozialdaten zu legitimieren, sollen die Teilnehmerinnen und Teilnehmer eine datenschutzrechtliche Einwilligungserklärung abgeben. Ein Entwurf für ein Einwilligungsformular wurde uns vorgelegt.

Wir wandten uns an das Amt für Jugend, Familie und Frauen und baten um die Erstellung eines Datenschutzkonzeptes, das eine Darstellung der Erhebung, Verarbeitung und Nutzung

von Sozialdaten in diesem Projekt sowie eine Beschreibung der technischen und organisatorischen Maßnahmen enthält. Insbesondere baten wir um Darstellung der Verwendung von Sozialdaten im Rahmen der Auswahl der potentiellen Projektteilnehmenden, um Mitteilung, ob und gegebenenfalls in welchem Umfang eine gemeinsame Dokumentation beziehungsweise Datenverarbeitung der Kooperationspartner vorgesehen ist, und um Erstellung eines Löschkonzepts für eine eventuelle gemeinsame Datenhaltung. Wir baten ebenfalls um Darlegung des Evaluationskonzeptes. Für das Einwilligungsformular sahen wir den folgenden Änderungsbedarf: Die Betroffenen müssen detailliert über das Projekt und die dafür geplanten Erhebungen, Verarbeitungen und Nutzungen ihrer Sozialdaten, zum Beispiel für das Profiling und die Bedarfsanalyse, informiert werden. Zudem wiesen wir darauf hin, dass die Datenübermittlung an weitere Dritte, wie zum Beispiel Beschäftigungsträger oder andere Kooperationspartner nur mit Einwilligung der Betroffenen zulässig ist, die jedoch erst eingeholt werden kann, wenn bekannt ist, welche Stellen eingebunden werden sollen. Auch die Verarbeitung und Nutzung von Sozialdaten zum Zweck der Evaluation bedarf einer informierten Einwilligung der Betroffenen. Das Einwilligungsformular sollte zudem einen Hinweis auf die Freiwilligkeit und die Möglichkeit zum Widerruf und dessen Folgen enthalten. Zudem wiesen wir darauf hin, dass die Erklärung von allen betroffenen Familienmitgliedern höchstpersönlich erteilt werden muss. Dies gilt auch für Jugendliche, die die erforderliche Einsichtsfähigkeit zur Abgabe einer solchen Erklärung besitzen. Zudem empfahlen wir die Verwendung einer einfacheren Sprache.

Das Jugendamt teilte daraufhin mit, dass keine gemeinsame elektronische Datenhaltung der beiden Kooperationspartner vorgesehen sei, sondern dass der Austausch von personenbezogenen Daten lediglich in Papierform vorgesehen sei. Die Umsetzung unserer Anforderungen wurde zugesagt. Diesbezüglich wiesen wir darauf hin, dass diese vor Projektstart erfolgen müsse.

Mitte Juni dieses Berichtsjahres wurden uns überarbeitete Projektunterlagen zur Verfügung gestellt, die den überwiegenden Teil unserer Anforderungen nicht erfüllten. Es fehlten weiterhin die detaillierte Darstellung der Datenverarbeitung zum Zweck der Auswahl der Teilnehmenden und eine Darstellung des Evaluationskonzeptes. Im Einwilligungsformular fehlten weiterhin die umfassende schriftliche Aufklärung der Betroffenen über das Projekt und die in diesem Zusammenhang geplante Verwendung ihrer Sozialdaten. Das Formular enthielt immer noch die von uns als unwirksam abgelehnte pauschale Einwilligung in die Datenübermittlung an gegebenenfalls zu beteiligende Beschäftigungsträger. Wir baten insoweit erneut um Nachbesserung.

Daraufhin teilte uns das Amt für Jugend, Familie und Frauen mit, dass der Auswahlprozess durch Ansprache von Familien erfolge, ohne dass dafür Daten an den Kooperationspartner

übermittelt würden, lehnte dann jedoch eine entsprechende Konkretisierung im Konzept ab. Zudem wurde mitgeteilt, dass ein Flyer mit Informationen für die Teilnehmenden des Projektes mangels Ressourcen erst zu einem späteren Zeitpunkt erstellt werden solle. Zu Evaluationszwecken würden keine Sozialdaten verwendet und an Dritte weitergegeben. Zumindest für die Evaluation für den Europäischen Sozialfonds ist dies unzutreffend. Der Bitte, uns auch das Evaluationskonzept darzustellen, kam das Amt nicht nach. In Bezug auf das Einwilligungsformular wurde die Umsetzung unserer Anforderungen abgelehnt.

Daraufhin teilten wir dem Amt für Jugend, Familie und Frauen mit, dass eine Konkretisierung des Auswahlprozesses und der Datenverarbeitung zu Evaluationszwecken in den Konzeptunterlagen erforderlich ist. Zudem wiesen wir darauf hin, dass mit dem aktuellen Entwurf für ein Einwilligungsformular aufgrund der bestehenden Mängel von den Betroffenen keine wirksame Einwilligungserklärung eingeholt werden kann. Schließlich teilten wir mit, dass unter diesen Umständen eine Abstimmung dieses Projekts mit uns nicht möglich sei.

Anfang September dieses Berichtsjahres erhielten wir dann aber noch einmal geänderte Unterlagen, die jedoch weiterhin viele der von uns im März 2015 gestellten Anforderungen nicht enthielten. Als datenschutzrechtlichen Zugewinn sehen wir es aber an, dass die Einwilligungserklärung zur Datenübermittlung an gegebenenfalls einzuschaltende Beschäftigungsträger erst eingeholt werden soll, wenn feststeht, um welchen Beschäftigungsträger es sich handeln wird.

Der Projektstart war zum Oktober des Berichtsjahres geplant. Zum Redaktionsschluss erhielten wir keine Bestätigung, dass unsere bislang nicht erfüllten Anforderungen mittlerweile umgesetzt worden sind.

8.3 Fachverfahren OK.JUG des Amtes für Soziale Dienste

Im September 2012 erfuhren wir erstmalig vom Amt für Soziale Dienste, dass das Fachverfahren OK.JUG des Jugendamtes keine Möglichkeit bietet, Zugriffsrechte auf einzelne Fälle zu beschränken. Es besteht lediglich die Möglichkeit, Zugriffe auf einzelne Bildschirmmasken zu beschränken. Bildschirmmasken sind Formulare, die Benutzerinnen und Benutzer des Systems beim Erstellen, Erarbeiten und Anzeigen von Daten eines Vorgangs unterstützen. Sie ermöglichen keine Zugriffsbeschränkungen auf einzelne Fälle. Dies widerspricht den Darstellungen im Datenschutzkonzept für das Fachverfahren OK.JUG. Da aus diesem Grund für die Mitarbeiterinnen und Mitarbeiter des Jugendamtes und einige Mitarbeiterinnen und Mitarbeitern der senatorischen Behörde insoweit ein unbeschränkter Zugriff eingerichtet worden ist, wird damit seit Jahren in erheblicher Weise gegen das Sozialgeheimnis verstoßen. Das Sozialgeheimnis legt fest, dass jeder Anspruch darauf hat, dass seine Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden und die Verpflichtung umfasst, auch innerhalb des Leistungsträgers

sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden.

Das Amt für Soziale Dienste wurde von uns auf diese Verstöße und die Notwendigkeit der Beseitigung der Mängel hingewiesen. Um diese Angelegenheit kümmerte sich zunächst der behördliche Datenschutzbeauftragte, dem wir dabei beratend zur Seite standen. Für verschiedene Mitarbeiterinnen und Mitarbeiter der senatorischen Behörde wurden die Zugriffsberechtigungen auf deren Initiative daraufhin kurzfristig abgeschaltet. Weitere Maßnahmen erfolgten jedoch nicht.

Unsere Nachfrage im April 2013 ergab, dass das Datenschutzkonzept kurzfristig korrigiert und von der senatorischen Behörde eine technische Lösung zur Behebung der Mängel erarbeitet werden soll. Kurz darauf erhielten wir eine überarbeitete Version des Datenschutzkonzeptes, das nach Auskunft des Amtes für Soziale Dienste jedoch noch immer nicht aktuell war. Eine Bewertung konnte daher von uns nicht erfolgen. Seitdem ergingen in regelmäßigen Abständen Sachstandsanfragen und ab August 2014 auch klare Aufforderungen an das Amt für Soziale Dienste zur Anpassung des Konzeptes und Beseitigung der Datenschutzmängel, die jedoch kein Ergebnis brachten. In der Zwischenzeit gab es auch Beschwerden von Mitarbeiterinnen und Mitarbeitern des Amtes für Soziale Dienste über die von uns angemahnten Datenschutzmängel.

Im Februar 2015 wurde uns vom Amt für Soziale Dienste dann mitgeteilt, dass der Bedarf zur Überarbeitung dort gesehen wird, jedoch eine umfangreiche Bearbeitungszeit in Anspruch nehmen wird. Ein Ergebnis werde daher für Sommer 2015 angestrebt. Daraufhin empfahlen wir dem Amt für Soziale Dienste, zunächst eine Risikoanalyse zur Identifizierung aller aktuellen Mängel durchzuführen und einen Zeitplan zur Beseitigung der Mängel bis zum Sommer 2015 zu erarbeiten. Als wir darauf keine Reaktion erhielten, teilten wir dem Amt für Soziale Dienste im Juli 2015 noch einmal ausdrücklich mit, dass wir den gegenwärtigen Zustand, dass mit OK.JUG seit Jahren ein Fachverfahren betrieben wird, das entgegen der Beschreibung im Datenschutzkonzept keine Möglichkeit bietet, differenzierte Zugriffsrechte für einzelne Vorgangsakten einzurichten, für inakzeptabel halten, da damit gegen die datenschutzrechtlichen Vorschriften zum Sozialgeheimnis, die Verpflichtung zur Einrichtung von Maßnahmen zur Zugriffskontrolle und die Verpflichtung zur Erstellung eines Datenschutzkonzeptes beziehungsweise einer Verfahrensbeschreibung verstoßen wird. Eine Beseitigung der Mängel ist gleichwohl nicht absehbar. Wir forderten das Amt für Soziale Dienste daher noch einmal auf, sich in dieser Angelegenheit dringend um die Beseitigung der datenschutzrechtlichen Mängel zu kümmern und baten dabei unsere Beratung an. Bis Ende des Berichtsjahres sind in dieser Angelegenheit jedoch keine entsprechenden Maßnahmen des Jugendamtes getroffen worden.

9. Bildung, Wissenschaft und Kultur

9.1 Lernsoftware an Bremer Schulen

Das Landesinstitut für Schule bat uns nach der Auswahl einer Lernsoftware um die Begleitung der Entwicklung des Datenschutzkonzeptes. Einvernehmen besteht, dass in den Bremer und Bremerhavener Schulen nur eine Lernsoftware zum Einsatz kommt. Besonders hervorzuheben ist, dass im Rahmen dieser Lernsoftware personenbezogene Daten über Schülerinnen und Schüler sowie Lehrkräfte nur auf Rechnern innerhalb des europäischen Wirtschaftsraums verarbeitet werden dürfen.

Darüber hinaus werden nur die für die pädagogischen Zwecke erforderlichen Daten verarbeitet. Insbesondere können die Lehrkräfte nicht feststellen, wie oft oder wie lange eine Schülerin oder ein Schüler in das System eingeloggt und mit Lernaufgaben befasst war. Festgelegt wurde auch, dass die Schülerstammdaten am Ende des Schuljahres gelöscht und zu Beginn des neuen Schuljahres die aktuellen Daten der jeweiligen Schule beziehungsweise Klasse in die Lernsoftware eingegeben werden. Hinzu kommt, dass die Logdaten (IP-Adresse, Betriebssystem und Browser des Rechners, Art des Zugriffs) nach spätestens 24 Stunden gelöscht werden. Nach dem Vertrag zur Auftragsdatenverarbeitung verpflichtet sich der Dienstleister der Lernsoftware, die vorgenannten Bedingungen durch vorgegebene technische und organisatorische Maßnahmen zu gewährleisten. Außerdem regelt eine Dienstvereinbarung die Belange der Lehrkräfte auch im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten. Die Lernsoftware ist seit Beginn des Schuljahres 2015/16 im Echtbetrieb. Wir begrüßen es, dass das Landesinstitut für Schule, der Personalrat Schulen und der Zentralelternverband gut mit uns kooperiert haben.

9.2 Übermittlung einer Klassenliste an die Erziehungsberechtigten

Das Bremische Schuldatenschutzgesetz sieht seit dem 1. Mai 2015 vor, dass eine Klassenliste in der Primarstufe und der Sekundarstufe I erstellt und diese an die Erziehungsberechtigten der Schülerinnen und Schüler der betreffenden Klasse übermittelt werden darf. Die Liste darf Name, Vorname, Geburtsdatum, Adresse, Telefonnummer und E-Mail-Adresse enthalten. Nach der Gesetzesbegründung soll im Einzelfall die Auseinandersetzung darüber vermieden werden, ob und wie Erziehungsberechtigte vor der Aushändigung der Liste ihre Einwilligung in die Veröffentlichung erklären müssen. Insoweit solle klargestellt werden, dass die genannten Daten innerhalb einer Klasse weitergegeben werden dürfen, um ein lebendiges Klassenleben und einen umfassenden Meinungsaustausch zu ermöglichen. Da wir im Gesetzgebungsverfahren nicht rechtzeitig beteiligt wurden, hatten wir keine Gelegenheit, unsere Bedenken gegen die Regelung vorzubringen. Beispielsweise bestehen erhebliche Bedenken gegen die Weiterleitung dieser

Daten eines Schulkindes, dessen Mutter sich gemeinsam mit dem Kind – auch nur kurzzeitig – in einem Frauenhaus aufhält. Auch sind erhebliche Unannehmlichkeiten für Betroffene zu befürchten, wenn ein Elternteil mit dem Kind im Falle einer Trennung umzieht.

Aus diesem Grund haben wir die Schulaufsicht (Senatorin für Kinder und Bildung sowie Schulamt Bremerhaven) gebeten, vor der Erstellung der Klassenliste die betroffenen Erziehungsberechtigten auf ihr Widerspruchsrecht – auch bezogen auf einzelne Daten – hinzuweisen. In besonderen familiären Situationen kann gegen die Aufnahme der oder einzelner Angaben in die Liste widersprochen werden. Dies hat zur Folge, dass eine aktuelle Liste erstellt und ausgehändigt werden muss, verbunden mit dem Hinweis an die Erziehungsberechtigten, die alte Liste zu vernichten. Nach beziehungsweise beim Aushändigen der Klassenliste sind die Erziehungsberechtigten darauf hinzuweisen, dass die Daten auf der Liste nur zu den konkreten Zwecken verwendet werden dürfen. Die Liste ist am Schuljahresende zu vernichten. Auf den Rechnern oder sonstigen Kommunikationsgeräten, beispielsweise Smartphones, sind zumindest die E-Mail-Adressen und Telefonnummern zu löschen, wenn kein weiterer privater Kontakt zu anderen Eltern oder Schülerinnen und Schülern mehr besteht.

Die Senatorin für Kinder und Bildung hat uns darauf hingewiesen, nach dem Bremischen Datenschutzgesetz gelte das Widerspruchsrecht nicht, wenn eine Rechtsvorschrift zur Verarbeitung der Daten verpflichte. Wir haben diesen Einwand nicht akzeptiert, weil die neue Regelung die Schulaufsicht beziehungsweise Schule zur Aushändigung der Klassenliste nicht ausdrücklich verpflichtet. Zumindest haben wir erhebliche Zweifel, ob der Landesgesetzgeber das Widerspruchsrecht insoweit aushebeln wollte. Daraufhin erklärte das Ressort, unsere Anforderungen erfüllen zu wollen. Sie hat uns den Entwurf einer Verfügung für die Grundschulen und Schulen des Sekundarbereichs I sowie eine Anpassung der Informationen über datenschutzrechtliche Bestimmungen für die entsprechenden Erziehungsberechtigten vorgelegt, die unsere Anforderungen erfüllen.

