40. 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 2017. Redaktionsschluss für die Beiträge war der 31. Dezember 2017.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. 3 .. 2 .. 1 .. Europa: #40 = #0

Das 40. Jahr des Datenschutzes in der Freien Hansestadt Bremen ist gleichzeitig der Beginn einer neuen Zeitrechnung. 2018 ist das Geburtsjahr, also das Jahr Null der durch die Europäische Datenschutzgrundverordnung garantierten informationellen Selbstbestimmung. Wie sich die informationelle Selbstbestimmung im Land Bremen vom Volkszählungsurteil bis heute entwickelt hat, zeigen 40 Jahresberichte für Datenschutz. Meine Vorgänger Hans Schepp, Prof. Dr. Alfred Büllesbach, Dr. Stefan Walz, Sven Holst und ich haben in 40 Berichten über die Hochs und Tiefs des Datenschutzniveaus in Bremen berichtet. Seit dem 32. und damit meinem ersten Jahresbericht tragen die Druckwerke eine blaue Farbe. Nicht erst mit dem Bericht, den Sie in Händen halten, ist diese Farbe ein Statement für Europa, für die Charta der Grundrechte der Europäischen Union, die in ihrem Artikel 7 das Recht auf Achtung des Privatlebens und der Kommunikation und in ihrem Artikel 8 das Recht auf Schutz personenbezogener Daten garantiert. Die europäischen Grundrechte sind wichtiger Bestandteil der EU-Verträge, was zeigt, dass das Fundament der politischen und wirtschaftlichen Entwicklung der Europäischen Union (EU) auf starken Säulen garantierter Grundrechte ruht.

Der 25. Mai 2018 wird der erste Geltungstag der Europäischen Datenschutzgrundverordnung (DSGVO) sein. Ab diesem Tag gilt für die Verarbeitung der Kundennamen des Kaufhauses in Uppsala dieselbe Norm wie für die Verarbeitung der Kundennamen des Restaurants auf der Insel Kreta. Dieselbe Regelung müssen auch die bremischen Unternehmen einhalten. Für Datenverarbeitungen durch private Unternehmen gibt es von diesem Grundsatz nur sehr wenige Ausnahmen. Dass sich Unternehmen nicht mehr umstellen müssen, wenn sie personenbezogene Daten in anderen EU-Ländern verarbeiten, erleichtert ihnen den geschäftlichen Schritt über die mitgliedstaatlichen Grenzen. An dieser Stärkung Europas und der EU in Zeiten, in denen die in der Europäischen Grundrechtscharta garantierten Rechte der Menschen zunehmend von innen und von außen infrage gestellt werden, müssen wir alle ein massives Interesse haben. Weil diese Rechte Ausgangspunkt der DSGVO sind, ist das Inkrafttreten der DSGVO am 25. Mai 2018 deshalb für uns alle eine gute Nachricht.

Dafür, dass es überhaupt gelingen konnte, dass sich die europäischen Akteure nach langem Ringen auf ein gemeinsames Regelwerk einigen konnten, müssen wir auch Edward Snowden danken. Erinnern Sie sich noch an seine Enthüllungen? Die Weltöffentlichkeit war vom Ausmaß der anlasslosen Überwachungen des Internets durch die amerikanischen Geheimdienste überrascht. Aber auch Missbräuche Privater hatten schon zuvor und seitdem immer wieder durch neue Skandale weiter genährte Zweifel begründet, ob unsere Daten wirklich nur dort landen, wo sie hingeschickt werden. Nach einer Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) hatten im Sommer 2017 zwei Drittel

der repräsentativ Befragten ein geringes Vertrauen in die Kompetenz von Unternehmen, Sicherheit für ihre Kundinnen und Kunden im Internet zu garantieren. Als die Europäische Kommission im Januar 2012 den ersten Vorschlag für eine Europäische Datenschutzgrundverordnung vorlegte, war es ihr erklärtes Ziel, das Vertrauen der Menschen in die Sicherheit von Transaktionen über das Internet (wieder?)herzustellen, um die europäische Wirtschaft zu stärken. Nach vier Jahren kontroverser Diskussion (siehe hierzu 35. Jahresbericht, Ziffern 1.2, 18.3; 36. Jahresbericht, Ziffern 1., 22.2; 37. Jahresbericht, Ziffer 17.2 und 38. Jahresbericht, Ziffern 1., 17.2, 15.1) erhielt die DSGVO ihre endgültige Gestalt. Die datenschutzpolitische Diskussion beschäftigt sich seitdem vor allem mit der Umsetzung der DSGVO (siehe hierzu 39. Jahresbericht, Ziffern 1., 2., 18.1)

Wird nun alles anders? Nein, hier gilt das Motto des Reiseführers "Per Anhalter durch die Galaxis": KEINE PANIK! Wir können unbesorgt sein, weil auf unseren Datenschutzkompass Verlass bleibt. Unsere Rechte, also die der von der Verarbeitung personenbezogener Daten Betroffenen werden dabei noch gestärkt (siehe hierzu 39. Jahresbericht, Ziffer 2.1) und die vielleicht weitreichendste Änderung ist die Geltung des Marktortprinzips, das nichts anderes besagt, als dass alle, die die Daten der Menschen in Europa verarbeiten, sich an die in der EU geltenden Regeln, also an die DSGVO halten müssen. Aber sonst bleibt fast alles beim Alten: Es geht "nur" um personenbezogene Daten (siehe hierzu Ziffer 1.1 dieses Berichts), ohne unsere Erlaubnis oder die des Gesetzgebers sollten Verarbeiter die Finger von unseren Daten lassen (siehe hierzu Ziffer 1.2 dieses Berichts), die Verarbeitung unserer Daten ist nur erlaubt, wenn sie ein passendes Werkzeug ist (siehe hierzu Ziffer 1.3 dieses Berichts), wir haben Ansprüche auf die Richtigkeit unserer Daten und die Transparenz der Verarbeitung (siehe hierzu Ziffern 1.4 und 1.8 dieses Berichts) und Verstöße gegen unser Grundrecht auf informationelle Selbstbestimmung kosten etwas, ab dem 25. Mai 2018 sogar deutlich mehr (siehe hierzu Ziffer 1.5 dieses Berichts).

Nicht nur für Unternehmen, die die Ausrichtung an der DSGVO als Qualitätssicherung begreifen können (siehe hierzu Ziffer 1.6 dieses Berichts), sondern auch für den bremischen Gesetzgeber muss bis zum 25. Mai 2018 noch einige Arbeit erledigt werden: Auch die für öffentliche Stellen geltenden Regelungen müssen an die DSGVO angepasst werden. Hier bleibt mein Wunsch nach einem europa- und grundrechtsgewogenen bremischen Profil der informationellen Selbstbestimmung aktuell (siehe hierzu Ziffer 1.7 dieses Berichts).

1.1 Es geht "nur" um personenbezogene Daten

Datenschutz bleibt Grundrechtsschutz. Umfasst sind deshalb nur personenbezogene Daten, oder solche, die zum Beispiel mit Hilfe von Kennnummern auf Personen bezogen werden können. Wenn es Datennutzerinnen und Datennutzern gelingt, personenbezogene Daten so zu verändern, dass diese Informationen nicht mehr auf eine bestimmte Person zurückgeführt

werden können, sind sie vor der datenschutzrechtlichen Aufsichtsbehörde sicher. Eine solche Anonymisierung ist aber nicht so einfach. Sie funktioniert beispielsweise nicht, wenn so viele Daten über eine Person zusammengesammelt werden, dass diese Kombination nur noch auf diese Person zutrifft, oder wenn Dritte über Zusatzwissen verfügen, das eine Identifikation erlaubt.

1.2 Erlaubnis oder Finger weg

Personenbezogene Daten zu verarbeiten, ist weiterhin nur erlaubt, wenn es dafür eine gesetzliche Grundlage gibt, oder die Menschen, um deren Daten es geht, einwilligen. Deshalb bleibt es selbstverständlich, dass Beschäftigte gefragt werden, bevor ihre privaten Adressdaten, die die Personalverwaltung nach dem Gesetz für Personalverwaltungszwecke speichern durfte, an ein Fitnessstudio weitergegeben werden. Das gilt selbst dann, wenn das betreffende Unternehmen für seine Beschäftigten Sonderkonditionen ausgehandelt hat. Immerhin kann es sein, dass jemand genau mit diesem Studio schlechte Erfahrungen gemacht hat und deshalb nicht von ihm angeschrieben werden möchte. Nur, wer die Daten anderer ausschließlich für sich selbst verwendet, kann dies auch ohne Einwilligung der Betroffenen tun. Schon das "Teilen" von Fotos, auf denen auch andere zu erkennen sind, mit Freundinnen oder Freunden ist nur in Ausnahmefällen ohne die Einwilligung der Abgebildeten (oder eine andere Rechtsgrundlage) erlaubt. Dass das nicht zu viel verlangt ist, zeigt ein ehrlicher Rollentausch: Dass andere finden, das Foto von mir im zerknautschten morgendlichen Zustand sei witzig, heißt noch nicht, dass ich möchte, dass auch meine ebenfalls mit der Fotografin befreundete frühaufstehende Chefin mich so sieht. Der möchte ich lieber die auf meinem eigenen Blog eingestellten selbstironischen Morgenmuffel-Selfies zeigen, aus denen jedenfalls nicht die schlechte Laune spricht.

1.3 Datenverarbeitung bleibt ein Werkzeug, das passen muss

Ein falscher Schlüssel kann die Tür nicht öffnen. Eine Spitzhacke kann dies zwar. Trotzdem ist es sinnvoller, stattdessen den passenden Schlüssel zu nutzen. Und für die Öffnung einer Bürotür wird niemand sämtliche Schlüssel eines Betriebes mit Werkshallen und 100 Beschäftigten bei sich tragen. Entsprechende Gedanken über Datenverarbeitungen finden sich in der Datenschutzgrundverordnung:

Die Verarbeitung personenbezogener Daten muss rechtmäßigen Zwecken dienen. Selbstverständlich gehört die permanente Videoüberwachung, derer sich Beschäftigte nicht entziehen können, nicht dazu. Aber Diebstahlsprävention in einer leer stehenden Lagerhalle ist ein legitimes Interesse, genauso wie die Information der Kundinnen und Kunden über neue Produkte. Wichtig ist, dass die Verarbeitungszwecke genau formuliert werden, weil nur so erkannt werden kann, wann sich Zwecke ändern und deshalb eine neue Rechtsgrundlage

benötigt wird. Es ist etwas anderes, ob Adressdaten als Lieferanschrift oder zu Werbezwecken verwendet werden. Eine Kundin kann beispielsweise sichergestellt haben, dass sie eine Lieferung selbst entgegennehmen kann. Werbung lehnt sie aber vielleicht ab, weil sie ihre Familie später überraschen will und sichergehen will, dass zwischenzeitlich niemand bemerkt, dass sie Kundin des Spieleversandes ist.

Wie falsche Schlüssel können auch Datenverarbeitungen schlicht ungeeignet sein, rechtmäßige Zwecke zu erfüllen. Adressbuchdaten, die die Taschenlampen-App anfordert, können die Lichtsteuerung des Smartphones nicht aktivieren. Auch sind nur "erforderliche" Datenverarbeitungen erlaubt: Zwar kann die Installation einer Kamera Diebstähle aus Aktenschränken möglicherweise verhindern. Die Schränke zu verschließen ist aber mindestens genauso geeignet und greift nicht in die informationelle Selbstbestimmung der Beschäftigten ein. Datenstaubsauger wie Gesichtserkennungssysteme dürfen nur in besonderen Fällen benutzt werden: Mit ihrer Hilfe herauszufinden, wer das vergünstigte Kantinenessen in der Betriebskantine erhalten darf, ist offensichtlich unverhältnismäßig und gehört deshalb nicht dazu. Das Grundprinzip der Datenminimierung wird durch die Speicherung der Mitgliedsseiten der Kundinnen und Kunden in sozialen Netzwerken verletzt, selbst wenn ihre Auswertung Lieferadressen ergeben könnte.

1.4 Transparenz und Richtigkeit

Die Datenschutzgrundverordnung setzt auf transparente (siehe hierzu Ziffer 1.8 dieses Berichts) Informationen für uns als Kundinnen und Kunden und Beschäftigten von Unternehmen, als diejenigen, deren Daten von Meldeämtern, Krankenkassen oder App-Anbietern verarbeitet werden. Darüber, was Verarbeiter mit unseren Daten vorhaben, müssen sie uns von sich aus informieren, bevor sie die Daten erheben. Wie bisher gibt es das Recht auf Berichtigung falscher Informationen, und darauf, dass Daten wieder gelöscht werden, wenn sie nicht mehr für den Zweck gebraucht werden, zu deren Erfüllung sie erhoben wurden.

1.5 Falsch Datenparken kann Unternehmen etwas kosten, gefährliche Eingriffe in den Datenverkehr sogar eine Menge

Eine nicht ganz unwichtige Neuerung ist der Bußgeldrahmen für Verstöße gegen die Datenschutzgrundverordnung. Er wurde drastisch erhöht: 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes können es für Unternehmen pro Verstoß werden. Aber auch Reputationsschäden können kosten, denn Datenschutzverstöße werden von den Betroffenen schon lange nicht mehr als Kavaliersdelikt angesehen. Deshalb ist Unternehmen zu raten, lieber einmal zu transparent und vorsichtig zu sein als einmal zu

wenig und im Zweifel auf Verarbeitungen verzichten, bei denen "ein mulmiges Gefühl in der Datengegend" entsteht.

1.6 Datenschutz ist Qualitätssicherung

Nach Artikel 30 Datenschutzgrundverordnung (DSGVO) müssen alle, die nicht nur äußerst selten Kundendaten oder Beschäftigtendaten digital verarbeiten, ein Verzeichnis der Verarbeitungstätigkeiten führen. Darin müssen sich Informationen über die verarbeiteten Daten finden, darüber, ob sie erhoben, gespeichert, weitergegeben oder anders verarbeitet werden und zu welchen Zwecken dies geschieht. Auch sollten sich Unternehmen Gedanken darüber machen, wann die Daten gelöscht werden sollen, und wie sie in technischer und organisatorischer Hinsicht etwa durch Zugangsberechtigungen und Verschlüsselungen vor Missbrauch geschützt werden. Bei der Erstellung oder Aktualisierung eines solchen Verzeichnisses bis zum 25. Mai 2018 werden also dieselben Fragen wie in Projekten zur Verbesserung von internen Verfahrensabläufen gestellt: Wer im Unternehmen braucht welche Daten wofür? Welche Daten müssen personenbezogen sein, welche können anonymisiert werden? Brauchen die Daten unnötigen Speicherplatz? Erhalten zu viele Stellen zu viele Informationen, was es ihnen erschwert, die wichtigen zu finden? Wahrscheinlich finden sich beim Beantworten dieser Fragen Belege für meine These, dass Datenschutz Qualitätssicherung ist und damit auch jede Menge Geld sparen kann. Eine große Hilfe bei der Beantwortung dieser Fragen sind interne Datenschutzbeauftragte. Deshalb sollten Unternehmen auch dann darüber nachdenken, sie zu bestellen, wenn sie nach der DSGVO vielleicht gar nicht hierzu verpflichtet sind.

1.7 Das europa- und grundrechtsgewogene bremische Profil der informationellen Selbstbestimmung

Schon in der Einleitung zum 38. Jahresbericht (siehe hierzu Ziffer 1.4 dieses Berichts) hieß es: "Da kommt was auf uns zu. Oder: Was der Landesgesetzgeber nach Erlass der Datenschutzgrundverordnung (DSGVO) entscheiden muss". Und im letzten Jahresbericht hatte ich mir schon auf dem Titelblatt ein europa- und grundrechtsgewogenes bremisches Profil der informationellen Selbstbestimmung gewünscht. Mittlerweile liegt der Entwurf eines "Bremischen Ausführungsgesetzes zur Datenschutzgrundverordnung vor (BremAGDSGVO)" vor, der damit schon im Titel deutlich macht, dass verstanden worden ist, dass der europäische Gesetzgeber unsere Grundrechte ausgestaltet hat und deshalb keine bremische Vollregelung getroffen werden kann, sondern dass es im Ausführungsgesetz nur darum gehen kann, Regelungsaufträge zu erfüllen, die an den Landesgesetzgeber gerichtet sind, und Regelungsspielräume auszufüllen, die die DSGVO noch gelassen hat. Schon die Tatsache, dass der Regelungsentwurf bereits mit einem Paragrafen 27 endet – der

festschreibt, dass das BremAGDSGVO am 25. Mai 2018 in Kraft und das Bremische Datenschutzgesetz am selben Tag außer Kraft tritt – macht deutlich, dass das Bestreben des europäischen Gesetzgebers, möglichst viele Sachverhalte direkt der DSGVO zu unterstellen, respektiert wurde und von den Regelungsbefugnissen sparsam Gebrauch gemacht werden soll. Auch die übrigen bremischen Fachgesetze werden Änderungen erfahren. Bei all diesen Gesetzesvorhaben freue ich mich auf grundrechtsgewogene Diskussionen mit allen Akteurinnen und Akteuren!

1.8 facebook-agb – das musical

Der Bericht zum Datenschutzjahr 2017 im Land Bremen darf nicht enden, ohne eine besondere Veranstaltung zu erwähnen, die im letzten Jahr in Bremen stattgefunden hat und im Mai 2018 noch zumindest zwei Mal in der Bremer Shakespeare Company wiederholt werden wird: Bundesweite Beachtung (http://www.sueddeutsche.de/wirtschaft/facebook-die-agb-als-musical-1.3624972) erfuhr das von Peer Gahmert und Tim Gerhards auf die Bühne im ehemaligen Güterbahnhof gebrachte Musical "facebook-agb – das musical" (http://facebook-agb-das-musical.de/ueber/). Das Stück erzählt die Liebesgeschichte der jungen Autorin des Werks "Die allgemeinen Geschäftsbedingungen von Facebook inklusive Datenrichtlinie und Cookierichtline". Weil es unlesbar sei und niemanden interessiere, will kein Verlag das Buch auf den Markt bringen. Erst ein junger Informatiker, der am Aufbau eines sozialen Netzwerkes arbeitet, interessiert sich für das Werk und verliebt sich in seine Autorin. Der gesprochene, gesungene und gerappte Text des Musicals besteht fast ausschließlich aus echten Zitaten der Allgemeinen Geschäftsbedingungen von facebook, deren zum Teil überraschender Inhalt schon einige Gerichte beschäftigt hat. In ihrem Artikel 12 fordert die Datenschutzgrundverordnung, dass wir künftig Informationen über die Verarbeitung unserer Daten "in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erhalten müssen. Nicht nur uns Besucherinnen und Besucher des Stücks wurde deutlich vor Ohren geführt, dass facebook – auch was seine Allgemeinen Geschäftsbedingungen anbelangt – vor dem 25. Mai 2018 noch Einiges zu tun hat. Dabei haben wir die Worte immerhin aus den berufenen Mündern der Schauspielerinnen und Schauspieler gehört, die das sinnvolle Betonen gelernt haben…

Dr. Imke Sommer

2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 39. Jahresberichts

Bericht und Beschlussempfehlung des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zum 39. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit und zur Stellungnahme des Senats.

I. Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 5. April 2017 den 39. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 10. März 2017 (Drucksache 19/972) und in ihrer Sitzung am 21. September 2017 die dazu erfolgte Stellungnahme des Senats vom 29. August 2017 (Drucksache 19/1213) an den Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Beratung und Berichterstattung.

Der Ausschuss stellte bei den nachfolgend aufgeführten Punkten des 39. Jahresberichts Beratungsbedarf fest:

Ziffer 2.5 Richtlinie zu europäischem Datenschutzstandard für Justiz und Polizei

Ziffer 6.1 Allgemeines zu Polizeiverfahren

Ziffer 6.2 BodyCam bei der Polizei Bremen

Ziffer 6.4 Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz

Ziffer 6.6 Polizei Bremen – Personenbezogene Daten auf der facebook-Fanseite

Ziffer 7.2 Keine Verschlüsselung von E-Mails mit sensiblen Daten

Ziffer 9.2 Keine vollständige Vorlagepflicht für private Kontoauszüge

In seinen Sitzungen am 22. November 2017 und 20. Dezember 2017 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für Datenschutz und Informationsfreiheit und mit den Vertreterinnen und Vertretern der betroffenen Ressorts.

Der Ausschuss begrüßt, dass es in vielen Fällen, die Anlass zur Kritik gegeben haben, bereits zu einer Klärung mit den betroffenen Ressorts und Dienststellen gekommen ist beziehungsweise im Rahmen von Gesprächen zwischen den Beteiligten konstruktiv an Lösungsmöglichkeiten gearbeitet wird.

Durch das Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz aus dem Jahr 2016 ist es erforderlich geworden, das Bremische Polizeigesetz zu ändern (Ziffer 6.4). Insbesondere die Vorgaben des Bundesverfassungsgerichts für die verfassungsgemäße Ausgestaltung von polizeilichen Eingriffsbefugnissen und Datenübermittlungen sowie für zweckändernde Datennutzungen sind bei der Änderung des Bremischen Polizeigesetzes zu berücksichtigen. Das Innenressort hat dem Ausschuss berichtet, dass an dem Gesetzentwurf mit Nachdruck gearbeitet werde, jedoch noch keine endgültige Fassung vorliege.

Die Richtlinie zum europäischen Datenschutzstandard für Justiz und Polizei soll erstmalig eine Datenschutz-Mindestharmonisierung innerhalb der Europäischen Union herbeiführen (Ziffer 2.5). Eine Umsetzung in deutsches Recht ist bis zum Mai 2018 erforderlich. Die Ressorts Inneres und Justiz haben dem Ausschuss berichtet, dass die Arbeiten zur Umsetzung der Richtlinie zum jetzigen Zeitpunkt noch nicht abgeschlossen seien, es aber Arbeitsgruppen gäbe, die sich damit beschäftigten.

Bei der Polizei Bremen gibt es verschiedene Systeme, bei denen nach wie vor datenschutzrechtliche Mängel bestehen (Ziffer 6.1). Der Ausschuss kritisiert, dass von der Polizei Bremen immer noch kein überzeugendes Löschkonzept installiert worden ist, sodass sich möglicherweise in den polizeilichen Registern und Datenbanken zahlreiche Daten befinden, die dort nicht enthalten sein dürfen und möglicherweise auch falsch sind. Dies erscheint insbesondere vor dem Hintergrund bedenklich, dass aus Bremer Dateien Daten an bundesweite Register geliefert werden. Nach Ansicht des Ausschusses muss künftig sichergestellt werden, dass nur bereinigte Daten migriert werden. Ziel müsse es auch sein, durch geeignete Löschkonzepte dafür Sorge zu tragen, dass sich in den Bremer Systemen keine unzulässigen Daten mehr befinden.

Trotz der zahlreichen offenen Themen im Bereich des Datenschutzes hat das Ressort versichert, dass das Thema Datenschutz ernst genommen werde und ein Problembewusstsein bestehe. Inzwischen sei auch ein zentraler Datenschutzbeauftragter eingestellt worden, der sich um die Erstellung der noch fehlenden Datenschutzkonzepte kümmern werde.

Der Ausschuss hat zur Kenntnis genommen, dass inzwischen zum Einsatz der BodyCam bei der Polizei Bremen eine Evaluation vorliegt, die sich sehr differenziert mit dem Einsatz und dem Nutzen der BodyCam auseinandersetzt (Ziffer 6.2). Die Landesbeauftragte für Datenschutz hat darauf hingewiesen, dass aus der Evaluation hervorgehe, dass bei bestimmten Gruppen keine präventive Wirkung der BodyCam festzustellen sei, sondern die aufgezeichneten Daten eher der späteren Strafverfolgung dienten. Dies sehe sie im Hinblick auf die Gesetzgebungskompetenz für repressive Maßnahmen eher kritisch.

Der Ausschuss hat sich darauf verständigt, die Beratungen in der Innendeputation über den Evaluationsbericht abzuwarten und das Thema zu gegebener Zeit erneut aufzugreifen.

Zum Thema "facebook-Fanseite" hat die Landesbeauftragte für Datenschutz ausgeführt, dass sie die Nutzung dieser Fanseite durch die Polizei Bremen weiterhin kritisch sehe, auch vor dem Hintergrund der Entwicklung der europäischen Rechtsprechung in diesem Bereich (Ziffer 6.6). Das Innenressort sieht hingegen in der Nutzung dieses Mediums vor allem den Vorteil, einen großen Personenkreis zu erreichen und auf große Massen bei Veranstaltungen einwirken zu können. Eine Alternative zu facebook, mit der man eine vergleichbare Wirkung erziele, werde derzeit auf Seiten der Polizei Bremen nicht gesehen.

Der Ausschuss ist sich einig, dass die Nutzung von "facebook-Fanseiten" durch die Polizei viele datenschutzrechtliche Aspekte berührt und kommt überein, sich in einer gesonderten Sitzung erneut mit der Problematik zu beschäftigen.

Zum Thema "Verschlüsselung von E-Mails mit sensiblen Daten" (Ziffer 7.2) hat der Senator für Justiz und Verfassung dem Ausschuss überzeugend dargelegt, dass es sich bei dem im Bericht geschilderten Vorfall um einen Einzelfall gehandelt habe und es grundsätzlich im Ressort eine entsprechende Richtlinie gäbe, die die Übermittlung sensibler Daten per E-Mail nur unter Einsatz geeigneter Verschlüsselungsverfahren erlaube. Auf diese Richtlinie sei im Hinblick auf den Vorfall im Ressort noch einmal ausdrücklich hingewiesen worden.

Zur Vorlagepflicht von privaten Kontoauszügen (Ziffer 9.2) wurde dem Ausschuss berichtet, dass es bereits seit dem Jahr 2013 eine Dienstanweisung gäbe, die besage, dass zwar Kontoauszüge vorgelegt werden müssten, die Leistungsberechtigten aber Recht hätten, nicht relevante Daten selbst zu schwärzen. Der im Bericht geschilderte Vorfall habe Anlass dazu gegeben, die Mitarbeiterinnen und Mitarbeiter noch einmal explizit auf diese Dienstanweisung hinzuweisen und für das Thema zu sensibilisieren. Der Ausschuss geht daher davon aus, dass es sich um einen Einzelfall gehandelt hat und grundsätzlich im Amt für Soziale Dienste verantwortungsvoll mit Daten aus Kontoauszügen umgegangen werde.

II. Beschlussempfehlung

Die Bürgerschaft (Landtag) nimmt den Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Kenntnis.

3. Datenschutzbeauftragte

3.1 Rolle der Datenschutzbeauftragten nach Artikel 37 der DSGVO

Behördlichen und betrieblichen Datenschutzbeauftragten wird auch von der Datenschutzgrundverordnung (DSGVO) eine wichtige Rolle für die Gewährleistung des

Datenschutzes sowohl im öffentlichen als auch im nicht öffentlichen Bereich zugesprochen. Ihre Funktion ist ein wichtiges Instrument der behördlichen oder betrieblichen Selbstkontrolle bei der Verarbeitung personenbezogener Daten.

Nach Artikel 37 Absatz 5 DSGVO sind die Datenschutzbeauftragten auf der Grundlage ihrer beruflichen Qualifikation und insbesondere ihres Fachwissens zu benennen, das sie auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzen müssen, sowie auf der Grundlage ihrer Fähigkeit zur Erfüllung der in Artikel 39 DSGVO genannten Aufgaben. Nach Artikel 37 Absatz 6 DSGVO können sowohl interne als auch externe Datenschutzbeauftragte bestellt werden. Die Ausübung von anderen Aufgaben und Pflichten darf nicht zu einem Interessenkonflikt führen. Die in Artikel 39 DSGVO geregelten Pflichten und Aufgaben der Beauftragten umfassen die Unterrichtung und Beratung der Verantwortlichen beziehungsweise der Auftragsverarbeiterinnen und Auftragsverarbeiter und der Beschäftigten sowie die Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften der Europäischen Union und der nationalen Regelungen. Des Weiteren sind die Datenschutzbeauftragten für die Sensibilisierung, Schulung und die Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung verantwortlich. Um diesen Aufgaben und Pflichten nachkommen zu können, regelt die DSGVO in Artikel 38 Absatz 1 explizit, dass die Datenschutzbeauftragten "ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen" einzubinden sind. Dies bedeutet, dass die Datenschutzbeauftragten nicht eigene Nachforschungen betreiben müssen, sondern die erforderlichen Informationen für ihre Aufgabenwahrnehmung zur Verfügung gestellt bekommen müssen. Auch nach der DSGVO berichten die behördlichen und betrieblichen Datenschutzbeauftragten der Dienststellenleitung beziehungsweise der Geschäftsleitung und sind unmittelbar der höchsten Leitungsebene beziehungsweise Managementebene unterstellt.

Darüber hinaus arbeiten die Datenschutzbeauftragen bei der Erfüllung ihrer Aufgaben mit der Aufsichtsbehörde zusammen. Sie sind Anlaufstelle für die Aufsichtsbehörden bei allen mit der Verarbeitung personenbezogener Daten zusammenhängenden Fragen.

Die Datenschutzbeauftragten nehmen ihre Aufgaben nach Artikel 39 Absatz 2 DSGVO risikoorientiert wahr. Dies bedeutet, dass sie bei der Erfüllung ihrer Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung tragen, wobei sie die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen.

Die zugewiesenen Aufgaben führen nicht dazu, dass die Datenschutzbeauftragten an die Stelle der beziehungsweise des Verantwortlichen oder der Auftragsverarbeiterin beziehungsweise des Auftragsverarbeiters treten. Die datenverarbeitenden Stellen bleiben für die Einhaltung der datenschutzrechtlichen Vorschriften wie bislang selbst verantwortlich.

Mit der Bestellung einer oder eines Datenschutzbeauftragten wird die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften nicht berührt. Die Datenschutzbeauftragten haften nur insoweit, als sie erkennbar ihren Pflichten und Aufgaben nicht nachgekommen sind.

3.2 Zentrale behördliche Datenschutzbeauftragte im Innenressort

Im Vorjahr war im Haushalt des Senators für Inneres für die Aufgabe der beziehungsweise des behördlichen Datenschutzbeauftragten eine Vollzeitstelle eingerichtet worden (siehe hierzu 39. Jahresbericht, Ziffer 4.2), die im März des Berichtsjahres besetzt wurde. Die neue Datenschutzbeauftragte ist organisatorisch in der senatorischen Dienststelle angesiedelt und soll dienststellenübergreifend die Aufgaben der Datenschutzbeauftragten im gesamten Ressortbereich wahrnehmen. Insofern wird von einer durch das Bremische Datenschutzgesetz eröffneten Möglichkeit Gebrauch gemacht, wonach mehrere verantwortliche Stellen gemeinsam eine oder einen Beauftragten für den Datenschutz bestellen können.