9.3 Weitergabe anvertrauter Schülerdaten an andere Schüler

Wir wurden gefragt, ob Lehrkräfte Informationen, die ihnen von Schülerinnen oder Schülern anvertraut wurden, an andere Schülerinnen und Schüler weitergeben dürfen. Beispielsweise habe ein Schüler Probleme mit Lehrkräften gehabt. Diese Probleme habe er einer anderen Lehrkraft anvertraut. Dennoch habe die Lehrkraft anderen Schülerinnen und Schülern davon erzählt, ohne dass diese nachgefragt hätten.

Wir erklärten daraufhin, dass Lehrkräfte ihnen anvertraute Schülerdaten nur an andere Schülerinnen und Schüler weitergeben dürfen, soweit die oder der Betroffene darin eingewilligt hat. In dem beschriebenen Fall hätte die Lehrkraft wegen dieser Vertraulichkeit eine besondere Sorgfalt walten lassen müssen.

9.4 E-Mail an alle Eltern mit Angaben über einzelne Schülerinnen und Schüler

Die Lehrerin einer Schule schrieb die Eltern der Schülerinnen und Schüler ihrer Klasse per unverschlüsselter E-Mail an. Beim Hinweis auf zu erledigende Aufgaben erwähnte sie einige Schülerinnen und Schüler namentlich, ohne dass die Angaben der Namen der Betroffenen erforderlich waren.

Die Schulleitung erklärte, es habe sich um sachliche Informationen ohne persönliche Wertung gehandelt. Die Kollegin habe dies bedauert und werde zukünftig auf die Namensnennung bei E-Mails verzichten.

10. Medien/Telemedien

10.1 Veröffentlichung personenbezogener Daten auf privaten Internetseiten

Im Berichtsjahr erreichten uns zahlreiche Beschwerden und Hinweise über die Speicherung und Veröffentlichung von personenbezogenen Daten auf privaten Internetseiten. Häufig ging es dabei um die private Fahndung nach Personen oder um eine Form eines virtuellen Prangers. So stellte ein Marktleiter eines Supermarktes mittels seiner privaten Homepage ein Foto einer Überwachungskamera in das Internet und erhoffte sich so, Kenntnis über die abgebildete Person durch die Besucherinnen und Besucher der Seite zu erlangen. Nach unserem Einschreiten löschte der Marktleiter das Bild. In anderen Fällen berichteten private Internetseiten namentlich von Personen, die bei Behörden oder Unternehmen arbeiten. Die Betreiberinnen und Betreiber von Internetseiten fühlten sich dabei von den offiziellen und privaten Stellen schlecht oder falsch behandelt. In einigen Fällen konnten wir hier bereits argumentativ überzeugen, sodass die Daten geschwärzt oder gelöscht wurden, ein Fall ist noch offen.

Diejenigen, die personenbezogene Daten veröffentlichen wollen, benötigen dafür eine Rechtsgrundlage oder eine Einwilligung der Betroffenen. Eine Einwilligung liegt in den uns gemeldeten Fällen in der Regel nicht vor. Damit sich die Betreiberin beziehungsweise der Betreiber der Internetseite beispielsweise auf die Rechtsgrundlage § 28 Bundesdatenschutzgesetz berufen kann, – diese würde die Veröffentlichung der personenbezogenen Daten erlauben – muss die Veröffentlichung zur Verfolgung der berechtigten Interessen der Betreiber erforderlich sein und außerdem dürfen keine schutzwürdigen Interessen der Betroffenen entgegenstehen.

Bei der "Privatfahndung" und auch bei der wahrscheinlich beabsichtigten Prangerwirkung muss die im Gesetz verlangte Erforderlichkeit verneint werden. Solche Privatpersonen

maßen sich Befugnisse an, die ausschließlich den staatlichen Stellen, insbesondere den Strafverfolgungsbehörden, zustehen. Auch wiegen die schutzwürdigen Interessen der Betroffenen schwerer. Neben der zu großen Gefahr, dass sich eine Veröffentlichung im Internet viral verbreitet und dass die veröffentlichende Person dabei die Kontrolle über die Informationen verliert, haben die Betroffenen einen Anspruch auf ein geordnetes staatliches Verfahren. Stigmatisierung und Sanktionierung durch die öffentliche Namensnennung oder durch die Veröffentlichung eines Fotos gehören nicht zu den rechtstaatlichen Verfahren unserer Gesellschaft.

10.2 Datenschutzbeschwerden zum Beitragsservice

Zur Umstellung von der vorher personenbezogenen Rundfunkgebühr auf ein haushaltsbezogenes Beitragsmodell seit dem 1. Januar 2013 war laut Angabe der Rundfunkanstalten ein vollständiger Meldedatenabgleich erforderlich, der mit gesetzlicher Verankerung im Rundfunkbeitragsstaatsvertrag durchgeführt wurde. Sofern bei den Meldebehörden eine Abmeldung, eine Anmeldung oder der Tod von volljährigen Einwohnerinnen oder Einwohnern registriert wird, erlaubt die Verordnung zur Durchführung des Meldegesetzes, insbesondere zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden (MeldDÜV) für Bremen zur Durchführung des Einzugs der Rundfunkbeiträge weitere regelmäßige Datenübermittlungen an Radio Bremen oder beauftragte Dritte. Schon gegen den einmaligen vollständigen Meldedatenabgleich, dessen Erforderlichkeit immerhin mit der Umstellung des Gebührensystems auf den Haushaltsbeitrag begründet werden konnte, bestanden seitens der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erhebliche Bedenken.

Nun argumentieren die Rundfunkanstalten, dass die Erforderlichkeit eines erneuten vollständigen oder gar regelmäßigen Meldedatenabgleichs deshalb gegeben sei, weil nach Auszug aus einer Wohnung (zum Beispiel wegen Trennung, Scheidung, Auflösung einer Wohngemeinschaft) oder nach dem Tod der bisherigen Beitragsschuldnerin beziehungsweise des Beitragsschuldners nicht bekannt sei, wer die Wohnung weiterhin innehabe und damit neue Schuldnerin oder Schuldner sei. Wenn die neue Wohnungsinhaberin beziehungsweise der neue Wohnungsinhaber der gesetzlichen Anzeigepflicht nicht nachkämen, entstehe ein Verlust von Beiträgen von circa 200.000 bis 300.000 Beitragspflichtigen jährlich. Aus datenschutzrechtlicher Sicht ist ein erneuter und gegebenenfalls regelmäßiger bundesweiter Meldedatenabgleich als unverhältnismäßig abzulehnen. Er ist nicht erforderlich, weil, wie dargestellt, regelmäßige Teilabgleiche nach der MeldDÜV vorgesehen sind. Insofern muss stark bezweifelt werden, dass tatsächlich jährlich 200.000 bis 300.000 Meldesätze der "Datenerosion" zum Opfer fallen würden. Gerade deshalb erscheint ein Abgleich mit 70 Millionen Datensätzen bundesweit unangemessen.

Immer wieder erreichen uns Beschwerden zum erhobenen Beitrag der Rundfunkanstalten, die auf die Umstellung zurückzuführen sind. In den meisten Fällen geht es dabei um Personen, die gemeinsam mit einer Beitragszahlerin oder einem Beitragszahler eine Wohnung bewohnen, aber einen anderen Nachnamen haben. Die Petentinnen und Petenten nahmen deshalb mit Radio Bremen persönlich Kontakt auf und schilderten ihre Situation, ohne dass die fälschlich versandten Schreiben daraufhin und für die Zukunft unterblieben. Nachdem wir uns jeweils an Radio Bremen gewandt hatten, versandte der Beitragsservice keine weiteren Schreiben an die Petenten. Warum deren Kontaktaufnahme mit dem Beitragsservice nicht schon direkt zu dem gewünschten und berechtigten Erfolg geführt hatten, ist uns unklar.

10.3 Runder Tisch Digitale Kultur

Der Runde Tisch Digitale Kultur besteht aus Vertreterinnen und Vertretern unter anderem der Universität, des Zentralelternverbands, der Senatorin für Kinder und Bildung sowie der Landesbeauftragten für Datenschutz und Informationsfreiheit. Im Berichtszeitraum befasste er sich mit einem Projekt, in dem Jugendliche zu Experten in Sachen Internetsicherheit ausgebildet werden. Sie sollen im Anschluss ihr Wissen in Workshops an Schülerinnen und Schüler in den Klassen 5 und 6 mehrerer Schulen weitergeben.

Außerdem beriet der Runde Tisch über digitale Medien in der frühkindlichen Bildung und die für alle Schulen im Land Bremen eingesetzte Lernsoftware (siehe Ziffer 9.1 dieses Jahresberichts).

11. Beschäftigtendatenschutz

11.1 Einholung einer SCHUFA-Auskunft über Bewerber

Ein Autohaus holte über einen Bewerber eine SCHUFA-Auskunft ein mit der Begründung, der Bewerber habe darin eingewilligt. Dies bestritt der Bewerber und führte an, durch die Einholung der Auskunft sinke sein Scorewert und somit seine Kreditwürdigkeit. Das Autohaus erklärte auf unsere Anfrage, es habe wohl ein Missverständnis wegen der Einwilligung vorgelegen. Grund für die Einholung der Auskunft bei der Auskunftei sei gewesen, dass der Bewerber als Autoverkäufer mit sehr viel Geld bei der Abwicklung eines Autoverkaufs in Kontakt hätte kommen können. In diesem Zusammenhang fragte das Autohaus, ob unseren Bedenken begegnet würde, wenn nur zwei Personen der Personalabteilung Einsicht in die SCHUFA-Auskunft bekämen und der Geschäftsleitung nur das Gesamtergebnis nennen würden.

Hierzu erklärten wir, dass eine Einwilligung in die Einholung von Auskünften bei Auskunfteien im Bewerbungsverfahren wegen des Abhängigkeitsverhältnisses regelmäßig

nicht wirksam ist, weil sie nicht auf der freien Entscheidung der Betroffenen beruht. Verweigern sie die Auskunft, droht ihnen die Nichteinstellung. Außerdem ist eine derartige Auskunft regelmäßig weder geeignet noch erforderlich. Einerseits enthalten diese Auskünfte erheblich mehr Daten über den Bewerber als für die Entscheidung über den zu besetzenden Arbeitsplatz erforderlich sind. Andererseits sind Daten zur Kreditwürdigkeit häufig falsch und sollen nach einem Spiegel-Online-Artikel aus dem Jahre 2009 in fast 50 Prozent der Fälle auf fehlerhaften Daten beruhen (www.spiegel.de/wirtschaft/Service/0,1518,druck-643778,00.html).

Soweit an Bewerberinnen und Bewerber besondere Anforderungen zu stellen sind, reicht es aus, im Wege der Direkterhebung bei den Betroffenen nach Verurteilungen wegen Straftaten im Zusammenhang mit Vermögensdelikten in den letzten fünf Jahren zu fragen. Daher ist die Einholung von Auskünften über Bewerberinnen und Bewerber bei Auskunfteien nicht zulässig, sodass entsprechend gespeicherte Daten zu löschen sind.

Daraufhin erklärte das Autohaus, zukünftig im Rahmen des Bewerbungsverfahrens auf die Einholung von Auskünften bei Auskunfteien oder sonstigen Dritten zu verzichten.

11.2 Kopien von Führerscheinen durch den Arbeitgeber

Ein Unternehmen nutzt ein Formular "Führerscheinkontrolle Nachweisbogen". Darin sind die wesentlichen Führerscheindaten der Beschäftigten aufgeführt, die Fahrzeuge des Unternehmens benutzen. Zugleich ist dort vorgesehen, Kopien der Führerscheine zu erstellen und zu den Vorgängen zu nehmen. Bei jeder Führerscheinkontrolle wurde der Führerschein mit der Kopie verglichen.

Wir halten die Anfertigung von Kopien der Führerscheine nicht für erforderlich. Es reicht aus, sich bei jeder Kontrolle davon zu überzeugen, ob die oder der Beschäftige einen gültigen Führerschein besitzt. Zudem stellt die Anfertigung von Kopien der Führerscheine eine Doppelspeicherung dar, die gegen den gesetzlichen Grundsatz der Datensparsamkeit verstößt.

Das Unternehmen verzichtet nunmehr auf die Anfertigung von Kopien der Führerscheine und vernichtete auf unsere Veranlassung sämtliche noch bestehenden Kopien.

11.3 Aushang der Ergebnisse von Leistungskontrollen

Laut einer bei uns eingegangenen Eingabe hängte ein großes Logistikunternehmen täglich vor jeder Schicht personenbezogene Daten über Leistungskontrollen der Beschäftigten aus. Dadurch waren die Beschäftigten einem unzumutbaren Leistungsdruck ausgesetzt. Wir wiesen das Unternehmen auf diesen Sachverhalt hin und verlangten Auskunft darüber, für welche konkreten Zwecke es diese Maßnahme für erforderlich halte.

Daraufhin erklärte das Unternehmen, es habe geprüft, in welchem Unternehmensbereich diese Praxis durchgeführt worden sein könnte. Dabei sei es auf einen Bereich aufmerksam geworden, in dem Leistungsdaten mit der mitarbeiterbezogenen Bearbeitungsnummer ausgehängt worden seien. Die Zuordnung der Bearbeitungsnummer zum Namen des Beschäftigten sei jedoch nicht veröffentlicht worden. Nach Bekanntwerden sei diese Praxis zeitnah eingestellt worden, sodass nunmehr generell auf den Aushang verzichtet werde. Hierzu ist aus datenschutzrechtlicher Sicht anzufügen, dass die Veröffentlichung der mitarbeiterbezogenen Bearbeitungsnummern ein personenbeziehbares Datum ist, das wie der Name der Beschäftigen selbst vom Grundrecht auf informationelle Selbstbestimmung geschützt ist. Auch die Veröffentlichung der Leistungsdaten mit Bearbeitungsnummern war daher rechtswidrig.

11.4 Übernahme der Gesundheitsakten der Beschäftigten ehemaliger Werften durch die Arbeitnehmerkammer

Der Landesgewerbearzt unterrichtete uns über den Plan des Gesundheitsressorts, Gesundheitsakten der Beschäftigten der ehemaligen Bremerhavener Werften AG Weser und Seebeckwerft zu übernehmen und in der Berufskrankheitenberatungsstelle, angesiedelt bei der Arbeitnehmerkammer, aufzubewahren. Mit den Gesundheitsakten der ehemaligen Werft des Bremer Vulkan, sei seinerzeit ähnlich verfahren worden. Die Übernahme der Akten sowie der Umgang mit den Akten in der Beratungsstelle sei damals vertraglich vereinbart worden. Jetzt solle ebenso verfahren werden. Es handelt sich hierbei vornehmlich um die Ergebnisse von Messungen und Ermittlungen von Schadstoffen, die nach der Strahlenschutzverordnung so lange aufzubewahren sind, bis die überwachte Person das 75. Lebensjahr vollendet hat oder hätte, jedoch mindestens 30 Jahre nach Beendigung der jeweiligen Beschäftigung. Die Unterlagen befanden sich in verschlossenen Räumlichkeiten eines Gebäudes, das zwischenzeitlich von einem anderen Unternehmen genutzt wurde. Zugriff hatte nur der ehemalige Betriebsarzt.

Wir konnten nicht eindeutig erkennen, ob es sich um Gesundheitsakten einzelner Beschäftigter des Betriebsärztlichen Dienstes der ehemaligen Werften oder um sonstige Unterlagen handelte. Unterlagen des Betriebsärztlichen Dienstes dürfen von anderen Stellen nur aufgrund von Schweigepflichtentbindungserklärungen übernommen und aufbewahrt werden. Hinsichtlich der sonstigen Unterlagen, soweit daraus ein Personenbezug herstellbar ist, sind die Betroffenen über die Übernahme zu benachrichtigen. Soweit eine Schweigepflichtentbindungserklärung oder eine Benachrichtigung aufgrund fehlender Kenntnis über die aktuellen Wohnanschriften der Betroffenen nicht möglich ist, soll über Tageszeitungen und andere Medien über die Übergabe der Gesundheitsakten berichtet werden, um so zumindest eine Benachrichtigung der Betroffenen über den Verbleib ihrer

Akten sicherzustellen. Nur so können ihre Rechtsansprüche auf Anerkennung von Berufskrankheiten gewahrt werden.

Sowohl der Landesgewerbearzt als auch die Arbeitnehmerkammer und der ehemalige Betriebsarzt erklärten, unsere Anforderungen bei der Übernahme der Akten einhalten zu wollen.

12. Videoüberwachung

12.1 Flugdrohneneinsatz durch Private

Im Berichtszeitraum wandten sich mehrere Betroffene an uns, weil sie sich durch den Einsatz von Flugdrohnen belästigt fühlten oder sich über deren rechtmäßigen Betrieb informieren wollten. Da die Drohnen meist mit Kameras ausgestattet sind und zwischenzeitlich bereits zu sehr günstigen Preisen zu erwerben sind, werden sie immer öfter auch von Privatleuten genutzt.

Was die meisten Besitzerinnen und Besitzer von Flugdrohnen jedoch nicht wissen, ist, dass die Nutzung der eingebauten Kameras nur unter ganz engen rechtlichen Grenzen möglich ist. Der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung bedarf keiner luftverkehrsrechtlichen Erlaubnis, wenn nicht einer der in § 20 Absatz 1 Nummer 1 Luftverkehrs-Ordnung aufgeführten Fälle vorliegt. Beachtenswert ist hier, dass unter Buchstabe d) eine Erlaubnispflicht für den Aufstieg von Flugmodellen aller Art in einer Entfernung von weniger als 1,5 Kilometer von Flugplätzen festgelegt ist. Zu den Flugplätzen gehören insbesondere auch Sonderlandeplätze, zu denen auch Hubschrauberlandeplätze zählen, die sich vor allem an Krankenhäusern befinden und damit auch relativ häufig zu finden sind.

Zudem sind stets die Beschränkungen des Bundesdatenschutzgesetzes zu beachten, wenn mithilfe von Drohnen personenbezogene Daten erhoben und gespeichert werden und dies nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Ob eine bestimmte Verarbeitung in den Anwendungsbereich persönlicher oder familiärer Verarbeitung fällt oder nicht, ist durch Heranziehung und Auswertung verschiedener Faktoren zu bestimmen. Es ist daher zu prüfen, ob die personenbezogenen Daten an eine unbegrenzte Anzahl von Personen und nicht an eine begrenzte Gemeinschaft von Freunden, Familienmitgliedern oder Bekannten verteilt werden. Ein weiteres Kriterium ist, ob die personenbezogenen Daten über Personen gesammelt worden sind, die keine persönliche oder familiäre Beziehung mit der Person haben, die sie verbreitet. Darüber hinaus ist zu beachten, ob es zu möglichen nachteiligen Auswirkungen auf Personen einschließlich Eingriffs in deren Privatsphäre kommt und ob es Nachweise für eine Reihe von Personen gibt, die kollektiv und organisiert zusammenarbeiten, die auf eine professionelle Tätigkeit oder Vollzeittätigkeit hinweisen.

Weitere Details und Erläuterungen können in dem hierzu inzwischen von uns unter https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Beschluss%20Drohnennutzung%20durch%20Private.pdf veröffentlichten Beschluss der datenschutzrechtlichen Aufsichtsbehörden im nicht öffentlichen Bereich nachgelesen werden, der Betroffene sowie Drohnenbetreiber über die Rechtslage informiert.

12.2 Bremer Filiale eines internationalen Bekleidungsunternehmens

Über einen Zeitungsartikel wurden wir auf eine umfangreiche Videoüberwachung eines internationalen Bekleidungsunternehmens in seiner Filiale in Hannover aufmerksam. Da das Unternehmen auch in Bremen eine Filiale betreibt, nahmen wir dies zum Anlass, mit der Aufsichtsbehörde in Niedersachsen eine gemeinsame Vorgehensweise abzustimmen. Unsere daraufhin gestellte Anfrage wurde vom Unternehmen fristgerecht und umfassend beantwortet. Dabei wurde uns mitgeteilt, dass auch in der Filiale in Bremen eine Vielzahl von Videokameras installiert sei.

Zwischenzeitlich wurde von der Aufsichtsbehörde in Niedersachsen in der hannoverschen Filiale eine Vorortprüfung durchgeführt, die aus Sicht der Behörde positiv verlief, da das Unternehmen bereit war, die geforderten Maßnahmen anzuerkennen und umzusetzen. Aufgrund der Prüfung übersandte das Unternehmen einen mit dem betrieblichen Datenschutzbeauftragten abgestimmten Maßnahmenkatalog zur Umsetzung der datenschutzrechtlichen Anforderungen an die Videoüberwachung. Darüber hinaus wurde aufgrund der durchgeführten Prüfung sowie der hierdurch vorgenommenen Bewertungen ein Konzept zur Videoüberwachung in allen deutschen Filialen entwickelt. In diesem Konzept erfolgte eine allgemeine Bewertung von Kameragruppen, die auch in Bremen umgesetzt werden sollte.

Wir setzten dem Unternehmen eine Frist zur Umsetzung, um vor unserer anschließenden Prüfung diese Basisanforderungen sowie die für den Bremer Standort relevanten örtlichen Besonderheiten gezielt zu überprüfen und gegebenenfalls anzupassen. Im Verlauf unserer Prüfung konnten wir dann feststellen, dass sich die Anzahl der Kameras deutlich verringert hatte und die Erfassungsbereiche bei verschiedenen Kameras den geforderten Vorgaben entsprechend angepasst wurden. Erfreulich war in diesem Zusammenhang, dass das Unternehmen sogar mehr Kameras abgebaut hatte als ursprünglich von uns gefordert worden war.

Auch bundesweit entschloss sich das Unternehmen zu einem Rückbau bereits installierter Kameras und erklärte, die abgestimmten Anforderungen auch bei den geplanten Neueröffnungen umsetzen zu wollen.

12.3 Überwachung durch Webcams

Von einer Reporterin wurden wir im Rahmen eines Interviews zu Webcams an touristisch bedeutsamen Plätzen darauf hingewiesen, dass auf den in das Internet übertragenen Bildern von zwei Kameras auch Personen erkennbar seien. Auf unsere schriftliche Anfrage hin erklärte uns die verantwortliche Stelle, dass sie die Bilder der installierten Webcams in der jetzigen Form für zulässig halte, da keine Gesichter oder Autokennzeichen erkennbar seien. Außerdem sei durch die Häufigkeit der Aktualisierung des Motivs jede Darstellung nur kurz sichtbar. Hierdurch werde die Möglichkeit verringert, dass jemand ein Motiv lange betrachte und nach Ähnlichkeiten zu ihm bekannten Personen aufgrund von Kleidung oder anderen Merkmalen suchen könne. Daraufhin legten wir dar, dass Webcams aus datenschutzrechtlicher Sicht problematisch sind, da durch sie Live-Bilder ins Internet eingestellt werden, die hierdurch einer unbestimmten Zahl von Personen weltweit zugänglich gemacht werden. Einmal ins Internet eingestellt, können auch unbewegte nur kurzeitig eingestellte Bilder aufgrund der technisch einfach zu handhabenden Möglichkeiten weiterverarbeitet und auch vervielfältigt werden. Des Weiteren erläuterten wir, dass Personen nicht nur dann identifizierbar sind, wenn ihre Gesichter zu erkennen sind, sondern beispielsweise auch bereits dann, wenn weitere Umstände wie etwa auffällige Kleidung, Frisur, Körpergröße, eine ersichtliche körperliche Behinderung oder ein bestimmtes Verhalten die Identifizierung einer Person ermöglichen. Dabei genügt es, wenn Menschen mit besonderem Zusatzwissen einzelne Personen auf den Bildern erkennen und identifizieren könnten. Es kommt nicht darauf an, dass die Personen auch tatsächlich identifiziert werden. Schon der Umstand, dass durch Abgleich mit Bilddatenbanken über automatisierte Mustererkennungsverfahren, aber auch durch visuellen Abgleich von Screenshots oder durch Kenntnisnahme über Bekannte eine Identifizierung möglich ist, genügt für die rechtliche Annahme eines Eingriffs in das Persönlichkeitsrecht sowie zur Beeinträchtigung des Rechts, unbeobachtet zu sein. Daraufhin wurden von der verantwortlichen Stelle die installierten Webcams so verändert, dass nunmehr auch unter den zuvor geschilderten Umständen keine Personen mehr zu identifizieren sind.

12.4 Kameraattrappen

Für die Betroffenen macht es subjektiv keinerlei Unterschied, ob eine Kamera in Betrieb oder ausgeschaltet ist oder ob es sich um eine Attrappe handelt. Immer wird der Eindruck erweckt, es finde eine Videoüberwachung statt. Der beabsichtigte Abschreckungseffekt kann nur erreicht werden, wenn die Kamera nicht ohne weiteres als Attrappe zu erkennen ist. Damit unterscheidet sich die Situation für Außenstehende nicht wesentlich von derjenigen, die durch Anbringung einer funktionsfähigen Kamera geschaffen wird. Da für die Betroffenen nicht erkennbar ist, ob sie tatsächlich gefilmt werden oder nicht, wird auch durch eine

Attrappe, die einer funktionsfähigen Kamera optisch gleicht, bei den Betroffenen der Eindruck erweckt, sie müssten ständig mit einer überwachenden Aufzeichnung rechnen.

Da von einer Attrappe also derselbe Überwachungsdruck ausgeht wie von einer tatsächlich funktionsfähigen Überwachungskamera, hat dies in der Regel eine Verhaltensänderung zur Folge, was wiederum einen Eingriff ins allgemeine Persönlichkeitsrecht darstellt. Nach § 1 Absatz 1 Bundesdatenschutzgesetz (BDSG) ist Zweck dieses Gesetzes, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. So ist auch das Bundesverfassungsgericht zu Recht davon ausgegangen, dass schon das "diffus bedrohliche Gefühl des Beobachtetseins" eine unbefangene Wahrnehmung der Grundrechte beeinträchtigen kann (Urteil zur Vorratsdatenspeicherung vom 2. März 2010). Da durch die täuschend echte Simulation (Attrappe) des Umgangs mit personenbezogenen Daten auch eine Beeinträchtigung des Persönlichkeitsrechts gegeben ist, sind nach unserer Auffassung die Grundsätze des BDSG entsprechend heranzuziehen. Videoüberwachungsattrappen dürfen daher nur dort installiert werden, wo auch eine Videoüberwachung durch funktionsfähige Anlagen rechtmäßig wäre.

12.5 Kleingartenverein

Im Berichtszeitraum wurden vermehrt Anfragen von Betroffenen, Pächtern sowie Vorständen von Kleingartenvereinen an uns gestellt, in denen es um Probleme mit Videokameras in Kleingartengebieten ging. Vorwiegend ging es um Fragen, welche Bereiche von einer Kamera erfasst werden dürfen und welche rechtlichen Vorschriften zu beachten sind, damit der Betrieb einer Kamera aus Datenschutzsicht zulässig ist. Den Anfragenden wurden die gesetzlichen Regelungen zur Videoüberwachung erläutert, deren Ziel es ist, einen angemessenen Ausgleich zwischen den unterschiedlichen Interessen zu gewährleisten.

Darüber hinaus wurden die Anfragenden auf die aktuelle Orientierungshilfe "Videoüberwachung durch nicht öffentliche Stellen" hingewiesen[5]. In der Orientierungshilfe werden den von der Überwachung Betroffenen die gesetzlichen Vorgaben erläutert, damit es ihnen selbst möglich ist, zu erkennen, ob sie eine Videoüberwachung hinnehmen müssen oder ob sie sich dagegen wehren können. Den für die Videoüberwachung Verantwortlichen werden konkrete Hinweise für ihre eigenverantwortliche Prüfung gegeben, damit ihre Überwachung den gesetzlichen Anforderungen des Datenschutzes gerecht wird. Abschließend hatten wir allen Anfragenden angeboten, sich erneut an uns zu wenden, falls sie anhand der erhaltenen Erläuterungen sowie der Orientierungshilfe ihr Videoüberwachungsproblem nicht selbst zufriedenstellend lösen konnten. Da uns keine

[5]https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Orientierungshilfe%20Video%FCberwachung%20durch%20nicht-%F6ffentliche%20Stellen.pdf

weiteren Anfragen oder Eingaben derselben Personen erreichten, gehen wir davon aus, dass die erteilten Informationen sowie der Hinweis auf die veröffentlichte Orientierungshilfe zur Abhilfe der geschilderten Probleme geführt haben.

12.6 Urteil des Europäischen Gerichtshofs zur privaten Videoüberwachung

Ein Urteil des Europäischen Gerichtshofs (EuGH) im Dezember 2014 bestätigte die Verfahrensweise der deutschen Datenschutzbehörden, auch den Einsatz von im Privatbereich eingesetzten Videokameras kritisch zu hinterfragen. Beispielsweise Passanten, Nachbarn oder Mitbewohner beschweren sich in den letzten Jahre stetig zunehmend über solche Kameras. Aufgrund der schutzwürdigen Interessen der Betroffenen ist eine Videoüberwachung öffentlicher Räume in aller Regel unzulässig. Ein geringfügiges Überschreiten der Grundstücksgrenze durch den Erfassungsbereich der Kamera kann allenfalls zulässig sein, wenn es zum Beispiel in der Vergangenheit zu massiven Beeinträchtigungen oder zu Angriffen auf die unmittelbare Wohnsphäre gekommen ist.

Durch das Urteil wurde entschieden, dass private Videoüberwachung durch das Datenschutzrecht begrenzt ist, wenn sie sich auch nur teilweise auf den öffentlichen Raum erstreckt. Für die Bejahung einer ausschließlich persönlichen oder familiären Tätigkeit, die die Anwendbarkeit der Europäischen Datenschutzrichtlinie ausschließt, müsse eine enge und objektive Verbindung mit dem Privatleben einer Person bestehen und die Privatsphäre anderer dürfe nicht spürbar berührt werden, was bei einer systematischen Videoüberwachung des öffentlichen Raums nicht der Fall sei.

Darüber hinaus bestätigte der EuGH auch, dass ein Kameraeinsatz aus Sicherheitsgründen gerechtfertigt sein kann, wobei jedoch ein gesteigertes Sicherheitsbedürfnis der Betreiberin beziehungsweise des Betreibers nicht genüge. Bei der Abwägung der widerstreitenden Grundrechtsinteressen müssten vielmehr die berechtigten Sicherheitsbelange der Aufnehmenden gegenüber den Schutzinteressen von Betroffenen überwiegen. Da wir die Ausnahme der persönlichen und familiären Tätigkeit bereits zuvor restriktiv ausgelegt haben, hatte das Urteil des EuGH im Ergebnis keine Änderung unserer aufsichtsbehördlichen Praxis zur Folge.