Laut eines an uns gerichteten Schreibens des Staatsrates des Senators für Inneres nimmt die neue Datenschutzbeauftragte ihre Funktion für die Behörde des Senators für Inneres und alle ihr im Ressort nachgeordneten Dienststellen bis auf das Statistische Landesamt und das Landesamt für Verfassungsschutz, die weiterhin eine andere Datenschutzbeauftragte beziehungsweise einen anderen Datenschutzbeauftragten haben, wahr. Trotz unseres mehrfachen Hinweises fehlt es weiterhin an der ausreichenden Bestellung durch die Dienststellen der Polizei, der Feuerwehr, des Migrationsamtes, des Bürgeramtes und des Ordnungsamtes. Wir vereinbarten mit dem Senator für Inneres, dass wir zum Nachweis der korrekten Bestellung eine Liste beziehungsweise eine Sammlung mit den Unterschriften der einzelnen Leiterinnen und Leiter der zum Ressort gehörenden Dienststellen erhalten. Hierdurch würde auch der sich aus dem Bremischen Datenschutzgesetz ergebenden Verpflichtung, die Bestellung der oder des behördlichen Datenschutzbeauftragten der Landesbeauftragten für Datenschutz und Informationsfreiheit zu melden, entsprochen werden. Bedauerlicherweise steht die Übersendung der Liste beziehungsweise der Sammlung der Unterschriften trotz mehrfacher Erinnerung seit mehreren Monaten aus.

Erhebliche Probleme ergaben sich bei mehreren von der Umorganisation des Innenressorts betroffenen Dienststellen im Hinblick auf die Beendigung der Amtsübertragung an die bisherigen Datenschutzbeauftragten. In diesen Fällen war zu beachten, dass die Amtsübertragung behördlicher Datenschutzbeauftragter nur mit dem Einverständnis der Amtsinhaberin oder des Amtsinhabers oder in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs widerrufen werden kann.

Der Senator für Inneres bedauerte die entstandenen Probleme und sagte zu, diese in Zusammenarbeit mit den betreffenden ihm nachgeordneten Dienststellen des Ressorts zu lösen. Am Ende des Berichtszeitraums waren alle bisherigen Datenschutzbeauftragten mit ihrem Einverständnis abberufen worden.

Die Zukunft wird zeigen, ob es einer einzigen Person möglich ist, die Funktion der oder des behördlichen Datenschutzbeauftragten im Ressort des Senators für Inneres mit einer Vielzahl unterschiedlicher Datenverarbeitungsverfahren und personenbezogener Verarbeitungen wahrzunehmen.

3.3 Organisatorische Anbindung der behördlichen Datenschutzbeauftragten

Die von den Dienststellen der bremischen Verwaltung nach dem Bremischen Datenschutzgesetz bestellten behördlichen Datenschutzbeauftragten nehmen im Hinblick auf die Umsetzung und Einhaltung der bei der Datenverarbeitung zu beachtenden datenschutzrechtlichen Anforderungen wichtige Aufgaben wahr. Um ihrem gesetzlichen Auftrag nachkommen zu können, sind sie bei der Erfüllung ihrer Aufgaben weisungsfrei und unmittelbar der Leitung der Dienststelle zu unterstellen. Die Datenschutzbeauftragten müssen deshalb Anregungen und Kritik direkt bei der Behördenleitung vortragen können. Dies gilt auch für externe behördliche Datenschutzbeauftragte.

Auch die ab Mai 2018 geltende Europäische Datenschutzgrundverordnung (DSGVO) enthält in ihrem Abschnitt 4 Vorschriften über von Verantwortlichen oder Auftragsverarbeitern bestellte Datenschutzbeauftragte, die der für behördliche Datenschutzbeauftragte in Bremen bestehenden Rechtslage vergleichbar sind. Artikel 37 Absatz 1 Buchstabe a DSGVO stellt klar, dass Behörden und öffentliche Stellen in jedem Fall Datenschutzbeauftragte bestellen müssen, es sei denn, es handelt sich um die justizielle Tätigkeit von Gerichten. Nach Artikel 38 Absatz 1 DSGVO sind Datenschutzbeauftragte in die Klärung aller mit dem Schutz personenbezogener Daten zusammenhängenden Fragen ordnungsgemäß und frühzeitig einzubeziehen. Nach Artikel 38 Absatz 3 DSGVO haben die Verantwortlichen und die Auftragsverarbeiter sicherzustellen, dass die Datenschutzbeauftragten bei der Erfüllung ihrer Aufgaben keine Anweisungen bezüglich der Ausübung ihrer Aufgaben erhalten. Auch ist festgelegt, dass sie unmittelbar der höchsten Leitungsebene berichten.

Die Vorschriften hinsichtlich der Stellung der behördlichen Datenschutzbeauftragten werden von den Dienststellen der bremischen Verwaltung sehr unterschiedlich gehandhabt. Mit einem Rundschreiben, auch im Hinblick auf die künftige Umsetzung der DSGVO, baten wir alle senatorischen Dienststellen bis auf den Senator für Inneres wegen der dortigen Umorganisation (siehe hierzu Ziffer 3.2 dieses Berichts), sowie die Bremische Bürgerschaft,

die Senatskanzlei, die Bremische Zentralstelle für die Verwirklichung der Gleichberechtigung der Frau und den Gesamtpersonalrat um Mitteilung, wem die oder der behördliche Datenschutzbeauftragte organisatorisch zugeordnet ist, wem die oder der Datenschutzbeauftragte über das Ergebnis ihrer beziehungsweise seiner Tätigkeit berichtet und wem sie oder er Kritik und Verbesserungsvorschläge vorträgt. Die Antworten auf unsere Anfrage fielen sehr unterschiedlich aus. Während bei der Bremischen Bürgerschaft, der Senatskanzlei, der Bremische Zentralstelle für die Verwirklichung der Gleichberechtigung der Frau und dem Gesamtpersonalrat die rechtlichen Vorgaben korrekt umgesetzt sind, ergaben sich aus den Antworten der senatorischen Behörden verschiedentliche Mängel. Der behördliche Datenschutzbeauftragte war bei der Senatorin für Kinder und Bildung in der Abteilung "Zentrale Dienste" angesiedelt. Der Datenschutzbeauftragte gab seine Berichte an den Abteilungsleiter ab. Auch beim Senator für Umwelt, Bau und Verkehr gab der dortige externe Datenschutzbeauftragte seine Kritik und Verbesserungsvorschläge gegenüber der Abteilung "Zentrale Dienste" ab. Bei der Senatorin für Finanzen ist der Datenschutzbeauftragte zwar direkt der Dienststellenleitung unterstellt. Anregungen und Kritik trägt er jedoch den Fachabteilungen und Projektgruppen vor, eine Berichterstattung direkt gegenüber der Behördenleitung erfolgt nicht.

Wir wiesen die betreffenden Dienststellen auf die festgestellten Mängel hin und baten sie, diese abzustellen. Die Senatorin für Kinder und Bildung erklärte daraufhin, die direkte Anbindung des behördlichen Datenschutzbeauftragten an die Dienststellenleitung zu beabsichtigen. Die Stelle der oder des Datenschutzbeauftragten solle künftig im Geschäftsverteilungsplan dementsprechend geführt werden und im Stab des Staatsrats angesiedelt sein. Der Senator für Umwelt, Bau und Verkehr teilte entgegen seiner früheren Auskunft nunmehr mit, dass der dortige Datenschutzbeauftragte selbstverständlich gegenüber der Dienststellenleitung zu berichten habe. Auch bei der Senatorin für Finanzen wollte man sich um die rechtskonforme Umsetzung der zu beachtenden Anforderungen bemühen.

3.4 Treffen der behördlichen Datenschutzbeauftragten

Die halbjährlichen Treffen der behördlichen Datenschutzbeauftragten aus Bremen und Bremerhaven sind für die Teilnehmenden zu wichtigen Veranstaltungen geworden, um sich im Hinblick auf ihre Funktion zu informieren, über ihre Tätigkeit zu berichten und sich hieraus ergebende Fragen zu erörtern. Auch im Jahr 2017 fanden diese Treffen statt.

Bei ihrem ersten Treffen im Frühjahr des Berichtsjahres befassten sich die Datenschutzbeauftragten schwerpunktmäßig mit der Datenschutzgrundverordnung (DSGVO). Die Datenschutzgrundverordnung, über die eine Referentin unserer Dienststelle die Teilnehmenden ausführlich informierte, hat erhebliche Auswirkungen auf die von den

Behörden in Bremen und Bremerhaven bei der Datenverarbeitung zu beachtenden datenschutzrechtlichen Anforderungen. Eine detaillierte Kenntnis der DSGVO ist deshalb gerade auch für die Aufgabenwahrnehmung der behördlichen Datenschutzbeauftragten in ihren Dienststellen von besonderer Bedeutung. Erörtert wurde bei dem Treffen auch die sogenannte JI-Richtlinie (EU-Richtlinie 2016/680).

In der Veranstaltung wurde erneut deutlich, dass die Umsetzung der DSGVO für die behördlichen Datenschutzbeauftragten mit zahlreichen neuen Anforderungen verbunden ist, für deren Erfüllung sie Unterstützung sowohl von ihren Dienststellen als auch von der Landesdatenschutzbeauftragten benötigen.

Die Arbeitsgruppe "Prüfung bei Dataport" berichtete beim Treffen im Dezember des Berichtsjahres über ihren Besuch im Rechenzentrum der Anstalt öffentlichen Rechts Dataport in Altenholz bei Kiel (siehe hierzu Ziffer 3.5 dieses Berichts).

Auch im Jahr 2018 wird es wieder Treffen der behördlichen Datenschutzbeauftragten geben. Ein Schwerpunkt dürfte dann insbesondere die Umsetzung der DSGVO mit den damit verbundenen Aufgaben für die Datenschutzbeauftragten sein.

3.5 Arbeitsgruppe "Prüfung bei Dataport"

Die Arbeitsgruppe "Prüfung bei Dataport" führte im Berichtsjahr im Rechenzentrum der Anstalt öffentlichen Rechts Dataport eine Prüfung hinsichtlich der dortigen Datenverarbeitung für die bremische Verwaltung durch (siehe hierzu Ziffer 3.4 dieses Berichts). Am Besuch des Rechenzentrums von Dataport in Altenholz bei Kiel im Oktober 2017 nahmen neben den Mitgliedern der Arbeitsgruppe unterstützend auch Vertreter des IT-Referats der Senatorin für Finanzen und der Landesbeauftragten für Datenschutz und Informationsfreiheit teil. Seitens Dataport nahmen Mitarbeiterinnen und Mitarbeiter aus allen von der Prüfung betroffenen Abteilungen sowie des IT-Sicherheitsmanagements und des betrieblichen Datenschutzes teil.

Die Arbeitsgruppe wollte sich zu Fragen der Gewährleistung notwendiger technischer und organisatorischer Sicherungsmaßnahmen und der Erbringung von Dienstleistungen für die bremische Verwaltung ein eigenes Bild verschaffen. An technischen und organisatorischen Maßnahmen standen insbesondere Maßnahmen der Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle sowie des Trennungsgebotes im Fokus. Die Dienstleistungen des Supports werden von Dataport durch einen User Help Desk im First-Level-Support, einen Second- und einen Third-Level-Support sowie einen sogenannten Field Service durch ein von hiermit beauftragtes Drittunternehmen, das bei Überlastung des Dataportrechenzentrums tätig wird, erbracht. Im Hinblick auf die Dienstleistungen des Supports wurde mit den Vertretern von Dataport in verschiedenen Szenarien die

Durchführung dieser Leistungen simuliert, bei denen sich die Mitarbeiterinnen und Mitarbeiter des Supports zur Lösung eines angezeigten IT-Problems mit dem Einverständnis der jeweiligen Inhaberin beziehungsweise des jeweiligen Inhabers des Arbeitsplatzes auf deren oder dessen Arbeitsplatzrechner aufschalten und diesen auch selbsttätig steuern können.

Während der ungefähr vierstündigen Prüfung erkannte die Arbeitsgruppe einige Mängel, deren Beseitigung die Arbeitsgruppe für notwendig erachtet. Sie betreffen insbesondere den Support und die Auftragserteilung von Dataport an Subauftragnehmer. Weitere Unterlagen zur Regelung der IT-Sicherheit, die Passwortrichtlinie und das Schulungskonzept für die mit der Verarbeitung personenbezogener Daten betrauten Mitarbeiterinnen und Mitarbeiter des Unternehmens übersandte Dataport nach dem Besuch an die Arbeitsgruppe. Sie werden von der Arbeitsgruppe geprüft.

3.6 Bestellung eines Datenschutzbeauftragten durch einen Konzern

Der Betriebsrat eines Bremer Maschinenbauunternehmens, das zu einer weltweit operierenden Firmengruppe gehört, wies uns darauf hin, dass das Unternehmen bislang keine beziehungsweise keinen Datenschutzbeauftragten bestellt hatte. Da die Firma über circa 80 Mitarbeiterinnen und Mitarbeiter verfüge und Beschäftigten-, Kunden- und Lieferantendaten automatisiert verarbeite, bat er uns um Prüfung, ob von dem Unternehmen eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter zu bestellen ist.

Gemäß § 4 f Absatz 1 Bundesdatenschutzgesetz (BDSG) haben nicht öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, eine Beauftragte oder einen Beauftragten für den Datenschutz schriftlich zu bestellen. Diese Verpflichtung gilt nicht, wenn mit der automatisierten Verarbeitung höchstens neun Mitarbeiterinnen beziehungsweise Mitarbeiter ständig beschäftigt sind. Unterliegt die Verarbeitung der Daten einer Vorabkontrolle, so ist eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen zu bestellen. Einer Vorabkontrolle bedarf unter anderem die Verarbeitung besonderer Arten personenbezogener Daten, zu denen gemäß § 3 Absatz 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder politische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben zählen.

Die Geschäftsleitung des Maschinenbauunternehmens hielt die Bestellung einer oder eines betrieblichen Datenschutzbeauftragten zunächst für nicht erforderlich. Sie erklärte, dass durch die Auslagerung der Bereiche Personal und Rechnungswesen an die in Baden-Württemberg ansässige Muttergesellschaft im Rahmen einer Funktionsübertragung keine personenbezogenen Daten von ihrem Unternehmen verarbeitet würden. Ein Prüfgespräch

mit der Geschäftsleitung am Firmensitz in Bremen ergab dann jedoch, dass von ihm automatisiert personenbezogene Daten zum Beispiel zu Urlaubsanträgen, zur Auszahlung der Gehälter, zur Arbeitszeiterfassung und zu Erkrankungen der Mitarbeiterinnen und Mitarbeiter erhoben, gespeichert und an die Muttergesellschaft zur weiteren Bearbeitung übermittelt werden. Im Bereich des Einkaufs des Unternehmens werden personenbezogene Lieferantendaten und Kundendaten erhoben, gespeichert und zur Erfüllung der Aufgaben des Rechnungswesens an die Muttergesellschaft übermittelt. Darüber hinaus werden im Technikbereich des Unternehmens personenbezogene Daten der Mitarbeiterinnen und Mitarbeitern zum Beispiel für arbeitsorganisatorische Zwecke verarbeitet. Die Ermittlung der Anzahl der bei den festgestellten unterschiedlichen Verarbeitungsaktivitäten mit der Verarbeitung personenbezogener Daten beschäftigten Personen führte zu dem Ergebnis, dass diese deutlich mehr als neun beträgt und somit eine betriebliche Datenschutzbeauftragte oder ein betrieblicher Datenschutzbeauftragter zu bestellen war. Unseren vorstehenden Erläuterungen entsprechend bestellte das Unternehmen einen Datenschutzbeauftragten. Auch die Muttergesellschaft holt die bislang versäumte Bestellung einer beziehungsweise eines Datenschutzbeauftragten nach.