12.7 Videoüberwachung und Tonüberwachung der Beschäftigten in einem Restaurant

In einem Restaurant wurden Beschäftigte per Videokameras mit integrierten Mikrofonen mindestens in der Küche überwacht; am Tresen sowie im mittleren Teil des Restaurants galt dies auch für die Gäste. Der Geschäftsführer des Restaurants erklärte uns, die Videoüberwachungsanlage und Tonüberwachungsanlage diene ausschließlich der

Einbruchsdiebstahlvorsorge, da er bereits mehrfach nachweislich Schäden durch Einbruchsdiebstahl habe hinnehmen müssen. Die Anlage würde erst nach Geschäftsschluss eingeschaltet.

Wir erklärten ihm, dass es nach unseren Erfahrungen zur Einbruchsvorsorge ausreicht, nur die Haupteingänge und Nebeneingänge per außen angebrachten Videokameras zu überwachen, die zudem weder schwenkbar noch zoombar sein dürfen. Daher verlangten wir, die Kameras innerhalb der Räumlichkeiten des Restaurants zu entfernen, auch weil die Betroffenen keine Gewähr hatten, ob die Videokameras im Tresenbereich, in der Küche und im mittleren Teil des Restaurants tatsächlich nur außerhalb der Geschäftszeiten aktiviert waren.

Eine Tonüberwachung ist für die Einbruchsvorsorge nicht erforderlich, weil hierzu die Videoüberwachung ausreicht. Zudem ist Tonüberwachung generell nicht zulässig, weil hierfür keine Rechtsgrundlage besteht, die dies ausdrücklich erlaubt. Außerdem wiesen wir darauf hin, dass sich alle strafbar machen, die das nicht öffentlich gesprochene Wort anderer unbefugt auf einen Tonträger aufnehmen. Wir verlangten daher, auf die Tonaufzeichnung beziehungsweise Tonüberwachung zu verzichten, und diese Funktion unverzüglich programmtechnisch zu deaktivieren. Sofern eine Deaktivierung nicht möglich ist, sind die Videokameras an den Haupteingängen und Nebeneingängen unverzüglich durch Kameras zu ersetzen, die Tonaufnahmen technisch ausschließen.

Daraufhin erklärte der Geschäftsführer, er habe die Videoüberwachungsanlage und Tonüberwachungsanlage abmontiert.

12.8 Verdeckte Überwachung der Beschäftigten bei Geld- und Werttransporten

Ein Geld- und Werttransportunternehmen ließ seine Beschäftigten während eines stichprobenartig ausgewählten Arbeitstages verdeckt überwachen, auch per Videokamera. Die Protokolle darüber enthielten neben betrieblich bedeutsamen Angaben (Trageweise der Waffen, Dienstkleidung, Fahrzeug richtig abgestellt, Schusshand frei) auch sonstige Beobachtungen im Umfeld (zum Beispiel Beschäftigter kauft ein). Auffälligkeiten, Mängel und sonstige Sachverhalte wurden notiert. Zur Begründung wies das Unternehmen auf die Einhaltung des Arbeitsrechts und des Unfallverhütungsrechts hin. Es sei erforderlich, die Betriebsabläufe "stichprobenartig" zu kontrollieren, um die Sicherheit der Geld- und Werttransporte sowohl zur Sicherheit der Beschäftigten als auch der Allgemeinheit zu gewährleisten.

Wir erklärten dem Unternehmen, dass für die Einhaltung der genannten Zwecke stichprobenartige Kontrollen zulässig sind, soweit sie verhältnismäßig sind und die

schutzwürdigen Interessen der Beschäftigten nicht überwiegen. Weder eine verdeckte noch eine offene Videoüberwachung ist dafür erforderlich. Es reicht aus, wenn Personen die Betroffenen stichprobenartig zunächst verdeckt kontrollieren, hierbei nur die für Revisionszwecke erforderlichen Sachverhalte notieren und dies dann offengelegt und zeitnah mit den Betroffenen besprochen wird. Außerdem müssen die Beschäftigten eindeutig über die erforderliche Datenverarbeitung für konkret festzulegende verdeckte Kontrollen durch Personen und sonstige verhältnismäßige Kontrollen sowie die Speicherdauer der Daten unterrichtet werden. Diese Unterrichtung – beispielsweise in einem leicht verständlichen Merkblatt – muss auch die Zwecke der Datenverarbeitung benennen.

Das Unternehmen teilte uns mit, unsere Vorgaben einzuhalten und nur Kontrollen mit ausschließlich schriftlicher Protokollierung vorzunehmen. Sämtliche Videoaufzeichnungen und daraus erstellte Fotografien seien gelöscht worden.

13. Auskunfteien, Inkasso, Kreditwirtschaft, Versicherungen

13.1 Fehlerhafte Meldung eines Inkassounternehmens an eine Auskunftei

Ein Petent wandte sich mit der Bitte an uns, die Datenmeldung eines Inkassounternehmens an eine Auskunftei auf ihre datenschutzrechtliche Zulässigkeit hin zu untersuchen.

Wie sich aus den bei uns eingereichten Unterlagen ergab, lag dieser Prüfbitte folgender Sachverhalt zugrunde: Seit mehreren Jahren schuldete der Betroffene einem Kreditinstitut einen mehrstelligen Betrag. Das Kreditinstitut hatte schließlich ein Inkassounternehmen mit der Einziehung dieser Forderung gegenüber dem Betroffenen beauftragt. Da der Betroffene zur Zahlung seiner Schulden willens, aber lediglich zu einer Abzahlung in kleinen Raten imstande war, hatte das Inkassounternehmen mit dem Betroffenen eine Vereinbarung zur schrittweisen Begleichung der Schuld getroffen. Der Forderungsbetrag war unter deutlicher Reduzierung der ursprünglichen Schuldsumme auf einen neuen Betrag festgeschrieben worden, Schuldzinsen sollten auf diesen Betrag nicht (mehr) anfallen. Im Gegenzug sollte der Betroffene den neu festgelegten Schuldbetrag in kleinen Raten monatlich zu einem bestimmten Termin abtragen. Bei einem Verzug mit einer Ratenzahlung sollte diese Vereinbarung hinfällig sein. Entsprechend dieser Vereinbarung überwies der Betroffene seit mehreren Jahren monatlich seine Raten. Er hatte auf diese Weise immerhin schon etwa ein Zehntel der neu festgeschriebenen Schuld getilgt. Das Inkassounternehmen hatte dem Betroffenen die Gesamtsumme seiner bisherigen Ratenzahlungen und die noch verbleibende Restschuld – ausgehend vom neufestgelegten Schuldbetrag – im Jahr 2015 schriftlich bestätigt.

Der Betroffene erbat kurz nach dieser Mitteilung bei einer bundesweit tätigen Wirtschaftsauskunftei eine datenschutzrechtliche Eigenauskunft zu seiner Person. Als ihm

diese vorlag, musste er zu seinem Erschrecken feststellen, dass das Inkassounternehmen bei der Wirtschaftsauskunftei lediglich den ursprünglich geschuldeten Betrag gemeldet hatte und seitdem monatlich einen Anstieg der Schuldsumme nachmeldete. Hingegen war aus der Datenbestandsübersicht der Auskunftei weder die getroffene Vereinbarung noch der bereits mehrjährige monatliche Ratenabtrag der Schuld durch den Betroffenen ersichtlich.

Wir konnten nicht nachvollziehen, weshalb das Inkassounternehmen nicht den neu festgelegten Forderungsbetrag bei der Auskunftei gemeldet und jene über den monatlichen Schuldabtrag informiert hatte. Denn die einschlägige Vorschrift des Bundesdatenschutzgesetzes verpflichtet Stellen, die zulässigerweise eine ausstehende Forderung bei einer Auskunftei in den Datenbestand zu einer Person gemeldet haben, nachträgliche Änderungen der Tatsachen innerhalb eines Monats nach Kenntnis an die Auskunftei weiterzugeben. Im Übrigen dürfen stets nur richtige Daten übermittelt werden.

Zwecks näherer Aufklärung und datenschutzrechtlicher Nachprüfung baten wir das Inkassounternehmen daher um schriftliche Erläuterung.

Das Inkassounternehmen erklärte uns daraufhin, dass zwar eine Festschreibung der einzuziehenden Forderung auf einen neuen Betrag erfolgt und ein monatlicher Ratenabtrag in bestimmter Höhe mit dem Betroffenen vereinbart worden sei. Dieser Vergleich sei aber "aufschiebend bedingt" abgeschlossen worden, werde also erst dann rechtlich zur Gänze wirksam, wenn der Betroffene mit seinen Raten die neu bestimmte Schuldsumme tatsächlich abgezahlt habe. Bis dahin sei es richtig, dass die Auskunftei weiter die ursprüngliche Schuldsumme im Datenbestand führe. Das Anwachsen der Schuldsumme im Datenbestand der Auskunftei beruhe im Übrigen darauf, dass für die ursprünglich geschuldete Forderung Schuldzinsen anfielen und die monatliche Ratenzahlung geringer sei, als der monatliche Schuldzinsanfall.

Diese Ansicht teilten wir nicht. Wir gingen aufgrund der eindeutigen Erklärungen beider Seiten bei der Vereinbarung vielmehr davon aus, dass das Inkassounternehmen und der Betroffene einen Vergleich mit einem üblichen Regelungsgehalt geschlossen hatten, nämlich Eintritt der Rechtsfolge "Reduzierung und Neufestlegung der Forderung ohne Schuldverzinsung" mit sofortiger Wirkung und Fortbestand dieser Rechtsfolge solange der Betroffene vereinbarungsgemäß pünktlich seine Ratenzahlungen erbringt (zivilrechtlich: "auflösende Bedingung"). Das Inkassounternehmen hätte also nach der Annahme des Vergleichsangebots durch den Betroffenen bei der Auskunftei für eine Änderung der gelisteten Forderung auf die Vergleichssumme sorgen und den monatlichen Schuldabtrag melden müssen.

Da zwischenzeitlich auch die Wirtschaftsauskunftei auf mehrfache Intervention des Betroffenen eine eigene Überprüfung eingeleitet und bereits den Forderungsstand im Sinne des Betroffenen berichtigt hatte, konnten wir uns darauf beschränken, von dem

Inkassounternehmen eine ausdrückliche Bestätigung der weiteren Beachtung und Umsetzung unserer Rechtsauffassung einzuholen. Da das Inkassounternehmen dies letztlich zusagte, bedurfte es keiner Anordnung zur Durchsetzung des Rechts des Betroffenen.

13.2 Anspruch auf Unterlassung einer Scorewertauskunft

Scoringverfahren bei Wirtschaftsauskunfteien bergen massive Risiken für das Persönlichkeitsrecht und die wirtschaftliche Betätigungsfreiheit Betroffener. Dies beruht nicht zuletzt darauf, dass Scorewerte – anders als vielfach angenommen – tatsächlich nicht das wirtschaftliche Verhalten einer Person bewerten, sondern vielmehr nur Ausdruck des statistischen finanziellen Durchschnittsverhaltens einer mehr oder weniger vergleichbaren und mehr oder weniger repräsentativen Personengruppe sind (zur Problematik siehe bereits 37. Jahresbericht, Ziffer 14.1).

Eine im Berichtszeitraum ergangene beachtenswerte Entscheidung des Oberlandesgerichts Frankfurt stellt nunmehr klar, dass auch bei der Erstellung (und Beauskunftung) von Scorewerten durch Wirtschaftsauskunfteien Anforderungen an die Qualität und Quantität des zugrundeliegenden Datenmaterials zu beachten sind. Mit rechtskräftigem Urteil vom 7. April 2015 untersagte das Gericht einer Wirtschaftsauskunftei die Beauskunftung eines schlechten Scorewertes zu einem Einzelgewerbetreibenden, da der Scorewert keine ausreichende Tatsachenbasis hatte. Wegen der grundsätzlichen Erwägungen des Gerichts dürfte sich diese Entscheidung auf viele Fälle der Erstellung von Scorewerten zu natürlichen Personen übertragen lassen. Denn in der Praxis verfügen Wirtschaftsauskunfteien oftmals nicht über ausreichende Informationsgrundlagen zum Wirtschaftsverhalten der zu bewertenden Person. Leider hindert dies aber allzu oft Wirtschaftsauskunfteien nicht daran, Scorewertauskünfte zu erteilen.

In dem Sachverhalt, der durch das Oberlandesgericht entschieden wurde, hatte ein Einzelgewerbetreibender seitens eines Lieferanten die Mitteilung erhalten, er könne lediglich noch gegen Vorauszahlung Waren geliefert bekommen. Grund hierfür sei eine schlechte Bonitätsauskunft einer Wirtschaftsauskunftei. Der betroffene Gewerbetreibende wandte sich daraufhin an die Auskunftei und erbat dort auf Grundlage seines datenschutzrechtlichen Auskunftsanspruchs eine Mitteilung über die dort zu seiner Person gespeicherten Daten, insbesondere auch den Scorewert und die zugrundeliegenden Daten. Er stellte fest, dass dort kaum bonitätsrelevante Daten zu seiner Person gespeichert waren, einige Angaben zudem fehlerhaft waren. Er nahm daher die Auskunftei klageweise auf Unterlassung in Anspruch.

Nach eigenen Angaben erstellt die Wirtschaftsauskunftei ihren Scorewert aufgrund einer umfassenden Verwertung verschiedenster Wirtschaftsinformationen (Branche, Rechtsform und so weiter). Das Oberlandesgericht Frankfurt stellte in zweiter Gerichtsinstanz fest, dass

der schlechte Scorewert letztendlich im Wesentlichen darauf beruhte, dass der Betroffene Einzelkaufmann war. Das Gericht kam daher zu dem Schluss, dass die maßgebliche Verwertung lediglich eines Einzelfaktors offensichtlich nicht den Anforderungen eines wissenschaftlich anerkannten mathematisch-statistischen Berechnungsverfahrens genügen kann. Dies allerdings schreibt das Bundesdatenschutzgesetz als Voraussetzung einer Scorewertberechnung vor.

Die Wirtschaftsauskunftei hatte vergeblich damit zu argumentieren versucht, dass ihre Bewertung ein Werturteil sei. Diese Meinungsäußerung entziehe sich daher einer Bewertung als "wahr" oder "falsch", was der Bundesgerichtshof so entschieden habe. Das Oberlandesgericht wies diese Argumentation zurück. Zwar habe der Bundesgerichtshof im Allgemeinen Scorewertauskünfte als Meinungsäußerungen gewertet, jedoch im Urteil vom 22. Februar 2011 festgehalten, dass diese auf einer zutreffenden Tatsachengrundlage beruhen müssten. Die Entscheidung der Wirtschaftsauskunftei habe aber offensichtlich gerade keine ausreichende sachliche Basis gehabt.

13.3 Unzulässige Teilnahme bremischer Kreditinstitute an auskunfteiengeführten Betrugspräventionsdatenbanken

Im Berichtsjahr gingen zwei Wirtschaftsauskunfteien mit konkurrierenden Angeboten einer "Betrugspräventionsdatenbank" (Fraud-Prevention-Pools) an den Markt. Beide Datenbanksysteme sind letztlich darauf angelegt, Kreditinstituten und Finanzdienstleistungsinstituten untereinander den Austausch bestimmter Informationen zu solchen Personen zu ermöglichen, die sie eines Betruges oder einer sonstigen Vermögensstraftat verdächtigen.