3.7 Datenschutzbeauftragte in Arztpraxen

Ein Unternehmen, das unter anderem medizinische Berufsgruppen in Fragen von IT-Sicherheit und IT-Konzepten betreut, wandte sich mit der Frage an uns, ob Ärztinnen und Ärzte in Bremen künftig Datenschutzbeauftragte benennen müssen. Zur Beantwortung der Anfrage wiesen wir insbesondere auf Artikel 37 Absatz 1 Buchstabe c der Datenschutzgrundverordnung (DSGVO) hin. Danach haben auch nicht öffentliche Stellen eine oder einen Datenschutzbeauftragten zu benennen, wenn die Kerntätigkeit der oder des Verantwortlichen oder der Auftragverarbeiterin beziehungsweise des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO besteht. Zu den besonderen Kategorien von Daten zählen auch Gesundheitsdaten. Die Verarbeitung von Gesundheitsdaten gehört zur Kerntätigkeit von Ärztinnen und Ärzten, da der Zweck ihrer Tätigkeit in der Behandlung und Beratung von Patienten hinsichtlich ihres Gesundheitszustands besteht. Eine umfangreiche Verarbeitung besonderer Kategorien von Daten liegt vor, wenn sie eine große Zahl von Personen betrifft und/oder beträchtliche Datenmengen über einen langen Zeitraum verarbeitet werden. Dies ist insbesondere bei der Verarbeitung von Gesundheitsdaten in Kliniken, medizinischen Versorgungszentren und Gemeinschaftspraxen der Fall. Zumindest in diesen Fällen müssen bremische Ärztinnen und Ärzte beziehungsweise die Stellen, bei denen sie beschäftigt sind, deshalb nach der DSGVO Datenschutzbeauftragte benennen.

4. Verwaltungsübergreifende Verfahren

4.1 SAP – Einheitskreditor/Einheitsdebitor

Bei der Nutzung des Verfahrens SAP wird es im Rahmen des sogenannten Einheitspersonenkontos zu Änderungen kommen, welche auch datenschutzrechtlich bewertet werden müssen. Mussten bisher für jeden Zweck einzelne Stammdatensätze (Kreditoren und Debitoren) angelegt werden, soll zukünftig auch aufgabenübergreifend auf die Daten zugegriffen werden können. Der Entwurf der Einheitspersonenkontoverordnung wurde von uns begleitet. Unsere Anmerkungen wurden beachtet und in den Entwurf übernommen. Aus unserer Sicht ist der Betrieb eines Einheitspersonenkontos möglich, eine bewertbare Aussage kann jedoch erst mit der finalen Dokumentation des Systems abgegeben werden.

4.2 Länderübergreifende Zusammenarbeit im IT-Bereich

Auch in diesem Berichtsjahr beschäftigte uns das zentrale, durch das Rechenzentrum der Anstalt öffentlichen Rechts Dataport betriebene E-Mail-System CCMS (Community Cloud Mail System). So galt es, die Stellungnahme zu prüfen und zu bewerten, die die Senatorin für Finanzen – als in Bremen für das CCMS verantwortliche Stelle – erstellt hatte. Dies geschieht in Abstimmung mit den Landesbeauftragten für Datenschutz der an CCMS beteiligten Länder, die zum Redaktionsschluss noch andauert.

Im Berichtsjahr nahmen wir zusammen mit einer Teilgruppe der Landesbeauftragten für Datenschutz der Dataportträgerländer an einer gemeinsamen datenschutzrechtlichen Prüfung teil. Gegenstand dieser Prüfung war das Verfahren Zentraler Meldebestand (ZMB). Dieses Verfahren wird in den Ländern Hamburg, Sachsen-Anhalt und Schleswig-Holstein genutzt. Die Landesbeauftragten für Datenschutz der Dataportträgerländer hatten im Vorfeld der Prüfung ein durch Dataport betriebenes Verfahren gesucht, das in allen Ländern eingesetzt wird. Da es derzeit noch kein solches Verfahren gibt, wurde ein Verfahren ausgewählt, bei dem es die größte Anzahl an Berührungspunkten gab. In Bremen ist das Verfahren ZMB nicht im Einsatz. Da aber im Rahmen der Prüfung auch zentrale Komponenten beziehungsweise von Dataport erbrachte Dienste betrachtet wurden, nahmen wir an der Prüfung teil. Besonderes Augenmerk wurde dabei auf das zentrale Speichernetzwerk Dataports, das sogenannte Storage Area Network (SAN) gelegt. Die Prüfung fand im März 2017 statt. Der auf Basis dieser Prüfung von den Landesbeauftragten für Datenschutz der Dataportträgerländer gemeinsam erstellte Sachstandsbericht wurde Dataport im Herbst 2017 zur Stellungnahme vorgelegt. Die Stellungnahme hierzu wird zum Redaktionsschluss noch zwischen uns Landesbeauftragten für Datenschutz abgestimmt und wird gemeinsam mit dem auf Basis der Stellungnahme präzisierten Sachstandsbericht die

Grundlage für den gemeinsamen Prüfbericht bilden, der den für das Verfahren ZMB verantwortlichen Stellen in den jeweiligen Ländern vorgelegt werden wird.

4.3 Microsoft Office 365

Bei Microsoft Office 365 handelt es sich um ein Office-Paket, welches nicht mehr auf dem eigenen Rechner oder in der eigenen IT-Infrastruktur, sondern in der sogenannten Cloud, also auf Servern im Internet gespeichert wird. Bei der Nutzung von Cloud-Diensten, mit deren Hilfe von überall aus auf das System zugegriffen werden und die dort gespeicherten Daten (wie beispielsweise Word-Dokumente, Excel-Tabellen und PowerPoint-Präsentationen) weitergegeben werden können, gibt es aus Sicht des Datenschutzes eine Reihe ernstzunehmender Risiken. Am Beispiel der Verwaltung (Stichwort BASIS.Bremen) wurde dies bereits im 39. Jahresbericht unter Ziffer 5.3 thematisiert.

Nachdem sich die Arbeitskreise Technik und Verwaltungsmodernisierung, der Unterarbeitskreis Datenschutz und Schule sowie die Arbeitsgruppe Internationaler Datenverkehr der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit der Problematik befasst hatten, kam man zu dem Schluss, das Thema "Microsoft Office 365" zentral in einer eigenen Unterarbeitsgruppe zu behandeln. Das Augenmerk liegt dabei auf den von Microsoft betriebenen Rechenzentren in Deutschland. Das Unternehmen plant eine Zusammenarbeit mit T-Systems als Datentreuhänder, um dem möglichen Zugriff amerikanischer Geheimdienste entgehen zu können und europäisches Datenschutzrecht einzuhalten. Die Tatsache, dass die Daten in Deutschland gespeichert werden, reicht allerdings nicht aus, um von einem datenschutzkonformen System sprechen zu können. So wird den Anwenderinnen und Anwendern eine Rund-um-die-Uhr-Unterstützung (der sogenannte follow-the-sun-support) geboten, die zu kontaktierenden Callcenter können sich dabei – je nach Tages- oder Nachtzeit – auch in Ländern außerhalb Europas befinden. Um die geeignete Unterstützung liefern zu können, ist ein Zugriff auf das System notwendig, wobei im Zweifel Daten in ein (datenschutzrechtlich unsicheres) Drittland übertragen werden. Außerdem muss es Microsoft möglich sein, zu Wartungs- und Revisionszwecken auf das System zuzugreifen. Wie genau Microsoft mit dieser Problematik umgehen wird, muss noch geklärt werden. Ein von den Datenschutzaufsichtsbehörden formulierter Fragebogen wurde von Microsoft beantwortet, eine Aussage über die teilweise sehr ausführlichen Antworten kann jedoch erst getroffen werden, nachdem diese von der Unterarbeitsgruppe im Detail überprüft worden sind. Eine Bewertung zu der datenschutzkonformen Nutzung von Microsoft Office 365 bleibt daher vorerst offen.

5. Inneres

5.1 Allgemeines zu den Polizeiverfahren

Aufgrund der Komplexität dieser beiden Systeme konnten wir die datenschutzrechtlichen Bewertungen des polizeilichen Vorgangsbearbeitungssystems @rtus und des polizeilichen Informations- und Analyseverbunds (PIAV) auch im Berichtsjahr noch nicht abschließen.

Das polizeiliche Vorgangsbearbeitungssystem @rtus (siehe hierzu 39. Jahresbericht, Ziffer 6.1 und 38. Jahresbericht, Ziffer 5.1) ist seit Januar 2014 das Basissystem der polizeilichen Arbeit, welches besonders wichtig für das Auskunftsrecht der Bürgerinnen und Bürger ist und damit den Bürgerinnen und Bürgern auf Antrag einen Überblick über die zur eigenen Person gespeicherten Einträge in diesem System geben kann. Wir erhoben keine Einwände dagegen, dass @rtus für eine Übergangszeit eine offenere Zugriffsstruktur hat. Wir empfehlen jedoch für das Jahr 2018, diese Zugriffsstruktur innerhalb des polizeilichen Systems @rtus zu beschränken.

Ein Löschkonzept für die Falldatei Rauschgift wurde uns bisher nicht vorgelegt (siehe hierzu 39. Jahresbericht, Ziffer 6.1 und 38. Jahresbericht, Ziffer 5.4). Als INPOL-Anwendung soll die Falldatei Rauschgift im Jahr 2018 durch PIAV abgelöst werden. Insoweit appellieren wir an die Polizei Bremen und die Ortspolizeibehörde Bremerhaven, nur bereinigte Rauschgiftdatenbestände nach PIAV zu migrieren.

Die offenen Themen mit den Polizeien der Freien Hansestadt Bremen sind neben dem oben genannten Polizeiverfahren @rtus und PIAV auch die jeweiligen Rahmendatenschutzkonzepte der Polizei Bremen und der Ortspolizeibehörde Bremerhaven (siehe hierzu Ziffer 5.3 dieses Berichts), das polizeiliche Informationssystem Ermittlung und Recherche, die Telekommunikationsüberwachung mit dem Landeskriminalamt Niedersachsen (siehe hierzu Ziffer 5.5 dieses Berichts) sowie das Rechen- und Dienstleistungszentrum für die Telekommunikationsüberwachung, das fehlende Datenschutzkonzept für das Verfahren INPOL-Land und der Umgang mit Desoxyribonukleinsäure (DNA) von Geschädigten im Rahmen der Spurensicherung und Spurenauswertung des Landeskriminalamts. Auch steht die Mitteilung der behördlichen Datenschutzbeauftragten über die Ergebnisse der Vorabkontrollen betreffend Intrapol (siehe hierzu 39. Jahresbericht, Ziffer 6.1 und 37. Jahresbericht, Ziffer 5.3) noch aus.

5.2 Online-Wache

Die Polizei Bremen und die Ortspolizeibehörde Bremerhaven betreiben seit Anfang des Jahres 2017 jeweils eine eigene Online-Wache. Dort ist es möglich, die Delikte Fahrraddiebstahl und Sachbeschädigung über das Internet anzuzeigen.

Bei der Polizei Bremen werden die zu übertragenden (personenbezogenen) Daten momentan mit Hilfe der Transportverschlüsselung geschützt. Eine von uns vorgeschlagene Ende-zu-Ende-Verschlüsselung konnte technisch aufgrund der bestehenden IT-Infrastruktur der Polizei Bremen noch nicht umgesetzt werden. In die bereits laufenden Planungen zur zeitnahen Umsetzung einer entsprechenden Verschlüsselung wurden wir ebenso wie die behördliche Datenschutzbeauftragte einbezogen.

Die Ortspolizeibehörde Bremerhaven hat für ihre IT-Infrastruktur bereits eine Lösung gefunden und setzt derzeit eine Ende-zu-Ende-Verschlüsselung ab dem ersten Server ein. Die Strecke von der Anwenderin beziehungsweise dem Anwender bis zu diesem ersten Server ist transportverschlüsselt. Auch hier wird momentan an einer Lösung gearbeitet, eine tatsächliche Ende-zu-Ende-Verschlüsselung von der Anwenderin beziehungsweise dem Anwender bis hin zur Polizei umzusetzen.

Trotz der unterschiedlichen Verschlüsselungsmethoden der beiden Polizeien rechnen wir in beiden Fällen mit der Umsetzung einer wirklichen Ende-zu-Ende-Verschlüsselung und werden die Projekte weiterhin begleiten.

5.3 Rahmendatenschutzkonzept

Das Rahmendatenschutzkonzept umfasst alle verfahrensübergreifenden Maßnahmen zum Schutz personenbezogener Daten. Eine datenschutzrechtliche Bewertung der einzelnen Verfahren kann daher nur mit Hilfe eines aktuellen Rahmendatenschutzkonzepts erfolgen, da auf dies entsprechend oft verwiesen wird.

Leider wurden die von uns angesprochenen Probleme mit den Rahmendatenschutzkonzepten der Polizei Bremen und der Ortspolizeibehörde Bremerhaven bisher nicht gelöst. Sind es bei dem Rahmendatenschutzkonzept der Ortspolizeibehörde Bremerhaven einzelne Punkte, die noch offen beziehungsweise zu klären sind (wie beispielsweise offensichtlich veraltete Formulierungen mit Verweis auf Microsoft Windows XP), liegt uns das Rahmendatenschutzkonzept der Polizei Bremen nach wie vor nur in der Entwurfsfassung aus dem Jahr 2009 vor.

5.4 BodyCam

Im November 2016 wurde das Projekt BodyCam bei der Polizei Bremen für den Bereich der Diskomeile und der Sielwallkreuzung gestartet (siehe hierzu 39. Jahresbericht, Ziffer 6.2). In diesem Berichtsjahr wurde der Einsatz der BodyCam evaluiert. Aus dem Abschlussbericht Projekt BodyCam (sogenannter Evaluationsbericht) vom 20. November 2017 geht hervor, dass nahezu alle betroffenen Personen (in 98 Prozent aller BodyCam-Einsätze, siehe hierzu Evaluationsbericht, Seite 8) stark alkoholisiert waren oder unter dem Einfluss von

Betäubungsmitteln standen. Der Bericht selbst kommt zu dem Schluss, dass in diesen Fällen kein präventiver oder deeskalierender Effekt durch den Einsatz einer BodyCam erreicht werden kann (siehe hierzu Evaluationsbericht, Seiten 6 und 15).

Die Aufzeichnung der BodyCam muss gemäß § 29 Absatz 5 Bremisches Polizeigesetz (BremPolG) offen erfolgen. Wir haben Zweifel daran, dass eine Ankündigung der Aufnahme zu dem Zeitpunkt, zu dem die Körperkamera bereits filmt (siehe hierzu Evaluationsbericht, Seite 5), dieser Offenheit genügt.

Die BodyCam kam in 78 Einsätzen bei 166 Einsatzsituationen zum Einsatz. Von 166 Einsatzsituationen wurden in 48 Fällen die Aufnahmen als relevant markiert. Damit waren die Aufnahmen in 108 Fällen ohne Relevanz. Diese nicht relevanten Bild- und Tonaufnahmen werden erst nach zwei Monaten gelöscht.

Im Evaluationszeitraum gab es 32 Vorgänge mit 48 relevanten personenbezogenen Ton- und Videoaufzeichnungen, wobei es auf Antrag in nur 21 Fällen zu einer Einsichtnahme der Videoaufnahmen zwecks weiterer Sachbearbeitung kam. Das wirft die Frage nach dem weiteren Umgang mit den verbliebenen, von der Polizei als relevant eingestuften Aufnahmen, die ungefähr ein Drittel der Vorgänge ausmachen, auf (siehe hierzu Evaluationsbericht, Seite 9).