Indes hat der Gesetzgeber für den zwischen Instituten erfolgenden Austausch von mehr oder weniger vagen beziehungsweise mehr oder weniger spekulativen Annahmen über strafbare, institutsvermögensgefährdende Handlungen eines (potentiellen) Kunden im Kreditwesengesetz Regelungen getroffen. In § 25h Absatz 3 heißt es:

"…[4]Institute dürfen im Einzelfall einander Informationen im Rahmen der Erfüllung ihrer Untersuchungspflicht nach Satz 1 übermitteln, wenn es sich um einen in Bezug auf Geldwäsche, Terrorismusfinanzierung oder einer sonstigen Straftat auffälligen oder ungewöhnlichen Sachverhalt handelt und tatsächliche Anhaltspunkte dafür vorliegen, dass der Empfänger der Information diese für die Beurteilung der Frage benötigt, ob der Sachverhalt gemäß § 11 des Geldwäschegesetzes anzuzeigen oder eine Strafanzeige gemäß § 158 der Strafprozessordnung zu erstatten ist. [5]Der Empfänger darf die Information ausschließlich zum Zweck der Verhinderung der Geldwäsche, der Terrorismusfinanzierung oder sonstiger strafbarer Handlungen und nur unter den durch das übermittelnde Institut vorgegebenen Bedingungen verwenden."

Diese Vorschrift stellt nach unserer Rechtsansicht eine für den Austausch derartiger Informationen unter Instituten spezielle und abschließende Regelung dar. Eine Teilnahme von Instituten an einem mit demselben Zweck durch eine Wirtschaftsauskunftei betriebenen Betrugspräventionsdatenbanksystem, das sich lediglich auf die allgemeinen datenschutzrechtlichen Erlaubnisnormen des Bundesdatenschutzgesetzes stützt, halten wir daher für unzulässig.

Nach dem klaren Wortlaut des § 25h Absatz 3 Satz 4 Kreditwesengesetz darf die Übermittlung der aus institutsinternen Sicherungsmaßnahmen gewonnenen Information(en) *ausschließlich von Institut zu Institut* erfolgen ("Institute…einander…"). Auch in der Begründung des Gesetzesentwurfs wird allein von "Informationsaustausch und Informationszusammenführung bei Instituten" gesprochen. Ferner richten sich die Einzelsätze des Absatzes 3 sowie die weiteren Absätze der Vorschrift ausschließlich an Institute als Normadressaten; allein Instituten hat der Gesetzgeber also spezielle Datenverarbeitungsbefugnisse im Hinblick auf mehr oder weniger vage Straftatverdächtigungen eingeräumt, nicht aber dritten Stellen ohne Institutseigenschaft. Hintergrund der Regelung ist es allein, einem – ebenfalls zu internen Sicherungsmaßnahmen nach dem Kreditwesengesetz verpflichteten – Institut frühzeitig die Kenntnis eines bei einem anderen Institut aufgekommenen Verdachtsmoments hinsichtlich eines mutmaßlich strafbaren, institutsvermögensschädigenden Verhaltens zu ermöglichen. Damit soll sichergestellt werden, dass das informationsempfangende Institut bei einer Geschäftsanbahnung oder bereits einer Geschäftsbeziehung mit derselben verdächtigten Person eigene Vermögensgefährdungen überprüfen und gegebenenfalls eine Strafanzeige erstatten oder seine Meldepflicht nach dem Geldwäschegesetz erfüllen kann. Im Übrigen darf der Informationsempfänger die Information(en) über auffällige, ungewöhnliche vermögensgefährdende Verhaltensweisen nach dem eindeutigen Wortlaut des Kreditwesengesetzes ausschließlich zum Zweck der Verhinderung von Geldwäsche, der Verhinderung von Terrorismusfinanzierung oder der Verhinderung von institutsvermögensgefährdenden Straftaten verwenden. Es besteht also von Gesetzes wegen eine strikte Verwendungszweckbindung für die übermittelten Informationen. Bei einer Weitergabe derartiger Informationen an eine dritte Stelle, die kein Institut ist, damit diese geschäftsmäßig die Information in einer Zentraldatenbank auf unbestimmte Zeit speichert und bei Abruf kostenpflichtig in einer Vielzahl von Fällen übermittelt, verfolgt die dritte Stelle als Informationsempfänger offensichtlich einen hiervon abweichenden, eigenständigen (Geschäfts-)Zweck. Dies ist mit der ausschließlichen Informationsverwendungs-Zweckbindung unvereinbar.

Sodann ist dem Wortlaut der Vorschrift unmissverständlich zu entnehmen, dass der Austausch einschlägiger Informationen von Institut zu Institut *ausschließlich im Einzelfall* erfolgen darf. Im Einzelfall muss das informationsweitergabewillige Institut sodann

tatsächliche Anhaltspunkte dafür haben, dass auf Seiten des potentiellen Empfängerinstituts ein entsprechender Informationsbedarf besteht, weil dort die Abgabe einer eigenen Verdachtsmeldung nach dem Geldwäschegesetz oder die Erstattung einer eigenen Strafanzeige zu prüfen ist. Ein solcher Anhaltspunkt könnte sich für ein Institut zum Beispiel daraus ergeben, dass es für eine verdächtigte Person ein Konto führt und über die Kontobewegungen Kenntnis davon erhält, dass die verdächtigte Person bei einem anderen Institut ein weiteres Konto besitzt. Bei einer vorsorglichen generellen Informationsweitergabe an eine institutsextern geführte zentrale Datenbank, die allein aufgrund der abstrakten Vermutung erfolgte, dass irgendein anderes Institut auch in seinem Geschäftsbereich die Information schon irgendwann einmal benötigen könne, könnte offenkundig nicht von tatsächlichen Anhaltspunkten im Einzelfall für einen Informationsbedarf gesprochen werden.

Der § 25h Absatz 3 Satz 4 Kreditwesengesetz ist auch eine abschließende Bestimmung. Das heißt, im Regelungsbereich der Vorschrift ist ein Ausweichen der Institute auf die allgemeine datenschutzrechtliche Befugnisnorm des § 28 Bundesdatenschutzgesetz ausgeschlossen.

Dies ergibt sich bereits aus Sinn und Zweck der Vorschrift in Verbindung mit ihrer Entstehungsgeschichte: Institute sollten, abgesehen vom Informationsaustausch betreffend Geldwäsche und Terrorismusfinanzierung (= Anwendungsbereich des Geldwäschegesetzes), auch Informationen zu vermögensgefährdenden Straftaten in datenschutzrechtlich einwandfreier Art und Weise austauschen können. Der Gesetzgeber hielt hierfür die Schaffung einer besonderen Vorschrift für notwendig. Er ging also davon aus, dass die bestehenden allgemeinen datenschutzrechtlichen Befugnisnormen einen solchen Informationsaustausch nicht legitimieren. Wäre ein entsprechender Informationsaustausch auch außerhalb der Ermächtigung des § 25h Absatz 3 Satz 4 Kreditwesengesetz möglich, liefe die Norm mit ihren speziellen Einschränkungen für den Datenaustausch im Übrigen praktisch leer, was offensichtlich der gesetzgeberischen Vorstellung zuwider liefe ("Gesetzesumgehung"). Zudem gelangten bei Einbindung institutsexterner Dritter (etwa Auskunfteien) in den Informationsaustausch solche Informationen, die allein präventiv im Interesse der Stabilität und Seriosität des Kreditwesens erhoben werden dürfen, die also exklusiv dem Institutssektor zugeordnet sind und die daher einer strikten Verwendungszweckbindung unterliegen (siehe § 25h Absatz 3 Satz 5 Kreditwesengesetz), unter Verlust ihres Erhebungskontexts aus dem Kreditwesenssektor.

Auch die Rechtssystematik zeigt, dass es sich bei § 25h Absatz 3 Satz 4 Kreditwesengesetz um eine die allgemeine datenschutzrechtliche Norm des § 28 Absatz 2 Ziffer 2a Bundesdatenschutzgesetz verdrängende Spezialvorschrift handelt. Denn ohne die besondere Verarbeitungsermächtigung in § 25h Absatz 3 Kreditwesengesetz griffe angesichts der vagen Mutmaßungsqualität der Information(en) zu ungewöhnlichen

beziehungsweise auffälligen, institutsvermögensgefährdenden strafbaren Verhaltensweisen häufig die allgemeine datenschutzrechtliche Vorschrift des § 35 Absatz 2 Satz 2 Ziffer 2 Bundesdatenschutzgesetz. Nach dieser sind personenbezogene Daten unmittelbar zu löschen, wenn es sich um Informationen zu strafbaren Handlungen handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann.

Für eine spezielle Ermächtigung (mit Sperrwirkung) spricht sodann auch ein Blick auf die europarechtlichen Vorgaben zur Ausgestaltung nationalen Datenschutzrechts: Artikel 8 Absatz 5 Satz 1 der Datenschutzrichtlinie legt deutliche Restriktionen für die Zulässigkeit der Verarbeitung von Informationen zu Straftaten durch private Stellen/Personen fest (= behördliche Aufsicht oder Vorschriften mit angemessenen Garantien). "Angemessene Garantien" im Sinne dieses Artikels enthält insbesondere § 28 Absatz 2 Ziffer 2a Bundesdatenschutzgesetz offensichtlich nicht.

Nicht zuletzt könnten Institutsmitarbeiter durch die Verbreitung von vagen Straftatverdächtigungen – ohne entsprechende besondere Erlaubnisnorm wie hier § 25h Absatz 3 Kreditwesengesetz – unter Umständen selbst eine Straftat begehen (§§ 164, 186, 190 Strafgesetzbuch).

Wir haben vor diesem Hintergrund durch Rundschreiben die Institute in unserem Aufsichtsbereich auf die Unzulässigkeit einer Teilnahme an auskunfteigetragenen Betrugspräventionsdatenbanken hingewiesen. Bei einer Nachprüfung im laufenden Berichtsjahr konnten wir kein Institut aus unserem Aufsichtsbereich als Teilnehmer feststellen. Sollten wir jedoch in unserem Aufsichtsbereich eine Teilnahme feststellen, würden wir aufsichtsbehördliche Schritte prüfen, um Personen vor einer – auch mit der verfassungsrechtlichen Unschuldsvermutung unvereinbaren – Diskreditierung durch eine Speicherung in einer zentralen "Straftatverdächtigungsdatenbank" in privater, gewinnorientierter Hand zu bewahren.

13.4 Speicherung vertraulicher Daten trotz Nichtzustandekommens eines Vertrages

Ein Versicherungsvertreter hatte einen Facharzt aufgesucht, vertrauliche Praxisdaten wie Jahresumsatz sowie Mitarbeiterzahl erfragt und in seinem Laptop gespeichert. Da ein Vertrag über eine Rechtsschutzversicherung nicht zustande kam, bat der Arzt erfolglos um die Bestätigung, dass die Daten gelöscht und nicht weitergegeben worden seien.

Der Versicherungsvertreter erteilte uns dann die Auskunft, er habe keinerlei Daten an die Hauptzentrale seiner Versicherung weitergegeben. Jahresumsatz, Mitarbeiterzahl und weitere Daten seien lediglich zur Berechnung des Versicherungsvorschlags genutzt und danach gelöscht worden. Dem Kunden gehe ein entsprechendes Bestätigungsschreiben zu.

13.5 Fotografien von Studienausweisen und Personalausweisen mit privaten Mobiltelefonen

Vertreter einer Versicherung, mit Geschäftsstelle in Bremen, schlossen an prominent platzierten Aktionsständen auf dem Campus der Universität Bremen mit Studierenden Giroverträge ab. Dabei bestanden die Vertreter auf Fotografien der Studienausweise und Personalausweise, ohne den Zweck dafür befriedigend zu erläutern. Diese Fotografien wurden mit privaten Mobiltelefonen digital angefertigt. Auf Nachfrage hatten die Vertreter erklärt, die Fotos würden später in der Zentrale ausgedruckt und von den Mobiltelefonen gelöscht.

Zunächst begründete die Versicherung die Fotografien mit entsprechenden Vorschriften im Geldwäschegesetz zur Legitimationsprüfung. Daraufhin erklärten wir, dass diese Vorschriften nur regeln, dass die Ausweisdaten aufgezeichnet werden.

Die betreffenden Vorschriften erlauben die Anfertigung von Kopien der Ausweise nicht. Die Versicherung hielt die rechtliche Lage hinsichtlich der Reproduktionsformen zur Erfüllung geldwäscherechtlicher Verpflichtungen für nicht abschließend geklärt. Das Anfertigen einer digitalen Bilddatei bei der Versicherung zur Erfüllung geldwäscherechtlicher Verpflichtungen insbesondere zur Vermeidung von Restrisiken sei aber weder gewünscht noch grundsätzlich Praxis. Auch das Fotografieren der Studentenausweise und insbesondere etwaige Fotos der Betroffenen seien nicht erforderlich zur Gewährung eines Studentenrabattes. Die Geschäftsstelle Bremen bestätigte inzwischen, dass alle angefertigten digitalen Bilddateien, auch die von den privaten Mobiltelefonen, gelöscht worden seien.

13.6 Keine gesetzlichen Verbesserungsvorschläge der Bundesregierung trotz aufgezeigten Reformbedarfs durch Scoring-Studie

Bereits in unserem letzten Jahresbericht hatten wir ausführlich über die persönlichkeitsrechtliche Problematik der Scoringverfahren bei Wirtschaftsauskunfteien berichtet (siehe hierzu 37. Jahresbericht, Ziffer 14.1).

Die Bundesregierung hatte bereits Mitte des Jahres 2013 eine Studie zum Scoring in Auftrag gegeben. In dieser Studie sollte unter anderem auch die Praxistauglichkeit und Praxisbewährung der 2010 neu geschaffenen Regelung des § 28b Bundesdatenschutzgesetz zum Scoring untersucht werden. Das federführende Bundesministerium der Justiz und für Verbraucherschutz veröffentlichte schließlich im Dezember 2014 die Studie. Der dortige Parlamentarische Staatssekretär äußerte sich bei der Vorstellung der Studie wie folgt: *"Die Studie hat einmal mehr bestätigt, wie wichtig ein klarer Rechtsrahmen für das Scoring ist. Wir nehmen die Ergebnisse der Studie ernst, denn das Scoring ist für Verbraucherinnen und Verbraucher von fundamentaler Bedeutung. Es*

darf nicht sein, dass jemand zu Unrecht ein Darlehen nicht erhält, eine Wohnung nicht anmieten kann oder im Versandhandel nicht auf Rechnung bestellen kann."

Bislang sind greifbare Umsetzungsergebnisse in Form gesetzlicher Nachbesserungsvorschläge, insbesondere bei der defizitären Regelung des § 28b Bundesdatenschutzgesetz, nicht ersichtlich.

Zur Rechtfertigung der gesetzgeberischen Untätigkeit im Datenschutzrecht wird derzeit häufig auf die europäischen Verhandlungen zur Schaffung einer europaweit einheitlichen Datenschutzgrundverordnung verwiesen. Bis zu deren Inkrafttreten kann es allerdings gut und gerne noch mindestens zwei Jahre dauern (siehe hierzu Ziffer 15.1 dieses Berichts). Sofern der Gesetzgeber tatsächlich bis dahin nicht reagiert, stehen diejenigen, denen in der Zwischenzeit aufgrund einer mehr oder weniger schlechten Scorewert-Berechnung einer Auskunftei zum Beispiel seitens eines scorewertabfragenden Kreditinstituts ein Darlehen oder seitens einer beziehungsweise eines – unzulässigerweise eine Bonitätsabfrage durchführenden – Vermieterin beziehungsweise Vermieters eine Wohnung versagt wird, im Regen.