Die Aufnahmetätigkeit der Polizei erfolgt in vielen Fällen zur Strafverfolgung. Die Aufnahme von Bildaufzeichnungen durch die Polizei zu Strafverfolgungszwecken wird durch § 100 h Strafprozessordnung (StPO) erlaubt (siehe hierzu Evaluationsbericht, Seiten 5 und 7). Allerdings verfügen die Körperkameras nicht nur über die Bildaufzeichnungsfunktion, sondern gleichzeitig werden mit den Bildern zusammen auch Tonaufzeichnungen angefertigt, was die präventive Erlaubnisnorm des § 29 Absatz 5 BremPolG erlaubt. Für Tonaufzeichnungen zu Strafverfolgungszwecken reicht § 100 h StPO als Rechtsgrundlage nicht aus. Vielmehr ist für die Anfertigung von Tonaufzeichnungen § 100 f StPO als Eingriffsgrundlage zur Strafverfolgung vorgesehen. Das Vorliegen der Voraussetzungen des § 100 f StPO ist dann durch die Polizei zu prüfen, um die BodyCam zur Strafverfolgung anzuschalten. Die Eingriffsschwelle von § 100 f StPO ist sehr hoch, sodass in Anhalte- oder Kontrollsituationen im öffentlichen Verkehrsraum in der Regel nicht vom Vorliegen der Tatbestandsvoraussetzungen des § 100 f StPO ausgegangen werden kann. In Bremen werden die sehr hohen Eingriffsschwellen des § 100 f StPO durch die sehr niedrigen Eingriffsschwellen des § 29 Absatz 5 BremPolG unterlaufen, sofern die BodyCam-Aufnahmen bereits im Anfertigungszeitpunkt nicht präventiver Art sind, sondern der Strafverfolgung dienen. Eine Änderung der StPO dahin gehend, dass auch Tonaufzeichnungen von § 100 h StPO erfasst werden sollen, liegt in den Händen der Gesetzgebungskompetenz des Bundes. Wir halten es für problematisch, den hauptsächlich

repressiven Einsatz der BodyCam-Aufnahme zur Beweissicherung in der Strafverfolgung durch eine präventive Befugnisnorm zu rechtfertigen. Es wird sowohl in dem Evaluationsbericht als auch in der Vorlage 19/163 vom 20. November 2017 zur Entwicklung der Videoüberwachung in Bremen der Mehrwert der Videoüberwachung für die Strafverfolgung in den Vordergrund gerückt. Die Verhinderung von Straftaten und damit der präventive, die Gefahrenabwehr beinhaltende Aspekt der Videoüberwachung ist auch nicht durch die Statistik, die einen Anstieg der Deliktszahlen vom Jahr 2014 bis zum Jahr 2016 anführt, belegt. Wir empfehlen, da die Videoüberwachung am Hauptbahnhof Bremen im Jahr 2002 und auf der Diskomeile in den Jahren 2007 und 2008 eingeführt wurde, diesbezüglich jeweils eine Statistik vor und nach Einführung von Videoüberwachung anzufertigen, um eine Aussagekraft zur Prävention von Straftaten überhaupt treffen zu können.

5.5 Telekommunikationsüberwachung

Gegenstand der aktuellen Telekommunikationsüberwachung durch die Polizeien sind allein strafrechtliche Ermittlungen. Insofern gehört die Telekommunikationsüberwachung gegenwärtig zum repressiven Bereich der Polizeiarbeit. Für den präventiven Bereich, also den Bereich der Gefahrenabwehr durch die Polizeien, zu dessen Regelung uns am Ende des Berichtsjahres ein Gesetzentwurf zur Änderung des bremischen Polizeirechts erreichte, der unter anderem eine Rechtsgrundlage für die präventive Telekommunikationsüberwachung beinhaltet (siehe hierzu Ziffer 5.7 dieses Berichts), gibt es bislang in Bremen keine Rechtsgrundlage.Im Oktober des Berichtsjahres diskutierten wir mit der Polizei Bremen aktuelle datenschutzrechtliche Probleme der repressiven Telekommunikationsüberwachung. Hierbei handelt es sich zum Beispiel um die lückenhafte Dokumentation des Betriebskonzepts, die fehlende Risikoanalyse und die fehlenden Netzpläne, die Unklarheiten in Bezug auf das Rechte-Rollen-Konzept, die unzureichende Verschlüsselung sowie die fehlende Mandantentrennung zwischen den jeweiligen polizeilichen Daten der Bundesländer und den Daten der verschiedenen Telekommunikationsüberwachungen. Sowohl die Dokumentation des Datenschutzkonzepts für die repressive Telekommunikationsüberwachung zusammen mit dem Landeskriminalamt Niedersachsen (siehe hierzu 37. Jahresbericht, Ziffer 5.2, 38. Jahresbericht, Ziffer 6.1 und 39. Jahresbericht, Ziffer 6.1) als auch die Überarbeitung des zugrunde liegenden Verwaltungsabkommens stehen noch aus. Ob den datenschutzrechtlich bemängelten Punkten abgeholfen werden wird, erscheint mit Blick auf das künftige Rechen- und Dienstleistungszentrum für die Telekommunikation mit den Polizeien der norddeutschen Bundesländer, dessen Inbetriebnahme für das Jahr 2020 anvisiert wird, zweifelhaft. Wir halten es aber weiterhin für erforderlich, den datenschutzrechtlichen Belangen Rechnung zu tragen und einzelne datenschutzrelevante Mängel zu beseitigen, da es sich um sensible personenbezogene Daten von tatverdächtigen Personen handelt.

5.6 Alternierende Telearbeit bei der Polizei

Die Polizei Bremen wollte ihren Mitarbeiterinnen und Mitarbeitern für Vorgänge einfacher Sachbearbeitung die alternierende Telearbeit anbieten. Das Arbeiten mit der klassischen Papierakte sollte am heimischen Arbeitsplatz nicht stattfinden. Der Zugriff auf die polizeilichen Informationssysteme war aus Sicht der Polizei zwingend erforderlich.

Für unsere Prüfung des Projekts aus datenschutzrechtlicher Sicht war unter anderem entscheidend, wo die Datenverarbeitung stattfindet, ob die Daten innerhalb des Systems verbleiben, ob der Zugang zu dem System zeitlich begrenzt ist und wie detailliert die Ereignisse protokolliert werden. Im Laufe der Zeit konnte die Polizei sämtliche Kritikpunkte ausräumen, sodass der alternierenden Telearbeit bei der Polizei Bremen aus unserer Sicht nichts mehr im Wege steht: Die Datenverarbeitung findet ausschließlich auf den Servern der Polizei und nicht auf dem Telearbeitsrechner statt; die Weitergabekontrolle wird eingehalten, da es weder per Ausdruck noch mittels externem Speichermedium möglich ist, unbefugte Kopien zu erzeugen; der Zugang zu dem System ist zeitlich begrenzt und es findet eine lückenlose Protokollierung statt. Zusätzlich wird die alternierende Telearbeit durch die behördliche Datenschutzbeauftragte kontrolliert.

5.7 Entwurf zur Änderung des Bremischen Polizeigesetzes

Der uns im November des Berichtsjahres zur Stellungnahme vorgelegte Entwurf zur Änderung des Bremischen Polizeigesetzes (BremPolG-E) wirft erhebliche rechtsstaatliche und datenschutzrechtliche Bedenken auf. Er enthält verschiedene polizeiliche Befugnisse für den präventiven Bereich wie zum Beispiel die neue Befugnis zur elektronischen Aufenthaltsüberwachung (auch elektronische Fußfessel genannt), die Erweiterung der Videoüberwachungsbefugnisse und die Schaffung neuer Telekommunikationsbefugnisse. Zu den Telekommunikationsbefugnissen zählen die klassische Telekommunikationsüberwachung, die Erhebung von Verkehrsdaten und von Bestandsdaten in der Telekommunikation, die Quellen-Telekommunikationsüberwachung und die Standortermittlung in der Telekommunikation.

Die Grenzen für gesetzgeberische Eingriffe in das Recht auf informationelle Selbstbestimmung ergeben sich unmittelbar aus der Verfassung. Die Ausgestaltung von Eingriffsbefugnissen muss dabei vor allem dem Grundsatz der Verhältnismäßigkeit genügen. Eingriffsbefugnisse sind zudem an dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit zu messen. Diesen Anforderungen wird der Gesetzentwurf, der einzelne Instrumente sowohl des derzeit geltenden Bundeskriminalamtgesetzes (BKAG) als auch des ab dem 25. Mai 2018 geltenden Bundeskriminalamtgesetzes übernimmt, in wesentlichen Teilen nicht gerecht.

Die entsprechenden Bestimmungen des derzeit geltenden Bundeskriminalamtgesetzes waren Gegenstand einer Verfassungsbeschwerde, über die das Bundesverfassungsgericht mit Urteil vom 20. April 2016 entschieden hatte (siehe hierzu 39. Jahresbericht, Ziffer 6.4). Nach diesem Urteil ist von zentraler Bedeutung für die Verfassungsmäßigkeit heimlicher Überwachungsmaßnahmen der Polizei im präventiven Bereich, dass diese auf die Abwehr von Gefahren des internationalen Terrorismus beschränkt sind, da nur Schutzgüter von hohem verfassungsrechtlichem Gewicht tief in die Privatsphäre eingreifende Ermittlungsbefugnisse und Überwachungsbefugnisse überhaupt rechtfertigen können. Sämtlichen im neuen Bundeskriminalamtgesetz enthaltenen heimlichen Ermittlungs- und Überwachungsbefugnisse, die das Bundesverfassungsgericht in seinem Urteil als dem Grunde nach noch verfassungsgemäß akzeptiert hatte, liegt deshalb die gesetzliche Beschränkung auf die Terrorismusabwehr zugrunde. Der Begriff des internationalen Terrorismus ist dabei durch die Aufgabenbeschreibung des Bundeskriminalamts im Zusammenhang mit der Abwehr von Gefahren des internationalen Terrorismus definiert. Dementsprechend enthält das neue Bundeskriminalamtgesetz eine ausdrückliche Definition des Begriffs der "Gefahren des internationalen Terrorismus".

Im BremPolG-E wird dagegen versucht, die vom Bundesverfassungsgericht in seiner BKAG-Entscheidung formulierten Anforderungen mit Hilfe einer eigenen Begriffsbestimmung umzusetzen. In § 2 BremPolG-E wird der bislang im Polizeirecht unbekannte und im Strafgesetzbuch nicht verwendete Begriff der "terroristischen Straftat" neu eingeführt. Aus unserer Sicht müsste der Verwendung dieses Begriffs in einem Landespolizeigesetz eine Änderung des Strafgesetzbuchs vorangehen, die verdeutlichen würde, welche Straftaten der Bundesgesetzgeber als "terroristische" Straftaten ansieht. Einmal davon abgesehen, dass für entsprechende Regelungen im Hinblick auf die konkurrierende Gesetzgebungskompetenz des Bundes für das Strafrecht eine Landesgesetzgebungskompetenz insofern schwer zu begründen sein wird, ist die geplante Neuschaffung des Begriffs der "terroristischen Straftat" auch in inhaltlicher Hinsicht verfassungsrechtlich problematisch und schwer vereinbar mit der polizeirechtlichen Ausrichtung an der Aufgabe der Gefahrenabwehr, die – soweit es um die Abwehr von Gefahren des internationalen Terrorismus geht – zudem in den präventivpolizeilichen Zuständigkeitsbereich des Bundeskriminalamtes fällt. Wir haben deshalb zum Verzicht auf die Einführung des Begriffs der "terroristischen Straftat" geraten.

Entgegen der Forderung des Bundesverfassungsgerichts beschränkt sich der Gesetzentwurf zum BremPolG bei der Schaffung der Überwachungsbefugnisse nicht auf die Zielsetzung der Abwehr von Straftaten mit terroristischem Hintergrund. Anders als dies im alten und auch im neuen BKAG der Fall ist, enthält der Entwurf keine entsprechende Beschränkung bei der Videoüberwachung gemäß § 29 Absatz 3 Nummer 1 und Nummer 2 BremPolG-E, bei der elektronischen Aufenthaltsüberwachung gemäß § 33 f Absatz 2 BremPolG-E, bei der

Standortermittlung gemäß § 33 c Ansatz 3 Nummer 2 BremPolG und auch nicht bei der Bestandsdatenerhebung gemäß § 33 d BremPolG-E ("für eine Gefahr Verantwortliche"). Auch bei den weiteren geplanten Befugnissen zur Telekommunikationsüberwachung gemäß §§ 33 a bis 33 c BremPolG-E, den Befugnissen der Videoüberwachung gemäß § 29 Absatz 3 Nummer 3 und Nummer 4 BremPolG-E und der elektronischen Aufenthaltsüberwachung gemäß § 33 f Absatz 1 BremPolG-E wird nicht ausschließlich auf die Straftaten mit terroristischem Bezug genommen. Vor dem Hintergrund der BKAG-Entscheidung des Bundesverfassungsgerichts haben wir große Zweifel, dass dies verfassungsrechtlich haltbar ist.

Auch im Hinblick auf die schon gegenwärtig bestehenden Probleme bei der länderübergreifenden Telekommunikationsüberwachung (siehe hierzu Ziffer 5.7.1 dieses Berichts), die die Richtung der Bundesverfassungsgerichtsentscheidung zum BKAG verzerrende Teilumsetzung des Urteils (siehe hierzu Ziffer 5.7.2 dieses Berichts), die Schwierigkeiten eines Vorbehalts der Anordnung präventiven Polizeihandelns durch Amtsgerichte (siehe hierzu Ziffer 5.7.3 dieses Berichts) und die noch ausstehenden Umsetzungen der JI-Richtlinie und der Datenschutzgrundverordnung (siehe hierzu Ziffer 5.7.4 dieses Berichts) haben wir Bedenken gegen den Entwurf zur Änderung des Bremischen Polizeigesetzes geäußert.

5.7.1 Probleme der länderübergreifenden Telekommunikationsüberwachung

Vor dem Hintergrund, dass das Rechen- und Dienstleistungszentrum für die Telekommunikationsüberwachung zusammen mit den Polizeien der anderen norddeutschen Bundesländer erst nach dem Jahr 2020 in Betrieb genommen werden soll, scheinen die die Überwachungsbefugnisse im Telekommunikationsbereich betreffenden Passagen des Gesetzentwurfs zur Änderung des Bremischen Polizeigesetzes (BremPolG) übereilt. Die bestehende Telekommunikationsüberwachungsanlage ist mit vielen datenschutzrechtlichen Mängeln behaftet (siehe hierzu Ziffer 5.5 dieses Berichts, 39. Jahresbericht, Ziffer 6.1, 38. Jahresbericht, Ziffer 6.1 und 37. Jahresbericht, Ziffer 5.2) Deshalb raten wir von einer Nutzung etwaiger neuer Befugnisse im Rahmen des Betriebs der Telekommunikationsüberwachung mit dem Landeskriminalamt Niedersachsen ab, solange keine Lösung gefunden wurde, die diese Mängel behebt.

Da die Überprüfbarkeit der Nutzung von Überwachungsbefugnissen bei nicht hinreichend bestimmten oder nicht hinreichend normklaren Befugnisnormen problematisch ist, empfehlen wir, im Entwurf umfangreiche Dokumentationsverpflichtungen, unter anderem in den Sätzen 3 und 6 des § 33 e Absatz 4 BremPolG, zu begründen. Zusätzlich empfehlen wir eine gesetzliche Verpflichtung zur Evaluation neuer Überwachungsbefugnisse und zum Bericht

an die Bremische Bürgerschaft zumindest über die jährliche Anzahl der jeweiligen Überwachungsmaßnahmen ähnlich der statistischen Erfassung und Berichtspflicht gemäß § 101 b Strafprozessordnung.

5.7.2 Teilumsetzung der Bundesverfassungsgerichtsentscheidung

Die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz (BKAG) wird durch den Gesetzentwurf nur teilweise umgesetzt. Dies halten wir für verfassungsrechtlich problematisch. Auch wirkt es, als würden nur die Rosinen aus der Entscheidung herausgepickt.

Mit dem Gesetzentwurf soll die Polizei weitere Befugnisse für verdeckte Maßnahmen erhalten. Hierbei ist die Auseinandersetzung mit einem wichtigen Grundsatz der BKAG-Entscheidung nicht erkennbar. Danach muss bei der Prüfung der Verfassungsmäßigkeit neuer Maßnahmen die Kumulation dieser neuen mit den bisherigen verdeckten Befugnissen (und die Kumulation auch der bisherigen verdeckten Maßnahmenbefugnisse miteinander) berücksichtigt werden. Eine nur unvollständige Anpassung des bremischen Polizeirechts an die vom Bundesverfassungsgericht formulierten Maßstäbe bewirkt, dass die Wertungen der Entscheidung des Bundesverfassungsgerichts aus dem Kontext gerissen werden und es unklar ist, ob zum Beispiel eine Regelung geschaffen werden wird, die die Kumulation von verdeckten Maßnahmen und ihre Auswirkungen auf das informationelle Selbstbestimmungsrecht berücksichtigen wird. Im vorliegenden Gesetzentwurf fehlt eine solche Regelung jedenfalls.

Außerdem wird in den neuen Befugnisnormen auf die Benachrichtigung in § 33 Absatz 5 des Bremischen Polizeigesetzes (BremPolG) verwiesen, obwohl auch diese Norm nach der Entscheidung des Bundesverfassungsgerichts einer Überarbeitung bedarf. Auch ist zweifelhaft, ob die Berichtspflicht der Polizei gegenüber der Bremischen Bürgerschaft gemäß § 36 BremPolG den Anforderungen des Bundesverfassungsgerichts genügt oder eine schriftliche Berichtspflicht mit vorgegebenen Einzelheiten auszugestalten ist. Diese Beispiele können nur ein kleines Schlaglicht auf die Problematik einer teilweisen Anpassung des Polizeirechts werfen. Wir empfehlen daher eine vollständige Anpassung des Polizeirechts an die Rechtsprechung des Bundesverfassungsgerichts.

5.7.3 Vorbehalt der Anordnung präventiven Polizeihandelns durch Amtsgerichte

Für einen Systembruch halten wir es, dass eine Reihe polizeilicher Maßnahmen nach dem Gesetzentwurf unter dem Vorbehalt einer Anordnung durch Richterinnen oder Richter des Amtsgerichts stehen, obwohl es sich um präventive, nicht repressive, also der

Strafverfolgung dienende Maßnahmen der Polizei handelt. Dies kollidiert damit, dass gegen präventive polizeiliche Maßnahmen der Rechtsweg zu den Verwaltungsgerichten eröffnet ist. In diesem Zusammenhang ist uns bekannt, dass bereits derzeit einige im Bremischen Polizeigesetz geregelte präventive polizeiliche Maßnahmen unter dem Vorbehalt der Anordnung durch Richterinnen oder Richter am Amtsgericht stehen. Der bremische Gesetzgeber sollte gleichwohl erwägen, die richterliche Entscheidung über entsprechende präventiv polizeiliche Maßnahmen ausdrücklich dem Oberverwaltungsgericht zuzuweisen, wie dies zum Beispiel im Polizeirecht in Rheinland-Pfalz der Fall ist.

5.7.4 Ausstehende Umsetzung der JI-Richtlinie und der DSGVO

Vor dem Hintergrund, dass die JI-Richtlinie vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr bis zum 6. Mai 2018 umgesetzt sein muss, haben wir die Aufnahme entsprechender Normen in den Entwurf zur Änderung des Bremischen Polizeigesetzes (BremPolG) angeregt. Eine entsprechende Anregung zur Änderung des BremPolG haben wir auch in Bezug auf die Geltung der Datenschutzgrundverordnung (DSGVO) ab 25. Mai 2018 gegeben, die im Bereich des Polizeirechts für die nicht auf Straftaten bezogene Gefahrenabwehr wie Suizidfälle und für den Schutz privater Rechte gilt und zu einer Änderung des BremPolG führt. Werden keine entsprechenden Änderungen im BremPolG vorgenommen, sind Regelungen des BremPolG, die der DSGVO entgegenstehen, ab dem 26. Mai 2018 nicht anwendbar.

5.8 Elektronische Akte beim Verfassungsschutz

Im April des Berichtsjahres wurden Vorschriften in das Bremische Verfassungsschutzgesetz (BremVerfSchG) aufgenommen, die es dem Landesamt für Verfassungsschutz ermöglichen, eine elektronische Akte zu führen. Mit dieser Änderung des Bremischen Verfassungsschutzgesetzes wurde unsere Forderung nach einer spezialgesetzlichen Bestimmung zur Führung von elektronischen Akten in einem Vorgangsbearbeitungssystem durch den Verfassungsschutz umgesetzt. Das Landesamt für Verfassungsschutz darf gemäß § 6 Absatz 6 BremVerfSchG zur Vorgangsverwaltung, zur befristeten Dokumentation seines Handelns, zu Zwecken der Datenschutzkontrolle und zur Sicherstellung des ordnungsgemäßen Betriebs seiner Datenverarbeitungsanlage personenbezogene Daten speichern. Der § 11 Absatz 2 BremVerfSchG erlaubt jetzt auch die Führung von Akten in elektronischer Form. Wichtig war in diesem Zusammenhang, dass der Auskunftsanspruch der Bürgerinnen und Bürger gegenüber dem Landesamt für Verfassungsschutz sich auch auf personenbezogene Daten, die in elektronischer Form gespeichert sind, erstreckt.

Mit dieser Änderung des Bremischen Verfassungsschutzgesetzes ging eine Änderung betreffend der Personenspeicherungen einher, die die Altersgrenze bei Minderjährigen von 16 Jahren auf 14 Jahre herabstufte. Diese Änderung wird dazu führen, dass mehr Personen gespeichert werden. Wir sehen diese Entwicklung kritisch, die es ermöglicht, bereits Kinder, die nicht voll geschäftsfähig sind, zu beobachten und ihre Daten zu speichern. Die Streichung der gesetzlichen Verpflichtung zur Evaluierung halten wir gerade vor dem Hintergrund der beschriebenen Erweiterung des Anwendungsbereichs des Bremischen Verfassungsschutzgesetzes für bedenklich.

5.9 Meldedatenübermittlungsverordnung

Im Juni des Berichtsjahres erhielten wir den Entwurf für eine Bremische Meldedatenübermittlungsverordnung, die im Oktober in Kraft trat. Diese Verordnung machte von Befugnissen für den Erlass landesrechtlicher Bestimmungen Gebrauch, die sich aus dem neuen Bundesmeldegesetz (BMG) ergeben. Danach können Gegenstand landesrechtlicher Bestimmungen sowohl regelmäßige Datenübermittlungen zur Aufgabenerfüllung als auch Erweiterungen des im BMG vorgesehenen Datensatzes bei Datenübermittlungen oder automatisiertem Datenabruf sein, soweit dadurch Anlass und Zweck der Übermittlung festgelegt und die Datenempfängerin beziehungsweise der Datenempfänger sowie die zu übermittelnden Daten bestimmt werden. Durch die Verordnung erfolgt darüber hinaus eine Anpassung der bremischen Regelungen an die Bestimmungen der ab 25. Mai 2018 geltenden Datenschutzgrundverordnung. Auch bedurfte es einer Überarbeitung der alten Meldedatenübermittlungsverordnung.

Durch die Verordnung werden beispielsweise die Datenübermittlungen der Meldebehörde an die Schulverwaltung erweitert, weil der Verordnungsgeber aufgrund der Förderung der beruflichen Ausbildung oder eines Studiums im Rahmen der Aufgabe der Berufsjugendagentur der Freien Hansestadt Bremen die Erweiterung der Datenübermittlung auf 5 bis 25-jährige Personen bei der Überwachung der Schulpflicht für erforderlich hält. Ein weiteres Beispiel sind erweiterte Datenübermittlungsbefugnisse zur Organisation der Kindertagesbetreuung, die gewährleisten sollen, dass die sich durch Geburten, Umzüge und Zuzüge kontinuierlich verändernden Bedarfe bei der Planung des Kinderbetreuungsangebots angemessene Berücksichtigung finden können. Die Rechtsgrundlage für diese Datenübermittlungen ergibt sich aus dem Achten Sozialgesetzbuch. Ein weiteres Beispiel sind erweiterte Datenübermittlungen an die Gesundheitsämter zum Beispiel zur Einladung zur Teilnahme an Früherkennungsuntersuchungen für Kinder (U4 bis U9) und zur Durchführung des Beratungsprogramms TippTapp. Die Rechtsgrundlage für diese Datenübermittlungen ergibt sich aus dem Gesetz über den Öffentlichen Gesundheitsdienst im Land Bremen und dem Gesetz zur Kooperation und Information im Kinderschutz.

Dem Amt für Soziale Dienste Bremen wurde durch die Verordnung der automatisierte Abruf von personenbezogenen Daten der Meldebehörde zur Erfüllung der gesetzlichen Aufgaben im Zusammenhang mit Vaterschaftsfeststellungen, Vaterschaftsanerkennungen und Unterhaltsansprüchen ermöglicht. Beistände für Minderjährige wie das Amt für Soziale Dienste Bremen sind bei Beurkundungen von Vaterschaftsanerkennungen verpflichtet, zu prüfen, ob die Vaterschaftsanerkennung missbräuchlich ist. Hierzu ist es aus Sicht des Verordnungsgebers erforderlich, dass der Fachdienst Beistandschaft Zugriff auf die personenbezogenen Daten des künftigen Vaters erhält.

In den Beratungen wurden letztendlich alle unsere datenschutzrechtlichen Anforderungen berücksichtigt.

6. Justiz

6.1 Datenschutz bei Gerichten

Unabhängig von der Reichweite der Aufsichtszuständigkeit der Landesbeauftragten für Datenschutz müssen Gerichte das materielle Datenschutzrecht einhalten. Auch im Berichtsjahr beschwerten sich Bürgerinnen und Bürger in einigen Fällen bei uns über Datenweitergaben der Gerichte.

Ob wir für die Überprüfung solcher Beschwerden zuständig sind, bemisst sich nach § 1 Absatz 4 Satz 1 Bremisches Datenschutzgesetz. Danach unterliegen Gerichte nur insoweit der datenschutzrechtlichen Kontrollbefugnis der Landesbeauftragten für Datenschutz, als sie in Verwaltungsangelegenheiten tätig werden. Damit gibt es zwar keine generelle Unzuständigkeit der Landesbeauftragten für Datenschutz für Gerichte, aber in laufenden Gerichtsverfahren werden wir aufgrund der richterlichen Unabhängigkeit nicht tätig.

Wie der Begriff der Verwaltungsaufgaben zu verstehen ist, ist umstritten und führte in der Vergangenheit immer wieder zu divergierenden Auffassungen zwischen der Landesbeauftragten für Datenschutz und den Gerichten. Jedenfalls hat der Gesetzgeber nicht nur eine Zuständigkeit für die Verwaltung von Sachmitteln gemeint. Vielmehr wollte der Gesetzgeber die richterliche Unabhängigkeit beachten. Richterinnen und Richter sind nach Artikel 97 Grundgesetz, dem Deutschen Richtergesetz und dem Gerichtsverfassungsgesetz unabhängig und nur dem Gesetz unterworfen. Diese Unabhängigkeit entstammt dem Grundsatz der Gewaltenteilung, nach dem die rechtsprechende Gewalt ausschließlich den Richterinnen und Richtern anvertraut ist. Ergänzt wird die sachliche Unabhängigkeit durch die persönliche Unabhängigkeit, die den Schutz vor persönlichen Sanktionen für missbilligte Entscheidungen gewährt. Die Richterin beziehungsweise der Richter soll in ihren

beziehungsweise seinen Entscheidungen frei von Einflussnahme, auch durch Rechtfertigungsgründe, sein. Wir nehmen deshalb selbstverständlich keine datenschutzrechtliche Prüfung von richterlichen Entscheidungen vor.

Die richterliche Unabhängigkeit bezieht sich dabei nicht nur auf die reine Spruchtätigkeit, sondern auch auf diejenigen Tätigkeiten, die mit der Rechtsfindung in unmittelbarem Zusammenhang stehen, wie Terminbestimmungen, Vernehmungen von Zeugen, sitzungspolizeiliche Maßnahmen, aber auch das Abfassen der Entscheidungsgründe.

Sofern aber Schriftsätze, Urteile oder Testamente ohne sachliche Gründe oder eine Rechtsgrundlage an Dritte oder Rechtsanwältinnen beziehungsweise Rechtsanwälte weitergegeben werden, steht dies mit der Rechtsfindung nicht in unmittelbarem Zusammenhang und ist daher nicht von der richterlichen Unabhängigkeit geschützt. Auch bei der Texterfassung, Weiterleitung, Bearbeitung von Daten und der Datensicherung muss geltendes Datenschutzrecht beachtet werden. Sofern uns darauf bezogene Eingaben erreichen, werden wir diese deshalb auch künftig bearbeiten.

6.2 Veröffentlichungen von Gerichtsentscheidungen

In den letzten Jahren gab es mehrere Fälle, in denen sich Bürgerinnen und Bürger an uns wandten, weil sie sich durch die Veröffentlichung von Gerichtsentscheidungen in ihrem Recht auf informationelle Selbstbestimmung, in ihrem allgemeinem Persönlichkeitsrecht und ihren Rechten aus dem Bremischen Datenschutzgesetz verletzt fühlten (siehe hierzu 38. Jahresbericht, Ziffer 6.3). Auch wenn die betroffenen Gerichte in Bremen Änderungen zur Anonymisierung zeitnah vornahmen, blieb das Problem, dass eine vollständige Korrektur einer Veröffentlichung im Internet fast immer unmöglich ist. Gegenstand eines Austauschs zu dieser Thematik mit dem Senator für Justiz und Verfassung und den Pressesprecherinnen und Pressesprecher der Gerichte zu Beginn des Berichtsjahres war insofern die folgende rechtliche Situation: Das Bundesverfassungsgericht und die verschieden Verwaltungsgerichte entscheiden immer wieder, dass Gerichte dazu verpflichtet sind, bestimmte Gerichtsurteile zu veröffentlich. Zuvor sollen die zu veröffentlichen Entscheidungen anonymisiert werden. Nach Erwägungsgrund 26 der Datenschutzgrundverordnung sind anonymisierte Informationen personenbezogener Daten, die derart verändert wurden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Ähnlich wird der Begriff im derzeit geltenden Bremischen Datenschutzgesetz definiert. Für die Frage der Identifizierbarkeit einer natürlichen Person müssen dabei alle Mittel berücksichtigt werden, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die Person direkt oder indirekt zu identifizieren. In der Praxis werden häufig die Namen, Orte und Straßen im Rubrum und in der Entscheidung gelöscht oder geschwärzt. Dies reicht aber nicht immer zur Anonymisierung des Urteils aus. Auch ist zu beachten, dass

bei konkreten einzelfallbezogenen Anfragen der Presse zu einem bestimmten Fall oder zu einer bestimmten Person, das Urteil vor der Herausgabe anonymisiert werden muss, auch wenn die Presse weiß, um wen es sich handelt. Dabei müssen persönliche Angaben und Umstände und besondere Arten von personenbezogenen Daten wie zum Beispiel auch Gesundheitsdaten nach dem Bundesverfassungsgericht geschwärzt werden.

Die Sprecherinnen und Sprecher der verschiedenen Gerichte erläuterten uns, dass die Beantwortung und die Weitergabe von Urteilen an die Presse und die Internetseiten der Gerichte in ihrem Aufgabenbereich liege, wohingegen es die jeweils zuständigen Richterinnen und Richter seien, die für die Veröffentlichung ihrer Gerichtsentscheidungen in Fachzeitschriften zur Rechtsfortbildung eigenständig verantwortlich seien.