13.7 Kennzeichnung von Scorewerten als Schätzdaten

Das Bundesdatenschutzgesetz verpflichtet seit einer Gesetzesnovellierung vor einigen Jahren datenverarbeitende Stellen zur deutlichen Kennzeichnung von solchen Daten, die lediglich geschätzt sind. Hiermit soll sichergestellt werden, dass geschätzte Angaben seitens eines Datenempfängers nicht als Tatsachen missverstanden werden. Besondere Relevanz besitzt die Vorschrift für Wirtschaftsauskunfteien.

Im Rahmen eines Prüfverfahrens hatten wir bei einer in unserem Aufsichtsbereich tätigen Auskunftei festgestellt, dass diese ihre Scorewerte nicht als ihre unternehmenseigene Schätzung beziehungsweise Einschätzung der Bonität der bewerteten Person kennzeichnete. Vielmehr suggerierte sie auf verschiedene Weise, es handele sich quasi um eine objektive Zahlungsfähigkeitsfeststellung zu der bewerteten Person. Mehrfach wiesen wir die Auskunftei nachdrücklich auf die Kennzeichnungspflicht auch bei Scorewerten hin und forderten eine Umsetzung, aber ohne Erfolg. Wir verpflichteten daher schließlich die Auskunftei im Wege einer Anordnung, künftig ihre mathematisch-statistischen Berechnungswerte (Scorewerte) zur Bewertung der Bonität von Personen als Schätzwerte zu kennzeichnen.

Der Gesetzgeber wollte ausweislich der Gesetzesbegründung unter geschätzten Daten insbesondere (auch) "Erfahrungswerte" verstanden wissen. Nun sind Erfahrungswerte nichts anderes als Erkenntnisse, die typischerweise aufgrund längerfristiger, bestätigender Analyse von Umständen gewonnen wurden und dazu dienen, künftige Gegebenheiten zu antizipieren. Art und Weise des Zustandekommens eines Erfahrungswerts sind für die

Einstufung einer Erkenntnis als Erfahrungswert ohne Bedeutung. Scorewerte sind nach ihrem Zustandekommen wie auch ihrem richtig verstandenen Aussagegehalt letztlich gerade solche Erfahrungswerte. Denn sie stellen im Ergebnis lediglich eine aus der mathematisch-statistischen Auswertung einer Vielzahl von historischen Zahlungserfahrungen bei Einzelpersonen gewonnene Information darüber dar, wie positiv oder negativ in der Vergangenheit die Erfahrungen mit der Zahlungsfähigkeit einer – dem zu Bewertenden aufgrund mehr oder weniger übereinstimmender Ausgangsparameter vergleichbaren – Gruppe von Personen waren. Diese historischen, der Auskunftei vergleichbar erscheinenden Erfahrungswerte, werden auf die zu bewertenden Personen übertragen und sollen bei diesen nun als Prognose ihrer individuellen (künftigen) Zahlungsfähigkeitsentwicklung dienen.

Es war außerdem gerade Sinn und Zweck der Einführung der gesetzlichen Kennzeichnungspflicht für Schätzwerte, jeder Empfängerin oder jedem Empfänger übermittelter geschätzter Angaben von vornherein unzweifelhaft klar zu machen, dass ihr oder ihm keine unumstößlichen Umstände mitgeteilt worden sind, sondern lediglich subjektive und daher hinterfragungswürdige Einschätzungen. Gerade bei Scorewerten greift dieser Schutzzweck. Denn statistische Zahlen(-werte) umgibt regelmäßig ein Schein der Objektivität und Faktizität. Dieser Anschein wird zudem dadurch verstärkt, dass Auskunfteien das Zustandekommen der Scorewerte regelmäßig explizit mit der Anwendung eines "wissenschaftlich anerkannten mathematisch-statistischen Verfahrens" bewerben.

Die Auskunftei akzeptierte unsere Anordnung nicht und erhob Klage. Ende des Berichtsjahres fand die mündliche Verhandlung vor dem Verwaltungsgericht statt. Den Fragen und Hinweisen der Richter in der mündlichen Verhandlung war zu entnehmen, dass das Gericht grundsätzlich unsere, der Anordnung zugrunde liegende Rechtsauffassung für zutreffend erachtete. Die klagende Auskunftei bot schließlich zwecks unmittelbarer Beendigung des Rechtsstreits ohne Urteil den Abschluss eines Prozessvergleichs an. Nach kurzen Verhandlungen über die inhaltliche Ausgestaltung des Vergleichs nahmen wir das Angebot an, da wir hiermit ausreichend sichergestellt sehen, dass die Auskunftei zukünftig ihre Scorewerte als ihre subjektive Einschätzung zur Bonität der bewerteten Person kennzeichnet.

Wir betrachten es als einen großen Gewinn für Betroffene, dass künftig jeder Empfängerin und jedem Empfänger einer Bonitätsauskunft eindeutig vor Augen geführt ist, dass die mitgeteilten Scorewerte zur abgefragten Person nicht deren tatsächliche – etwa auf Monatseinnahmen-Monatsausgaben-Vergleich basierende – individuelle Zahlungsfähigkeit wiedergeben, sondern vielmehr eine rein subjektive Einschätzung der Auskunftei auf der Grundlage durchschnittlicher Vergleichszahlen darstellen.

14. Weitere Wirtschaftsunternehmen und Vereine

14.1 E-Mail-Versand mit offenem E-Mail-Adressverteiler

Auch in diesem Berichtsjahr erreichten uns wieder mehrere Beschwerden darüber, dass Werbemails beziehungsweise Informationsmails privater Einrichtungen unter Nutzung des Adressverteilers "An" beziehungsweise "CC" an eine Vielzahl von Empfängerinnen und Empfängern versandt worden waren. Auf diese Weise erhielten sie nicht nur den eigentlichen Nachrichteninhalt, sondern über das einsehbare Adressfeld – im Unterschied zum verdeckten Adressfeld "BCC" – auch alle personenbezogenen E-Mail-Adressen (vergleiche hierzu 37. Jahresbericht, Ziffer 16.4).

Befinden sich im Adressverteiler personifizierte E-Mail-Adressen, also E-Mail-Adressen, die aus dem Namen, gegebenenfalls Vornamen oder Vornamenskürzel, oftmals noch der Arbeitsstelle einer Person zusammengesetzt und daher den Betroffenen zuzuordnen sind, greifen grundsätzlich die Regelungen des Bundesdatenschutzgesetzes. Für die Übermittlung einer personifizierten E-Mail-Adresse an Dritte bedarf es also von Rechts wegen entweder einer Einwilligung der jeweiligen Person oder zumindest einer gesetzlichen Erlaubnisnorm. Fehlt eine solche Befugnis, kann dies als Übermittlung nicht allgemein zugänglicher personenbezogener Daten einen Bußgeldtatbestand erfüllen und mit einer kostenpflichtigen Verwarnung oder sogar einem Bußgeld geahndet werden.

In den Beschwerdefällen hatten die Absender der Massen-E-Mails selbstverständlich keine Einwilligung aller Betroffenen in die Weitergabe der E-Mail-Adresse an alle Mitempfängerinnen und Mitempfänger der Massen-E-Mail. Ebenso wenig erlaubten die anwendbaren Normen des Bundesdatenschutzgesetzes eine solche massenhafte Verteilung der jeweiligen E-Mail-Adressen.

Da sich die Absender der Massen-E-Mails in allen Fällen bereits nach unserem schriftlichen Hinweis unmittelbar einsichtig zeigten, die Unachtsamkeit bedauerten und sich bemühten, durch rasche Information der Mitarbeiterinnen und Mitarbeiter eine Fehlerwiederholung nach besten Kräften zu vermeiden, ließen wir es in den Beschwerdefällen mit einer formlosen Beanstandung bewenden.

14.2 Rechtswidriges Verlangen der Vorlage von Personalausweiskopien

Auch in diesem Berichtsjahr erreichten uns wieder etliche Beschwerden darüber, dass – in unterschiedlichsten Situationen – Personalausweisdaten erhoben und gespeichert worden seien, ohne dass es hierfür aus Sicht der Ausweisinhaber/Betroffenen einen nachvollziehbaren Grund gab.

So hatte sich ein Betroffener brieflich unter Mitteilung der Angaben Name, Vorname und Anschrift an eine Freizeiteinrichtung gewandt und dort um Erteilung einer Eigendatenauskunft nach § 34 Bundesdatenschutzgesetz gebeten. Die Freizeiteinrichtung antwortete daraufhin, dass eine Bearbeitung der Anfrage von der Vorlage einer beidseitigen, gut lesbaren Kopie seines Personalausweises abhängig sei. Der Auskunftssuchende entgegnete, dass das Bundesdatenschutzgesetz den Eigendatenauskunftsanspruch nicht an die vorherige Vorlage einer Ausweiskopie binde. Als dieser Hinweis ohne Resonanz blieb, bat der Auskunftssuchende uns um Hilfe.

Wir überprüften die Angelegenheit mit folgendem Ergebnis: Die Stelle hatte neben Name und Vorname des Betroffenen eine abweichende (= also eventuell frühere) Wohnstraßenanschrift gespeichert. Aufgrund der Divergenz in den Angaben zur Wohnanschrift war also grundsätzlich eine weitere Verifikation der Identität des Auskunftssuchenden geboten. Denn unbefugte Datenübermittlungen an einen Dritten sind verboten und – im Falle von mindestens fahrlässigem Verhalten (= Außerachtlassung der verkehrserforderlichen Sorgfalt) – auch bußgeldbewehrt. Es ist also selbstverständlich Obliegenheit einer datenverarbeitenden Stelle, sich im Rahmen der verkehrsüblichen Sorgfaltsanforderungen der Identität einer auskunftserbittenden Person vor Herausgabe von personenbezogenen Daten an sie zu vergewissern. Hat eine datenverarbeitende Stelle aber die verkehrserforderliche Sorgfalt bei der Identitätsnachprüfung eines Auskunftssuchenden eingehalten, kann ihr selbst dann, wenn sich im Nachgang eine Fehlübermittlung herausstellt, kein Schuldvorwurf gemacht werden. Ihr droht in diesem Fall mangels Vorwerfbarkeit selbstverständlich auch keine Bußgeldsanktion. Die verkehrserforderliche Sorgfalt setzt aber selbstverständlich keine Erhebung von x-beliebigen Angaben voraus, welche zur Identifizierung nicht geeignet oder nicht erforderlich sind.

Die Freizeiteinrichtung hatte neben der – abweichenden – Wohnanschrift zusätzlich noch Geburtsdatum und Geburtsort einer namensgleichen Person gespeichert. Sie hätte daher schlicht diese Angaben (Geburtsdatum, Geburtsort, frühere Wohnstraßenanschrift) zur Vergewisserung der Übereinstimmung der Identität des Anfragenden und der Person, deren Daten sie gespeichert hatte, nutzen können. Eine schlichte Nachfrage nach diesen weiteren Identitätsangaben beim Auskunftssuchenden hätte genügt. Wären im Anschluss aufgrund besonderer, zu dokumentierender Umstände begründete Identitätszweifel geblieben, so hätte die Freizeiteinrichtung zum Beispiel über den Versand eines "Einschreibens eigenhändig" (das nur persönlich gegen Unterschrift ausgehändigt wird), eine Melderegisterauskunftsanfrage, eine Bitte um Vorlage einer Meldebestätigung, einen Versuch telefonischer Kontaktaufnahme oder weitere Maßnahmen zum Ausschluss einer Personenverwechslung nachdenken können.

Hingegen konnte die Zusendung einer einfachen, nicht fälschungssicheren Kopie eines Personalausweises mit einem x-beliebigen Lichtbild und x-beliebigen weiteren Personalausweisdaten der Freizeiteinrichtung bei der Verifizierung nicht weiterhelfen. Denn es fehlte insoweit schon eine Abgleichmöglichkeit der Personalausweisinformationen mit "Gegeninformationen" im eigenen Datenbestand. Mit Entgegennahme einer beidseitigen Kopie des Personalausweises hätte die Freizeiteinrichtung zudem zusätzlich Kenntnis über Personengröße, Augenfarbe, Staatsangehörigkeit, (gegebenenfalls) Künstlername sowie daneben Ausweisnummer, Gültigkeitsdatum, Ausstellungsdatum, Zugangsnummer (bei einem neuen Personalausweis) erlangt. Die Kenntnis dieser Angaben war aber – im Unterschied zu Kenntnis des Namens, Vornamens, der Anschrift, des Geburtsdatums und Geburtsorts – für Identifizierungszwecke nicht nötig. Nicht erforderliche Datenerhebungen haben nach dem Bundesdatenschutzgesetz zu unterbleiben. Dies ergibt sich aus dem Grundsatz der Erforderlichkeit der Erhebung eines jeden personenbezogenen Datums und dem generellen Gebot der Datensparsamkeit.

Die Aufforderung, eine gut leserliche, beidseitige Ausweiskopie vorzulegen, war also bereits insoweit mit dem Bundesdatenschutzgesetz unvereinbar.

Folgende weitere Aspekte waren – und sind generell – zu bedenken:

- Einfache (im Unterschied zu beglaubigten) Kopien eines Personalausweises erwecken zwar den Anschein, Abbild des Originals zu sein. Die inhaltliche Unverfälschtheit kann aber in keiner Weise festgestellt werden. Mit den heutigen technischen Möglichkeiten sind Kopien leicht zu manipulieren. Die Zusendung einer einfachen Kopie eines amtlichen Ausweises stellt daher im Rechtsverkehr kein anerkanntes Legitimationsmittel dar.
- Nach § 14 Personalausweisgesetz dürfen nicht öffentliche Stellen personenbezogene Personalausweisdaten (nur) nach Maßgabe der §§ 18 bis 20 Personalausweisgesetz erheben und verwenden, vorbehaltlich expliziter spezialgesetzlicher Ausnahmevorschriften. Eine Legitimationsvariante "Vorlage einer einfachen Kopie" kennt das Personalausweisgesetz dabei nicht.
- Auskunftssuchende haben ein gewichtiges, schützenswertes Interesse daran, dass ihre amtlichen Legitimationsdokumente und die darauf befindlichen Identitätsdaten nicht in fremde Hände geraten. Es besteht zugleich ein gewichtiges staatliches Interesse daran, die Verlässlichkeit, Verbindlichkeit und Vertraulichkeit amtlicher Ausweisdokumente sicherzustellen. Beides wäre mit einer weitreichenden Verbreitung von Kopien amtlicher Ausweisdokumente bei diversen privaten Stellen nicht zu gewährleisten.

14.3 Personalausweisnummer als "Pfand"

Wir wurden darüber informiert, dass der Initiator einer multimedia-gestützten Ausstellung Tablets an die Besucher ausgab, als "Pfand" aber die Nummer der Personalausweise der Besucher erfragte und aufschrieb. Er wollte sich hiermit vor Diebstahl der Tablets schützen, was selbstverständlich ein völlig legitimes Interesse ist.

Auch in diesem Fall wiesen wir auf die Regelungen des Personalausweisgesetzes hin: Danach ist unter Anwesenden eine Vorlage des Ausweises durch den Ausweisinhaber bei nicht öffentlichen Stellen zum Identitätsnachweis und zur Legitimation zulässig.

Das Ziel des Diebstahlsschutzes konnte im vorliegenden Fall also bereits mit folgendem Vorgehen ausreichend erreicht werden:

1. Erfragen der zur Personenidentifikation notwendigen Angaben (= Feststellung der Identität; es genügen in der Regel bereits Name, Vorname, aktuelle Wohnanschrift);
2. Bitte um Vorlage des Personalausweises oder eines anderen (amtlichen) Ausweisdokuments;
3. Vornahme einer Echtheits-Sichtprüfung und gegebenenfalls Prüfung der Gültigkeit des vorgelegten Dokuments anhand des Geltungsdatums;
4. Verifizierung der zuerst erfragten Identitätsdaten anhand Abgleichs mit dem vorgelegten Ausweisdokument (= Überprüfung der Identität);
5. Festhalten der zur Identifikation erhobenen und verifizierten Angaben.