6.3 Protokollierung lesender Zugriffe bei der Staatsanwaltschaft

Ein Bürger beschwerte sich bei uns, dass ein Mitarbeiter der Staatsanwaltschaft Bremen Abfragen für private Zwecke über Bekannte und über den Ausgang einer privat getätigten Anzeige ohne dienstliche Veranlassung getätigt habe. Der Abruf personenbezogener Daten, die nicht offenkundig sind, ist nur zulässig, wenn die Kenntnis zur Aufgabenerfüllung der Person erforderlich ist. Alle Mitarbeiterinnen und Mitarbeiter im öffentlichen Dienst werden über die einschlägigen Datenschutzvorschriften und das Datengeheimnis belehrt und müssen diese Belehrung durch Unterschrift bestätigen. Sofern sich erwiesen hätte, dass vorsätzlich unbefugt personenbezogene Daten abgerufen worden wären, hätte im Fall der genannten Beschwerde zumindest eine Ordnungswidrigkeit nach § 38 Absatz 1 Bremisches Datenschutzgesetz im Raum gestanden. Der Tatbestand der Ordnungswidrigkeit des unbefugten Abrufs wäre bereits mit Ausführung der Abfrage vollendet gewesen, da es nicht darauf ankommt, ob ein Abruf tatsächlich dazu führt, dass sich die oder der Betreffende erfolgreich geschützte personenbezogene Daten verschafft hat.

Zu unserem großen Bedauern konnte der Sachverhalt aufgrund der fehlenden Protokollierungsfunktion, des von der Staatsanwaltschaft Bremen verwendeten Informationstechnikverfahrens web-sta nicht ermittelt werden. Dieses IT-Verfahren unterstützt die Staatsanwaltschaft bei der Registrierung und Verwaltung von Akten und bei der Schriftguterstellung. Die Software web-sta beinhaltet nur Metadaten und keinen kompletten Akteninhalt. Vorgeworfene Straftaten, vollständiger Name der oder des Beschuldigten und der Ausgang des Verfahrens können jedoch über die Metadaten in Erfahrung gebracht werden. Bei der Staatsanwaltschaft haben etwa 180 und bei der Generalstaatsanwaltschaft etwa sieben Mitarbeiterinnen und Mitarbeiter eine Zugriffsberechtigung auf web-sta. Alle Mitarbeiterinnen und Mitarbeiter haben einen lesenden Zugriff. Davon sind nur bestimmte Bereiche ausgenommen wie etwa Ermittlungsverfahren im Zusammenhang mit organisierter Kriminalität oder

Kinderpornografie. Lesende Zugriffe werden nicht protokolliert. Der schreibende Zugriff ist mit Zugriffsberechtigungen differenziert geregelt. Die Servicekräfte haben aufgrund abteilungsübergreifender Vertretungssituationen volle Leserechte und Schreibrechte. Bei den schreibenden Zugriffen wie dem Erfassen, Ändern oder Löschen erfolgt eine systemseitige Protokollierung.

Dass es bei web-sta an einer Protokollierung des lesenden Zugriffs fehlt, wird schon seit längerem von uns kritisiert (siehe hierzu 38. Jahresbericht, Ziffer 6.2). Mit Hilfe der Protokollierung hätte im soeben berichteten Fall überprüft werden können, ob ein solcher Zugriff auf die Daten erfolgte oder sich der Vorwurf als haltlos erwiesen hätte. Diese Überprüfung des in der Beschwerde formulierten Vorwurfs war aufgrund der fehlenden Protokollierung nicht möglich. Wir erwarten deshalb, dass die von uns kontaktierte Staatsanwaltschaft Bremen diese Lücke der Protokollierung so bald wie möglich schließt.

6.4 Gesundheitsdaten im Justizvollzug

Da in einigen Bundesländern die Akten der Insassen von Strafvollzugsanstalten mit einer Kennung "Blutkontakt vermeiden" versehen worden waren und die jeweiligen Anstaltsleitungen über bestehende HIV-Infektionen automatisch unterrichtet wurden, wandte sich die Deutsche AIDS-Hilfe an uns. Dies nahmen wir zum Anlass, bei der Leitung der Justizvollzugsanstalt Bremen nachzufragen, ob die Bediensteten über eine HIV-Infektion von Gefangenen informiert werden und wie mit HIV-Infektionen und anderen gesundheitlichen Daten von Gefangenen umgegangen wird.

Unsere Abfrage ergab, dass keine datenschutzrechtlichen Bedenken bezüglich des Umgangs mit HIV-Infektionen im Strafvollzug in Bremen bestehen, da die Mitarbeiterinnen und Mitarbeiter nicht über Erkrankungen der Insassen informiert werden. Vielmehr seien alle in der Justizvollzugsanstalt gehalten, sich gegenüber sämtlichen Insassen so zu verhalten, dass eventuell bestehende Infektionsrisiken professionell beherrscht werden könnten. Das gelte auch für die Anstaltsleitung. Eine Ausnahme bestehe lediglich für Ärztinnen und Ärzte der Anstalt und Mitarbeiterinnen und Mitarbeiter des ärztlichen Dienstes, die mit der medizinischen Behandlung der einzelnen Insassen betraut seien. Dort gälten die Grundsätze der ärztlichen Schweigepflicht. In der medizinischen Behandlung und einer eventuell ärztlich veranlassten besonderen Versorgung, beispielsweise besonderer Ernährung, liege die einzige Ungleichbehandlung gegenüber nicht Infizierten.

7. Gesundheit

7.1 Formulare für Schweigepflichtentbindungserklärungen

Im Dezember 2014 wandte sich das Gesundheitsamt Bremerhaven an uns und bat um Beratung hinsichtlich des datenschutzgerechten Einsatzes von Einwilligungs- und Schweigepflichtentbindungserklärungen für die Erhebung und die Übermittlung von Klientendaten an Dritte, wie beispielsweise andere Behörden, Krankenkassen, Pflegekassen, Ärztinnen und Ärzte oder Krankenhäuser. Das Gesundheitsamt hatte Musterentwürfe mit Freitextfeldern erstellt, die von der zuständigen Mitarbeiterin oder vom zuständigen Mitarbeiter im Einzelfall um die relevanten Informationen ergänzt werden sollten. Dazu informierten wir das Gesundheitsamt über die gesetzlichen Anforderungen, denen eine Einwilligungs- und Schweigepflichtentbindungserklärung genügen müssen. Danach muss eine ausreichende Konkretisierung erfolgen, sodass für die Betroffenen klar erkennbar ist, welche Daten zu welchen Zwecken bei welchen Stellen erhoben werden sollen. Sofern die Daten bei schweigepflichtigen Personen erhoben beziehungsweise von diesen übermittelt werden sollen, müssen diese auch namentlich benannt werden. Zudem ist auf die Freiwilligkeit der Erklärung hinzuweisen und die Folgen der Verweigerung der Erklärung sind konkret im Formular zu benennen. Aus diesen Gründen sehen wir ein Formular sehr kritisch, das für eine Vielzahl von unterschiedlichen Anwendungsfällen im Hinblick auf die beteiligten Institutionen, Art und Umfang der Daten erstellt wird, und das viele Freitextfelder enthält, die im Einzelfall von der jeweiligen Mitarbeiterin beziehungsweise dem jeweiligen Mitarbeiter korrekt und vollständig ausgefüllt werden müssen. Ein solches Verfahren birgt das Risiko, dass in der Praxis nicht der für eine Wirksamkeit der Erklärung notwendige Konkretisierungsgrad erreicht wird. Wir rieten dem Gesundheitsamt daher, mehrere Formulare für jeweils bestimmte Fallkonstellationen zu erstellen.

Im Juni 2015 erhielten wir vom Gesundheitsamt überarbeitete Entwürfe. Anstelle der vom Gesundheitsamt abgelehnten Differenzierung der Formulare für bestimmte Fallkonstellationen hatte das Gesundheitsamt eine Handlungsanleitung für die eigenen Mitarbeiterinnen und Mitarbeiter erstellt, um so einen datenschutzgerechten Einsatz in der Praxis zu erreichen. In den überarbeiteten Entwürfen waren unsere inhaltlichen Anforderungen überwiegend umgesetzt. Aufgrund der genannten Probleme einer Mustereinwilligung mit Freitextfeldern hielten wir weitere Maßnahmen für notwendig, um soweit wie möglich sicherzustellen, dass der praktische Einsatz der Formulare den datenschutzrechtlichen Anforderungen auch tatsächlich entspricht. Deshalb forderten wir, das sichergestellt wird, dass jedem verwendeten Formular als Anlage die Handlungsanleitung beigefügt wird, und dass im Formular jeweils an den entsprechenden Stellen auf die passenden Erläuterungen in der Handlungsanleitung verwiesen wird. Auf

diese Anforderungen erhielten wir trotz Nachfragen erst im November 2016 eine Antwort, mit der erneut Entwürfe übersandt wurden, die keine Handlungsanleitung mehr enthielten. Daraufhin forderten wir erneut die Umsetzung unserer Anforderungen und wiesen insbesondere darauf hin, dass das Musterformular mit Freitextfeldern unserer Auffassung nach ohne die Handlungsanleitung nicht geeignet ist, um sicherzustellen, dass im praktischen Einsatz die gesetzlichen Wirksamkeitsvoraussetzungen durchgängig eingehalten werden können. Trotz mehrfacher Nachfragen auch auf Leitungsebene, erhielten wir in dieser Sache keine weitere Rückmeldung vom Gesundheitsamt. Sofern es zutrifft, dass das Gesundheitsamt Bremerhaven nunmehr bereits seit Jahren ohne datenschutzkonforme Formulare arbeitet, halten wir dies für inakzeptabel.

7.2 Festplattenverlust bei einer Laborarztpraxis

Von einer Laborarztpraxis wurden wir darüber unterrichtet, dass der Praxis eine Festplatte abhandengekommen war, die die Datensicherung des PC eines ärztlichen Mitarbeiters enthielt. Es wurde vermutet, dass die Festplatte entwendet worden war. Auf der Festplatte war eine unverschlüsselte Excel-Liste mit über 90.000 personenbezogenen Laborwerten enthalten, die von dem Arzt für wissenschaftliche Auswertungen genutzt worden war. Die Liste enthielt im Einzelnen die Daten: Name, Geburtsdatum, Messwert, Anforderungsdatum und Einsender. Die Messwerte enthielten beispielsweise Informationen über Hormonstatus, begleitende Untersuchungen bei Tumoren und Transplantationen, Depressionen, Bluthochdruck, Fruchtbarkeit, Geschlechtshormonstörungen oder Thromboseneigungen. Da nach Auskunft der Laborarztpraxis die Umstände um den Verlust der Festplatte nicht weiter aufgeklärt werden konnten, ist unklar, ob die personenbezogenen Laborwerte tatsächlich von Dritten zur Kenntnis genommen wurden.

Nach § 42 a Bundesdatenschutzgesetz (BDSG) besteht eine Informationspflicht der Aufsichtsbehörde und der Betroffenen, wenn sensible Daten Dritten unrechtmäßig zur Kenntnis gelangen und dadurch schwerwiegende Beeinträchtigungen für die Betroffenen drohen. Ob diese Voraussetzungen erfüllt sind, ist anhand einer Gefahrenprognose zu prüfen. Eine vergleichbare Regelung findet sich in Artikel 33 Datenschutzgrundverordnung. Da die Laborarztpraxis uns als Aufsichtsbehörde bereits informiert hatte, war das Ergebnis der nach § 42 a BDSG durchzuführenden Gefahrenprognose hier lediglich für die Frage relevant, ob die Betroffenen über den Datenverlust informiert werden mussten.

Die Laborarztpraxis kam bei der Bewertung des Risikos für die Betroffenen dazu, dass dies als gering einzuschätzen sei. Es sei unwahrscheinlich, dass die Patientendaten auf der Festplatte überhaupt gefunden würden. Der Dieb sei wohl eher an der Festplatte als an den darauf gespeicherten Daten interessiert gewesen. Die Daten seien ohne Adressen der Betroffenen schwer zuzuordnen. Sie seien zwar schützenswert, aber nicht besonders

sensibel. Im Ergebnis seien die Daten wohl als wertlos zu bezeichnen. Eine Benachrichtigung der Betroffenen würde zu Irritationen führen und könnte an dem Gefahrenpotenzial nichts ändern. Das Labor habe bereits Maßnahmen getroffen, um solche Vorfälle für die Zukunft zu verhindern. So würden zukünftig alle mobilen Datenträger verschlüsselt werden. Zudem solle ein Datenschutzaudit durchgeführt werden.

Diese von der Laborarztpraxis durchgeführte Gefahrenprognose genügt nicht den Anforderungen des § 42 a BDSG. Zur Risikobewertung müssen unter anderem die Art der betroffenen Daten und der potenziellen Auswirkungen der unrechtmäßigen Kenntniserlangung durch Dritte auf die Betroffenen in den Blick genommen werden. Immaterielle Beeinträchtigungen müssen immer dann angenommen werden, wenn sie gleichzeitig als gravierende Persönlichkeitsrechtsverletzungen einen immateriellen Schadensersatzanspruch begründen. Bereits geringe materielle Schäden oder soziale Nachteile ebenso wie Beeinträchtigungen reiner Vermögensinteressen sind als schwerwiegende Beeinträchtigungen zu werten. Der Schaden muss jedoch über die bloße Kenntnisnahme durch einen Dritten hinausgehen. Dafür muss die verantwortliche Stelle eine Gefahrenprognose treffen, bei der sie verschiedene Möglichkeiten der Verwendung der Daten, die Wahrscheinlichkeit der jeweiligen Verwendungsarten sowie die möglichen Auswirkungen auf die Betroffenen zu berücksichtigen hat.

Da die Umstände des Verlustes der Festplatte nicht aufgeklärt werden konnten und der Aufwand zum Auffinden der Daten auf der Festplatte entgegen den Ausführungen des Labors als gering einzustufen war, musste bei der Risikobewertung von einer Kenntnisnahme der Daten durch Dritte ausgegangen werden. An der Bewertung der Laborarztpraxis kritisierten wir insbesondere die folgenden Punkte:

- Es ist unzutreffend, dass medizinisch relevante Laborwerte zu namentlich benannten Patienten und deren behandelnden Ärzten faktisch nicht interpretiert werden können. Selbstverständlich lassen sich aus diesen Werten Informationen über den Gesundheitszustand und insbesondere auch über einzelne Erkrankungen schließen.

- Bei der Bewertung der möglichen Beeinträchtigungen der Betroffenenrechte fehlte die Betrachtung des grundsätzlichen Geheimhaltungsinteresses der Betroffenen in Bezug auf die aus den Werten erkennbaren Krankheiten beziehungsweise gesundheitlichen Störungen. Für Gesundheitsdaten ist grundsätzlich ein besonderes Geheimhaltungsinteresse anzunehmen. Hinzu kommt, dass es sich bei Angaben zu Bluthochdruck, Fruchtbarkeit, Geschlechtshormonstörungen, Thromboseneigungen, Krebs, Transplantationen oder Depressionen auch keineswegs um "unsensible" gesundheitliche Informationen handelt.

- Unzutreffend war im Übrigen die Einschätzung, mehr als 90.000 Laborwerte mit Namen, Vornamen und zum Teil auch Geburtsdaten der Betroffenen und den behandelnden Ärzten hätten keinen Wert.

- Es fehlte eine Betrachtung, zu welchen Zwecken die Daten nutzbar wären und an welche Stellen die Daten zu welchen weiteren Zwecken weitergegeben werden könnten beziehungsweise zu welchem Zweck sie durch Dritte genutzt werden könnten. Es wäre hier erforderlich gewesen, das Missbrauchsrisiko, zum Beispiel durch eigene Nutzung der Daten oder durch Verkauf zu beschreiben und zu bewerten.