Eine Befugnis zur Erhebung und Speicherung der Ausweisnummer bestand nicht. Da öffentliche Sicherheitsinteressen in Bezug auf den Umgang mit Personalausweisen beziehungsweise Personalausweisangaben bestehen, kam es auch nicht auf eine etwaige Einwilligung einer beziehungsweise eines Betroffenen an.

Nach ordnungsgemäßer Rückgabe der Tablets waren die erhobenen Besucherdaten im Übrigen unverzüglich zu löschen.

14.4 Buchungsunterlagen im Altpapiercontainer

Bei einer privat betriebenen Freizeiteinrichtung in Bremen stießen wir darauf, dass diese Anmeldeformulare, Rechnungen, Zahlungsbelege und andere kundenbezogene Unterlagen in einem unverschlossenen, allgemein zugänglichen Altpapiercontainer entsorgte. Anders als zu erwarten, waren diese Unterlagen zuvor nicht unleserlich gemacht worden.

Dabei hätte es nur einer geringen (Anschaffungs-)Mühe bedurft, nämlich der Besorgung eines geeigneten Aktenvernichtungsgeräts, um eine fachgerechte Entsorgung

sicherzustellen (näheres zur fachgerechten – und damit regelmäßig auch datenschutzgerechten – Entsorgung von Datenträgern findet sich in der DIN 66399).

Wir wandten uns umgehend an den Betreiber der Freizeiteinrichtung und machten ihn darauf aufmerksam, dass nach dem Bundesdatenschutzgesetz jeder Datenverarbeiter durch geeignete Organisation seiner Betriebsabläufe dafür Sorge zu tragen hat, dass personenbezogene Daten nicht in die Hände unbefugter Dritter gelangen und gegebenenfalls missbraucht werden können. Die Verantwortung lag insoweit unmittelbar bei der Geschäftsleitung.

Zu unserer Überraschung zeigte sich die Geschäftsleitung zunächst allein an der Klärung der Frage interessiert, wie wir den Sachverhalt festgestellt hätten. Einsicht, dass der Umgang mit persönlichen Kundendaten unzureichend war, bestand nicht. Erst als wir nachdrücklich deutlich machten, dass die Frage der Entdeckung des Sachverhalts völlig belanglos sei und ein pflichtwidriges Unterlassen einer fachgerechten Entsorgung mit hieraus folgender Möglichkeit einer Kenntnisnahme der Daten durch Dritte unter Umständen einen Bußgeldtatbestand verwirkliche, des Weiteren auch jederzeit eine ordnungsgemäße Entsorgung angeordnet und zwangsweise durchgesetzt werden könne, lenkte die Geschäftsleitung ein. Sie signalisierte, dass sie mit der Altpapierbeseitigung einen Entsorgungsfachbetrieb beauftragen werde. Ein Aktenvernichtungsgerät hätte allerdings sicherlich auch genügt.

In der Folge wurde uns jedoch keine entsprechende Beauftragung eines Entsorgungsfachbetriebs angezeigt. Erst nach mehrmaliger Nachfrage erhielten wir die Mitteilung, welcher Entsorgungsfachbetrieb beauftragt worden sei und wie die Entsorgung nunmehr sichergestellt sei. Eine Nachprüfung vor Ort steht noch aus. Insgesamt bestätigte sich auch in diesem Fall leider wieder unsere negative Erfahrung, dass wir gelegentlich selbst bei an und für sich unproblematisch zu beseitigenden Datenschutzmängeln erheblichen Aufwand betreiben müssen, um bei verantwortlichen Stellen die Einhaltung des Bundesdatenschutzgesetzes durchzusetzen.

14.5 Rentenversicherungsdaten in einer Rechnung eines Energieversorgungsunternehmens

Ein Petent teilte uns mit, dass er eine Rechnung eines Energieversorgungsunternehmens für seine verstorbene Mutter erhalten habe. Er äußerte Verwunderung darüber, dass in der Rechnung ein von der Deutschen Rentenversicherung zurückgeforderter Betrag aufgeführt sei. Wir forderten das Unternehmen daraufhin zur Stellungnahme auf. Der Energieversorger erklärte daraufhin, die Deutsche Rentenversicherung habe noch über den Sterbemonat hinaus Rente auf das Bankkonto der Mutter des Petenten überwiesen. Die Rentenversicherung habe die überzahlten Beträge zurückbuchen wollen, was aber nicht

möglich gewesen sei, weil zwischenzeitlich das Geld an das Unternehmen überwiesen worden sei. Das Bankinstitut habe daraufhin die Rentenversicherung darüber informiert, welche Stellen Geldleistungen erhalten hätten. Anschließend habe die Rentenversicherung den Betrag von dem Energieversorger zurück gefordert, der dann in der besagten Rechnung aufgeführt worden sei.

Das Vorgehen ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Das Sozialgesetzbuch bestimmt, dass Geldleistungen, die für die Zeit nach dem Tod des Berechtigten zu Unrecht erbracht worden sind, unter anderem von demjenigen der Rentenversicherung zu erstatten sind, der die Überzahlung durch Dauerauftrag, Lastschrifteinzug oder sonstiges bankübliches Zahlungsgeschäft erhalten hat. Ein Geldinstitut, das eine Rücküberweisung mit dem Hinweis abgelehnt hat, dass über den Betrag bereits anderweitig verfügt wurde, hat der überweisenden Stelle oder dem Träger der Rentenversicherung auf Verlangen Name und Anschrift der empfangenden oder verfügenden Person und etwaige neue Kontoinhaberinnen und Kontoinhaber zu benennen. Der Petent wurde von uns über die Rechtslage informiert.

14.6 Marktraumumstellung Bremen bei einem Energieversorgungsunternehmen

In den nächsten Jahren führt eine Konzerngesellschaft eines Engergieversorgers in Bremen eine Marktraumumstellung durch. Sie ist notwendig, um das derzeit verwendete, in Zukunft aber zur Neige gehende L-Gas durch das langfristig verfügbare H-Gas zu ersetzen. L-Gas steht für "low", also niedrig, während H-Gas "high", also hoch bedeutet. Die Bezeichnungen beziehen sich auf den Brennwert der Gase. Da die vorhandenen Gasgeräte an das L-Gas angepasst sind, müssen sie im Zuge der Marktraumumstellung angepasst oder ausgetauscht werden. Betroffen sind alle Erdgasnutzerinnen und Erdgasnutzer im Versorgungsgebiet der Konzerngesellschaft Zunächst ist eine umfangreiche Bestandsaufnahme nötig, um festzustellen, welche Geräte bei den Verbrauchern vorhanden sind. Dazu werden die Gaskunden mit Hilfe der vorhandenen Daten angeschrieben und um Terminvereinbarung gebeten. Im nächsten Schritt werden die Kundinnen und Kunden von Dienstleistern des Energieversorgers aufgesucht, um die Daten der Gasgeräte zu erfassen. Die Dienstleister werden dazu mit Tablets ausgestattet. Es ist auch geplant, die Geräte und Zählerstände zu fotografieren. Im Nachgang findet eine stichprobenhafte Überprüfung von etwa 10 Prozent der erhobenen Daten statt. Anschließend werden die benötigten Ersatzteile beschafft und bei einem erneuten Termin verbaut. An die Abrechnungsstelle wird die Information übermittelt, dass die Umstellung erfolgt ist. Zudem findet eine erneute Qualitätskontrolle statt. Wir werden das Verfahren begleiten und darauf achten, dass die datenschutzrechtlichen Vorschriften eingehalten werden. Für das Verfahren wird ein eigenes

mandatenfähiges informationstechnisches System eingerichtet, welches wir prüfen werden. Besonderes Augenmerk wird auf die eingesetzten Tablets zu richten sein. Es muss sichergestellt werden, dass keine unbefugten Personen auf die Geräte zugreifen können. Durch organisatorische Maßnahmen ist beispielsweise sicherzustellen, dass beim Fotografieren der Geräte und Zählerstände keine weiteren Details aus dem persönlichen Umfeld der Betroffenen erfasst werden.

14.7 Datenflüsse zwischen Sportvereinen und Dachverband

Immer häufiger treten Sportvereine an uns heran, um datenschutzrechtliche Beratungen in Anspruch zu nehmen, manchmal auch in Zusammenhang mit Beschwerden von Vereinsmitgliedern. Mit den datenschutzrechtlichen Bestimmungen für nicht öffentliche Stellen im Bundesdatenschutzgesetz können viele Sportvereine in der Praxis wenig anfangen. Gern versuchen sie, ihre Mitglieder über Einwilligungen ins Boot zu holen. Wir klärten darüber auf, dass Einwilligungen jederzeit mit Wirkung für die Zukunft von den Mitgliedern widerrufen werden können und damit zum Beispiel keine geeignete Basis für eine umfassende und vollständige Mitgliederdatenbank darstellen.

Im Berichtsjahr haben wir festgestellt, dass regionale Sportvereine häufig von den Kreisverbänden oder den Landesverbänden zur Weitergabe von immer mehr Mitgliederdaten aufgefordert werden, die aus unserer Sicht für die Arbeit auf den höheren Ebenen der Verbandsarbeit bis hin zum Dachverband nicht erforderlich sind. Allgemeingültige Aussagen lassen sich für solche Fälle hier nicht treffen. Wir prüfen in diesen Fällen im Hinblick auf die konkrete Vereinsarbeit genau, ob umfassende Übermittlungen von Mitgliederdaten oder auch allumfassende Mitgliederdatenbanken erforderlich und damit datenschutzrechtlich zulässig sind.

14.8 Mitgliedsausweis mit Barcode im Bremer Sportverein

Im Berichtsjahr tauchten mehrere Beschwerden in Zusammenhang mit der Einführung eines Mitgliedsausweises mit maschinenlesbarem Barcode in einem Bremer Sportverein auf. Diese Beschwerden nahmen wir zum Anlass, den neuen Mitgliedsausweis und die damit im Zusammenhang stehende Technik zu prüfen und zu bewerten. Gegenstand unserer datenschutzrechtlichen Prüfung waren die Online-Mitgliederverwaltung und die damit verbundene Auftragsdatenverarbeitung sowie das neue Barcode-Verfahren im Rahmen der Einlasskontrolle im Sportverein. In unserem aufsichtsbehördlichen Prüfverfahren stellten wir fest, dass marginale Änderungen in der Verfahrensbeschreibung sowie im Vertrag über die Auftragsdatenverarbeitung vorzunehmen waren, und dass hinsichtlich des konkreten technischen Verfahrens nichts zu beanstanden war.

Aufgrund des Umfangs der Datenverarbeitung im Sportverein war ein Datenschutzbeauftragter zu bestellen. Wir weisen an dieser Stelle aus Transparenzgründen darauf hin, dass die Mitglieder in Sportvereinen sich an ihren Datenschutzbeauftragten wenden können, um die zur automatisierten Datenverarbeitung gehörige Verfahrensbeschreibung von ihrem Sportverein gemäß § 4g Absatz 2 Satz 2 Bundesdatenschutzgesetz auf Antrag zur Verfügung gestellt zu bekommen.

15. Internationales und Europa

15.1 Datenschutzgrundverordnung

In den letzten Jahresberichten informierten wir immer wieder ausführlich über die geplante Datenschutzgrundverordnung (zuletzt im 37. Jahresbericht, Ziffer 17.2). Am 15. Juni 2015 legte der Europäische Rat als letztes europäisches Gremium seinen Entwurf zur Datenschutzgrundverordnung vor. Das Europäische Parlament (EU-Parlament) hatte dies bereits am 12. März 2014 getan. Der Entwurf der Kommission der Europäischen Union (EU-Kommission) stammt vom 25. Januar 2012.

Am 24. Juni 2015 begannen die drei Organe der Europäischen Union mit den entsprechenden Verhandlungen über einen einheitlichen Text (Trilog), welcher Ende 2015 abgeschlossen wurde. Bis Redaktionsschluss lag uns das Ergebnis noch nicht vor. Ein Inkrafttreten der Datenschutzgrundverordnung ist für zwei Jahre nach Abschluss des Trilogs geplant. Verhandelt wurde über eine direkt anwendbare Datenschutzregelung für die gesamte Europäische Union, zu deren Kernpunkten unter anderem Transparenzregelungen und Auskunftsansprüche über Stellen, Zweck und Speicherdauer, Beschwerdemöglichkeiten und Rechtsschutzmöglichkeiten sowie die Möglichkeit gehören, deutlich höhere Bußgelder als gegenwärtig verhängen zu können. Den derzeitigen Problemen mit international agierenden Unternehmen soll mit Hilfe der sogenannten One-Stop-Shop-Regelung begegnet werden können, wobei nur die Datenschutzaufsichtsbehörde zuständig ist, die sich am Hauptsitz des Unternehmens befindet.

Die Mitglieder des Trilogs vertreten dabei teilweise sehr unterschiedliche Auffassungen zu den zentralen Grundprinzipien des Datenschutzrechts. Wir sehen es als außerordentlich wichtig an, dass die Datenschutzgrundverordnung im Vergleich zur Europäischen Datenschutzrichtlinie von 1995 einen besseren, mindestens aber gleichwertigen Schutz gewährleistet. Dabei müssen die Prinzipien der Datenvermeidung, der Datensparsamkeit und der Zweckbindung weiterhin Teil der Grundverordnung sein; ebenso die Gewährleistungsziele Vertraulichkeit, Integrität und Verfügbarkeit sowie Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit (siehe hierzu die Stellungnahme der Konferenz der

Datenschutzbeauftragten des Bundes und der Länder zum Trilog (https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Kernpunktepapier%20DE.pdf).

Der Ausgang der Verhandlungen von EU-Parlament, dem Europäischen Rat und der EU-Kommission über der Datenschutzgrundverordnung war bis Redaktionsschluss noch offen. Wie auch immer die genauen Formulierungen letztendlich lauten werden, werden Richtschnüre ihrer Auslegung die sich aus Artikel 8 der Europäischen Grundrechtecharta und Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ergebenden Grundprinzipien des Datenschutzes und die darauf beruhende Rechtsprechung des Europäischen Gerichtshofes sein (siehe hierzu auch Ziffer 1.2 und Ziffer 1.3 dieses Berichts).

15.2 Safe Harbor

Am 6. Oktober 2015 erklärte der Europäische Gerichtshof die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig, die als Rechtsgrundlage für die Übermittlung personenbezogener Daten von Bürgerinnen und Bürgern der Europäischen Union (EU) in die Vereinigten Staaten von Amerika (USA) gedient hatte. Die Safe-Harbor-Entscheidung der Kommission wurde im Jahr 2000 getroffen und war immer wieder Thema unserer Jahresberichte (siehe 33. Jahresbericht, Ziffer 18.3, 36. Jahresbericht, Ziffern 1.1.2 und 18.2 und 37. Jahresbericht, Ziffer 17.1). Mit dem Urteil bestätigt der Europäische Gerichtshof die Auffassung der deutschen Datenschutzaufsichtsbehörden, welche bereits im Jahr 2013 direkt im Anschluss an die ersten Enthüllungen Edward Snowdens darauf hingewiesen hatten, dass "die Grundsätze in den Kommissionsentscheidungen (…) mit hoher Wahrscheinlichkeit verletzt" seien (siehe hierzu die Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Juli 2013)[6]. Gleichzeitig wiesen sie auf die Befugnisse der Aufsichtsbehörden hin, auf dieser Grundlage Datentransfers in die USA auszusetzen.

In seiner Entscheidung verweist der Europäische Gerichtshof darauf, dass die EU-Kommission selbst davon ausgegangen sei, dass die US-amerikanischen Behörden auf die aus der Europäischen Union übermittelten personenbezogenen Daten zugriffen. Eine solche Regelung, die es Behörden gestatte, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, verletze den Wesensgehalt des durch Artikel 7 der Grundrechtecharta garantierten Grundrechts auf Achtung des Privatlebens. Auch habe die EU-Kommission selbst festgestellt, dass es für die betroffenen EU-Bürgerinnen und EU-Bürger in den USA keine Rechtsbehelfe gebe, die es ihnen erlaubten, Zugang zu den sie betreffenden Daten zu erhalten und gegebenenfalls deren Berichtigung oder Löschung zu

[6] http://www.senatspressestelle.bremen.de/sixcms/detail.php?gsid=bremen146.c.71856.de&asl=

erwirken. Eine solche Regelung verletze den Wesensgehalt des in Artikel 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz.

Die Umsetzung des Urteils, das auf die Safe-Harbor-Entscheidung gestützte Datenübermittlungen in die USA die Rechtsgrundlage entzieht und auch andere Rechtsgrundlagen für Datenübermittlungen in die USA mit einem Fragezeichen versieht, stellt sowohl die Unternehmen als auch die Politik vor neue Herausforderungen. Betroffen sind alle Unternehmen, die beispielsweise ihren Muttersitz in den USA haben oder dortige Speicherlösungen (wie zum Beispiel Cloud Computing) nutzen. In Gesprächen mit Bremer Unternehmen ist deutlich geworden, wie schwierig diese Situation ist. Die Unternehmen sitzen "zwischen den Stühlen" (siehe hierzu unsere Pressemitteilung vom 7. Oktober 2015)[7]. Momentan ist es ihnen nicht möglich, sowohl das europäische als auch das US-amerikanische Recht gleichermaßen einzuhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einem Positionspapier unter anderem festgelegt, dass Datenübermittlungen, die ausschließlich auf Safe Harbor gestützt sind, untersagt werden. Die Möglichkeit, EU-Standardvertragsklauseln oder auch verbindliche Unternehmensregelungen (Binding Corporate Rules, BCR) zur Datenübertragung in ein unsicheres Drittland zu nutzen, sind zwar formal von der Entscheidung des Europäischen Gerichtshofs nicht betroffen. Die Ausführungen des Gerichts zum anlasslosen und massenhaften Ausspähen der Daten und zum Fehlen von Rechtsschutzmöglichkeiten in den USA stellen aber auch diese Instrumente in Frage. Die Aufsichtsbehörden für den Datenschutz werden aus diesem Grund vorerst keine neuen Genehmigungen für Datenübermittlungen in die USA erteilen. Einzig die Nutzung europäischer Server und Rechenzentren bietet gegenwärtig die Garantie für eine datenschutzkonforme Nutzung. Die Probleme des Datentransfers in die USA bleiben damit allerdings bestehen.

Ohne neue, einheitliche und dem europäischen Datenschutz entsprechende Regelungen ist es den betroffenen Unternehmen nicht möglich, sich aus dieser Situation zu befreien. Derzeit laufen die Verhandlungen zwischen der EU und den USA zu einem entsprechenden Abkommen; eine Aussage zu dessen Qualität kann zum jetzigen Zeitpunkt noch nicht getroffen werden. Den Anforderungen des Europäischen Gerichtshofes würde ein solches Abkommen genügen, wenn die USA auf die anlasslosen und massenhaften Zugriffe auf die Daten verzichten und somit die Grundrechte gewährleisten würden.

[7] https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Pressemitteilung%20Safe%20Harbor.docx.pdf

16. Ordnungswidrigkeiten/Zwangsmittelverfahren

16.1 Ordnungswidrigkeitsverfahren nach dem Bundesdatenschutzgesetz

Auch in diesem Berichtsjahr betrieben wir Ordnungswidrigkeitsverfahren und waren dabei mit unterschiedlichen Verstößen gegen das Bundesdatenschutzgesetz befasst. So richtete sich ein Verfahren gegen ein Betriebsratsmitglied eines Bremer Unternehmens, das dem Betriebsrat zur Verfügung stehende Beschäftigtendaten im Vorfeld der Wahlen zur Bremischen Bürgerschaft unzulässiger Weise für Wahlwerbung genutzt hatte. Bei der Versendung von E-Mails zum Zweck der Wahlwerbung an alle Mitarbeiterinnen und Mitarbeiter des Unternehmens hatte das betreffende Betriebsratsmitglied die Empfängerinnen und Empfänger nicht darauf hingewiesen, dass sie der Nutzung ihrer Daten für Zwecke der Wahlwerbung widersprechen können. Auch waren Beschäftigtendaten trotz Widerspruchs für Wahlwerbung genutzt worden. In einem anderen Fall hatte die Mitarbeiterin eines Unternehmens auf ein Auskunftsersuchen eines Bürgers diesem personenbezogene Daten, die nicht allgemein zugänglich sind, zugänglich gemacht.

16.2 Zwangsmittelverfahren

Auch im Berichtsjahr betrieben wir in mehreren Fällen Zwangsmittelverfahren. Die Verfahren betrafen erneut insbesondere die Nichterteilung von Auskünften, zu denen die für die Datenverarbeitung verantwortlichen Stellen verpflichtet sind. Auch die Nichteinhaltung von Anforderungen an die Videoüberwachung durch ein großes Bremer Unternehmen war Gegenstand eines solchen Verfahrens. Angedroht und festgesetzt wurden Zwangsgelder in Höhe von bis zu 1.600 Euro. Im Fall der Nichtumsetzung der Anforderungen an die Videoüberwachung wurde ein Zwangsgeld in Höhe von 5.000 Euro angedroht. Da das Unternehmen nach der Androhung den von ihm einzuhaltenden datenschutzrechtlichen Anforderungen entsprach, brauchte dieses Zwangsgeld nicht festgesetzt zu werden. In den Fällen, in denen rechtskräftig festgesetzte Zwangsgelder nicht bezahlt wurden, wurden von uns außerdem Mahnverfahren und Vollstreckungsverfahren betrieben.

16.3 Erzwingungshaft gegen einen Geschäftsführer zur Durchsetzung eines Bußgeldes

Wegen beharrlicher Verweigerung einer Auskunft, die wir im Zuge eines datenschutzrechtlichen Prüfverfahrens von einem Unternehmen gefordert hatten, hatten wir durch einen (selbständigen) Bußgeldbescheid eine Geldbuße im niedrigen vierstelligen Bereich gegen das Unternehmen verhängt. Nachdem diese Bußgeldentscheidung rechtskräftig geworden war, das Unternehmen aber keine Bereitschaft zur freiwilligen Zahlung gezeigt hatte, versuchten wir unsere Bußgeldforderung durch Zwangsvollstreckung

durchzusetzen. Vermögensgegenstände, wie beispielsweise Forderungen des Unternehmens gegen Dritte, in die wir hätten vollstrecken können, konnten wir jedoch nicht ausfindig machen. Da zu diesem Zeitpunkt indes noch keine Anhaltspunkte für eine Vermögenslosigkeit des Unternehmens existierten, machten wir von der im Ordnungswidrigkeitengesetz vorgesehenen Möglichkeit Gebrauch und beantragten beim zuständigen Amtsgericht die Anordnung einer Erzwingungshaft gegen den Geschäftsführer zur zwangsweisen Durchsetzung unserer Bußgeldforderung. Das Amtsgericht gab unserem Antrag statt und ordnete Erzwingungshaft gegen den Geschäftsführer an. Gegen diesen Beschluss legte der Geschäftsführer des Unternehmens beim Landgericht Rechtsmittel ein. Das Landgericht wies jedoch das Rechtsmittel des Geschäftsführers zurück. Wir hielten damit einen rechtskräftigen Erzwingungshaftbeschluss in den Händen. Nun hätte im weiteren Verfahren die Staatsanwaltschaft auf unsere Veranlassung den Geschäftsführer zum Haftantritt geladen. Lediglich die Zahlung der festgesetzten Geldbuße hätte grundsätzlich die Inhaftierung noch abwenden können. Zwischenzeitlich war jedoch das Unternehmen in Vermögensverfall geraten, also zu keinerlei Zahlungen mehr fähig. Es war daher von Amts wegen aufgelöst worden. Da unsere Bußgeldforderung gegen das Unternehmen somit nicht mehr durchzusetzen war, blieb der frühere Geschäftsführer des Unternehmens von einer Inhaftierung verschont.

17. Die Entschließungen der Datenschutzkonferenzen im Jahr 2015

17.1 Datenschutz nach "Charlie Hebdo": Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015)

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen

diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheitsrechte und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts – "elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens". Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

17.2 Datenschutzgrundverordnung darf keine Mogelpackung werden!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015)

Der Rat der Europäischen Innenminister und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutzgrundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören unter anderem die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.
- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang

zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, "ausdrücklich" zu streichen und durch den minder klaren Begriff "eindeutig" zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.
- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

17.3 Verschlüsselung ohne Einschränkungen ermöglichen

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015)

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von

Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (zum Beispiel Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,
- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist.[8] Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufsgeheimnissen und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen,

[8] Zitat: "Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nummer 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

17.4 IT-Sicherheitsgesetz nicht ohne Datenschutz!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (Bundestags-Drucksache 18/4096 vom 25. Februar 2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Meldepflichten und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungsprozess und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventionssysteme und Angrifferkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung,

Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des Bundesamtes für die Sicherheit in der Informationstechnik für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des oben genannten Abwägungsprozesses zwischen Informationssicherheitsmaßnahmen und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

17.5 Mindestlohngesetz und Datenschutz

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015)

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer – und gegebenenfalls auch dessen Subunternehmer – den Beschäftigten nicht den Mindestlohn

zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich – wie Industrie- und Handelskammern berichten – zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (zum Beispiel Lohnlisten, Verdienstbescheinigungen und so weiter) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

17.6 Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015)

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen ("eHealth-Gesetz") würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis "für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen" ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (zum Beispiel in § 203 Strafgesetzbuch) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

17.7 Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015)

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden (''Predictive Policing'').

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten – in einem Umfang und auf

eine Art und Weise – verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

17.8 Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. und 19. März 2015)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe-Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die Vereinigten Staaten von Amerika (USA) entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe-Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe-Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe-Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung beziehungsweise Löschung falscher beziehungsweise unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

17.9 Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Juni 2015)

Mit der Vorlage des "Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" (Bundesrats-Drucksache 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeitsprüfung und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (zum Beispiel Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standortdaten und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtsbegriffe (zum Beispiel angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

17.10 Verfassungsschutzreform bedroht die Grundrechte

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. September und 1. Oktober 2015)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem "Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes" (Bundesrats-Drucksache 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht unter anderem vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Videomaterial oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 "Keine Volltextsuche in Dateien der Sicherheitsbehörden" hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 "Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben"). Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert. Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU-Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt. Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 "Effektive Kontrolle von Nachrichtendiensten herstellen!").

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen. Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

17.11 Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. September und 1. Oktober 2015)

Namhafte Hersteller weit verbreiteter Betriebssysteme (zum Beispiel Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, das heißt Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch

gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben beziehungsweise verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud beziehungsweise an den Hersteller übermittelt werden.

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als datenverarbeitende Stelle gerecht werden können.

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

18.1 Nutzung von Kameradrohnen durch Private

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 15./16. September 2015)

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahrzeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in

den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Der potentiell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann der Einsatz von mit Videokameras ausgerüsteten Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Absatz 1 Nummer 1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Absatz 2 Nummer 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmenbedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichtsbehörde oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Absatz 1 des Bürgerlichen

Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201a des Strafgesetzbuches [StGB]), mithin Bereiche der Intimsphäre (im Einzelnen dazu: Bundestagsdrucksache 15/2466, Seite 5.) oder der Aufzeichnung des nicht öffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Fotoausrüstung oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

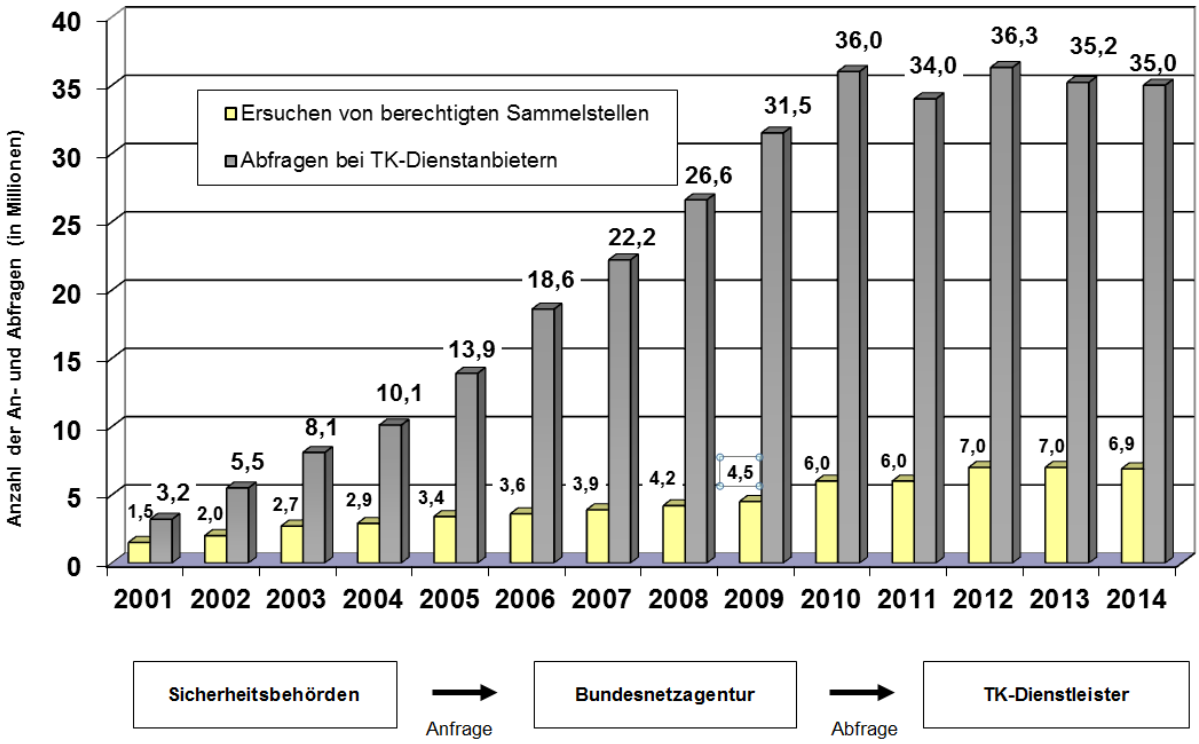
19. Die Europäische und die Internationale Datenschutzkonferenz

Die Entschließungen der Europäischen Datenschutzkonferenz im Jahr 2015 sowie Informationen zu den Entschließungen der Internationalen Datenschutzkonferenz am 27. Oktober 2015 in Amsterdam stehen auf der Internetseite der Bundesbeauftragten für den Datenschutz und für die Informationsfreiheit unter dem Link zur Verfügung: http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/entschliessungen-node.html.

20. Anhang

20.1 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 150 berechtigte Stellen und mehrere tausend hieran angeschlossene Abfragestellen der Strafverfolgungsbehörden automatisiert entsprechende Bestandsdaten bei den Telekommunikationsdiensteanbietern.



Quelle: Jahresbericht 2014 der Bundesnetzagentur

20.2 Liste des verfügbaren Informationsmaterials

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

20.3 Index

E

F

G

I

J

K

L

M

O

P

Z