Über die von der Praxis getroffenen Maßnahmen hinaus hielten wir weitere Maßnahmen für erforderlich, um entsprechende Datenverluste für die Zukunft auszuschließen. Da nach Auskunft der Praxis ein Personenbezug der Laborwerte für die hausinterne Forschung nicht erforderlich ist, war die Praxis nach § 40 BDSG verpflichtet, die Daten vor der Verwendung für Forschungszwecke zu anonymisieren. Hierzu forderten wir die Praxis ebenso wie zur Überarbeitung der Gefahrenprognose auf.

Auch die überarbeitete Gefahrenprognose genügte nicht den oben dargestellten Anforderungen, war im Ergebnis für uns jedoch ausreichend, um festzustellen, dass keine ausreichend konkreten Hinweise auf schwerwiegende Beeinträchtigungen der Betroffenenrechte im Sinne von § 42 a BDSG vorlagen. Da die gesetzlichen Voraussetzungen des § 42 a BDSG deshalb nicht erfüllt waren, bestand im Ergebnis keine Pflicht zur Information der Betroffenen über den Verlust ihrer Daten.

7.3 Verkauf von Rezeptdaten

Im 36. Jahresbericht hatten wir unter Ziffer 7.5 zur Zulässigkeit der Weitergabe von Rezeptdaten durch Apothekenrechenzentren an Marktforschungsunternehmen berichtet. Das im Jahr 2013 mit uns abgestimmte Konzept zur Weitergabe von Rezeptdaten erfüllt die Anforderungen des Sozialgesetzbuches, nach denen nur eine Weitergabe von anonymisierten Rezeptdaten durch Apothekenrechenzentren an Dritte zulässig ist. Nach diesem mit uns abgestimmten Konzept zur Weitergabe von Rezeptdaten, wurden die Identitätsdaten von Ärztinnen und Ärzten sowie Patientinnen und Patienten sowie die Krankenversichertennummer, die Arztnummer und das Apotheken-Institutionskennzeichen in den Rezeptdaten vor der Weitergabe gelöscht und die Betriebsstättennummer auf die Angabe des Bezirks der Kassenärztlichen Vereinigung reduziert.

Da die vollständig anonymisierten Daten sich jedoch schwerer verkaufen lassen, wurde nach einer Möglichkeit der Erweiterung der zu liefernden Daten gesucht. Im November 2015 erreichte uns deshalb ein neues Konzept zur Lieferung von Rezeptdaten von dem unserer Aufsicht unterliegenden Apothekenrechenzentrum mit der Bitte um datenschutzrechtliche

Bewertung. Das neue Konzept basierte auf der Zuordnung der einzelnen Rezeptdatensätze auf 212 regionale Segmente für den Sitz der Apotheke und der ausstellenden Ärztin oder des ausstellenden Arztes anstelle von 66 Bezirken der Kassenärztlichen Vereinigungen und sollte nun auch die Facharztgruppe enthalten, um den Empfängerinnen und Empfängern Auswertungen auf Facharztebene zu ermöglichen. Dabei sollte sichergestellt werden, dass in einem Segment nicht weniger als drei Datensätze einer Facharztgruppe zugeordnet werden.

In unserer Antwort wiesen wir darauf hin, dass für die Frage der Zulässigkeit der Weitergabe von Rezeptdaten irrelevant ist, in welchem Umfang diese von den Empfängerinnen und Empfängern genutzt werden können. Es kommt allein darauf an, ob die Datensätze anonymisiert sind. Davon konnten wir bei einer Verarbeitung nach dem vorliegenden Konzept nicht ausgehen. Durch die Übermittlung der Facharztgruppe mit dem Datensatz, die im Einzelfall dazu führen kann, dass lediglich eine Anzahl von drei Fachärzten in einem Segment vorhanden sind, konnte eine sichere Anonymisierung jedenfalls nicht sichergestellt werden. Insbesondere durch die Verknüpfung von aus anderen Quellen erlangtem Zusatzwissen war bei dem dargestellten Verfahren die Möglichkeit der Reidentifizierung der betroffenen Ärztinnen und Ärzte, Apothekerinnen und Apotheker oder Versicherten durch die Empfängerin beziehungsweise den Empfänger mit einem nicht unverhältnismäßig hohen Aufwand nicht mit Sicherheit auszuschließen. Das Konzept enthielt keine wirksamen Maßnahmen, um die Reidentifizierung der Betroffenen durch Verknüpfung mit Zusatzwissen auszuschließen.

Im Juni des Berichtsjahres erhielten wir ein weiteres überarbeitetes Konzept, mit dem unsere Bedenken jedoch erneut nicht ausgeräumt werden konnten. Zwar wurden in diesem Konzept Anonymisierungstechniken genannt, jedoch ohne die Grundlage für eine Bewertung der Validität der Maßnahmen geschaffen und dementsprechend auch keine Bewertung zu deren Eignung vorgenommen zu haben. Es fehlten Auswahlkriterien für die genannten Verfahren und begründete klare Festlegungen der Voraussetzungen (Kontext) und der durch die Verfahren zu erreichenden Ziele. Außerdem wurden die genannten Methoden nicht hinsichtlich wesentlicher Risiken wie Herausgreifen, Verknüpfbarkeit und Interferenz geprüft. Für den Fall eines effektiven Einsatzes der genannten Anonymisierungsmethoden fehlte auch die Analyse des Restrisikos. Selbst wenn dies festgestellt würde, bliebe fraglich, ob der Einsatz der analysierten Methoden für die geplanten Datenübermittlungen überhaupt ausreichen könnte.

7.4 Verfahrensbeschreibungen Gesundheitsamt Bremen

Im April des Berichtsjahres wandten wir uns mit dem Hinweis an die Leitung des Gesundheitsamtes Bremen, dass die uns vorliegenden Verfahrensbeschreibungen des

Gesundheitsamtes durchgängig keine ausreichende Beschreibung der technischen und organisatorischen Maßnahmen nach § 7 Bremisches Datenschutzgesetz enthalten. In sämtlichen uns vorgelegten Verfahrensbeschreibungen findet sich zu diesem Punkt nur der Hinweis, dass die technischen und organisatorischen Maßnahmen im Netzwerkdatenschutzkonzept des Gesundheitsamtes Bremen beschrieben sind. Im Netzwerkkonzept des Gesundheitsamtes (Stand: März 2015) wird die technische Sicherheit der Infrastruktur, der IT-Systeme und der Anwendungen sowie die Sicherheit im Netz dargestellt. Die Administration der Fachverfahren wird darin nicht beschrieben. In den Verfahrensbeschreibungen zu den einzelnen Fachverfahren ist es daher insbesondere erforderlich, eventuelle programmtechnische Anpassungen zu dokumentieren, die Berechtigungsstruktur festzulegen, die Berechtigungsadministration zu beschreiben und revisionssicher zu gestalten. Wir wiesen darauf hin, dass wir dies seit langer Zeit beim Gesundheitsamt erfolglos einfordern und baten darum sicherzustellen, dass die Verfahrensbeschreibungen des Gesundheitsamtes um eine ausreichende Beschreibung der technischen und organisatorischen Maßnahmen ergänzt werden.

Vom Gesundheitsamt wurde dazu mitgeteilt, dass im Rahmen der Migration der Fachverfahren zu Dataport eine Prioritätenliste erarbeitet worden sei, die eine Aufstellung enthalte, in welcher Reihenfolge diese gegebenenfalls behandelt werden sollen. Bei den Vorbereitungen für das jeweilige Verfahren würden auch die Verfahrensbeschreibungen aktualisiert, wobei die von uns genannten Punkte berücksichtigt würden. Die aktualisierten Verfahrensbeschreibungen würden uns dann sukzessive zur Verfügung gestellt. Auch auf Nachfragen erhielten wir keine weiteren Rückmeldungen zum Stand der Bearbeitung.

8. Bildung und Soziales

8.1 Aufnahme von Gesundheitsdaten im Abschlusszeugnis

Eine Schule in Bremerhaven erteilte einem Schüler das Abschlusszeugnis. Dies enthielt unter "Bemerkungen" besonders geschützte Gesundheitsdaten und den Hinweis, dass Notenschutz gewährt wurde. Dieser Vermerk dürfte eine starke Reduzierung der Bewerbungschancen des Betroffenen auf dem Arbeitsmarkt zur Folge haben und beeinträchtigt die schutzwürdigen Belange des Betroffenen daher in erheblicher Weise. Im Übrigen enthalten weder das Bremische Schuldatenschutzgesetz oder das Bremische Schulgesetz noch die Zeugnisverordnung eine Erlaubnis, in das Abschlusszeugnis Gesundheitsdaten aufzunehmen.

Auf unsere Anforderung hin erteilte das Schulamt Bremerhaven ein neues Abschlusszeugnis, in dem zwar die Gesundheitsdaten nicht mehr enthalten waren, der Hinweis, dass Notenschutz gewährt wurde, aber verblieb. Daraufhin verlangten wir

ergänzend, auch diesen Hinweis zu entfernen, weil auch dieser die Berufschancen des Betroffenen beeinträchtigen dürfte. Darauf angesprochen verwies uns das Schulamt Bremerhaven auf die Senatorin für Kinder und Bildung. Diese erklärte auf unsere Anfrage, ein derartiger Hinweis dürfe nur auf Antrag der Eltern oder des Prüflings erfolgen. Ein derartiger Antrag lag jedoch nicht vor. Daher bat die Senatorin für Kinder und Bildung das Schulamt Bremerhaven, die Schule zu veranlassen, ein neues Abschlusszeugnis ohne diesen Hinweis zu erteilen, was von dort zugesagt wurde.

8.2 Datenbank Haaranalysen

Im Juli 2012 hatten wir von einer durch das Amt für Soziale Dienste (Jugendamt) betriebenen Datenbanksoftware erfahren (siehe hierzu 38. Jahresbericht, Ziffer 8.1). Mit dieser wurden Daten von Gutachten für Haaranalysen zum Drogenkonsum drogenabhängiger und/oder substituierter Eltern und deren Kinder verwaltet. Wir forderten damals eine Verfahrensbeschreibung und ein Datenschutzkonzept an, die geeignet sein sollten, unsere begründeten Zweifel an der Einhaltung der datenschutzrechtlich erforderlichen technischen und organisatorischen Maßnahmen auszuräumen. Im November des Berichtsjahres erhielten wir ein Datenschutzkonzept.

Im Konzept für die neue Datenbank Haaranalysen werden grundsätzliche datenschutzrechtliche Anforderungen wie Zugriffssicherheit, Zweckbindung, Löschfristen und Löschverfahren, Zugangskontrolle zur Datenbank, Schutz vor Weitergabe und eine aussagefähige Protokollierung erfüllt, die das bisherige Verfahren nicht bieten konnte. Es enthält Vorschläge zur Implementierung wirksamer Maßnahmen, die durch eine neue Datenbankprogrammierung umgesetzt werden sollen. Die dem Konzept anliegende technische Beschreibung zur Sicherstellung des erforderlichen Schutzbedarfs scheint geeignet, im Rahmen einer entsprechenden Umsetzung unter der Voraussetzung einer sicheren Infrastruktur das für diese sensiblen Daten erforderliche Schutzniveau zu gewährleisten. Aus unserer Sicht wäre jedoch eine Verwendung des neuen Kinder- und Jugendhilfe-Fachverfahrens für die Datenverarbeitungen in der Datenbank Haaranalysen die datenschutzrechtlich bessere Lösung. Nach der uns vorliegenden Leistungsbeschreibung für das neue Kinder- und Jugendhilfe-Fachverfahren erwarten wir, dass zukünftig ein Fachverfahren eingesetzt wird, das mit komplexen Funktionen die technische Umsetzung des erforderlichen hohen Schutzniveaus garantieren wird. Auf unsere Anregung hin sagten uns das Amt für Soziale Dienste und die senatorische Behörde zu, die Möglichkeit der Nutzung des neuen Fachverfahrens anstelle der Datenbank Haaranalysen zu prüfen. Da dies jedoch nicht kurzfristig umsetzbar sein wird, soll parallel an der Umsetzung der neuen Datenbanklösung gearbeitet werden.

Aus dem Konzept für die neue Datenbank Haaranalysen ergibt sich, dass neben den Daten zur Haaranalyse in nicht unerheblichem Umfang Daten aus den Fallakten der Case Manager in der Datenbank Haaranalysen gespeichert werden. Die Betroffenen werden dort mit ihren Klarnamen gespeichert. Zudem werden die in der Datenbank gespeicherten Sozialdaten zusätzlich zu Qualitätssicherungs-, Auswertungs- und anderen Zwecken gespeichert und genutzt. Dies ist im Konzept nicht hinreichend beschrieben. Auch gibt es für die Datenverarbeitungen zum Teil keine Rechtsgrundlage. Zudem fehlen ein Löschkonzept und ein Anonymisierungskonzept.

Von Behördenseite wurde uns zusagt, ein Auswertungs- sowie ein Löschkonzept und ein Anonymisierungskonzept zu erstellen und mit uns abzustimmen. Zudem sollen der Datenkatalog und die Datenverarbeitung zu den unterschiedlichen Zwecken insgesamt auf ihre fachliche Notwendigkeit hin überprüft und gegebenenfalls überarbeitet werden. Die als fachlich notwendig identifizierten Prozesse sollen dann in Absprache mit uns in datenschutzrechtlich zulässiger Form umgesetzt werden. Eine pseudonymisierte Speicherung der Datensätze in der Datenbank Haaranalyse sowie eine Reduzierung des in der Datenbank gespeicherten Datenkatalogs sollen dabei ebenfalls geprüft werden.

8.3 Verarbeitung bei der Haaranalyse im Amt für Soziale Dienste

Im Amt für Soziale Dienste wird bei Verdacht auf einen kindeswohlgefährdenden Drogenkonsum auf der Grundlage einer Einwilligung der oder des Betroffenen eine Haaranalyse durchgeführt. Ein Betroffener beschwerte sich bei uns darüber, dass er keine ausreichende Aufklärung über Zweck und Umfang der Durchführung einer solchen Haaranalyse erhalten habe. Er sei lediglich über die Testung von Cannabis informiert worden, tatsächlich seien jedoch eine Vielzahl von weiteren suchtgefährdenden Substanzen getestet worden. Zudem seien ihm rechtliche Konsequenzen für die Verweigerung der Teilnahme an der Haaranalyse angekündigt worden, die jedoch nicht näher konkretisiert worden seien. Schließlich sei beabsichtigt gewesen, die Ergebnisse der Haaranalyse, für die dem Betroffenen im Einwilligungsformular strenge Vertraulichkeit zugesichert worden sei, der von ihm getrennt lebenden Mutter des gemeinsamen Kindes mitzuteilen. Der Betroffene stellte einen Antrag auf Sperrung der Ergebnisse seiner Haaranalyse beim Amt für Soziale Dienste, widerrief kurz darauf seine Einwilligung und beantragte die Übersendung der Ergebnisse und die Löschung der Daten im Amt für Soziale Dienste.

Wir forderten das Amt für Soziale Dienste zur Übersendung der Ergebnisse an den Betroffenen und zur Löschung der Ergebnisse der Haaranalyse im eigenen Hause auf. Diesen Aufforderungen kam das Amt für Soziale Dienste nach. Unsere Überprüfung des Einwilligungsformulars ergab datenschutzrechtliche Mängel in Bezug auf die Aufklärung über Zweck und Umfang der Datenverarbeitung im Zusammenhang mit der Haaranalyse und die

Folgen der Verweigerung. Das Amt für Soziale Dienste nahm dies zum Anlass, bei der Senatorin für Soziales, Frauen, Jugend, Integration und Sport eine grundlegende Überarbeitung des Formulars zu erwirken, die bis zum Ende des Berichtsjahres noch nicht abgeschlossen war.

8.4 Projekt Nachfolgesoftware OK.JUG

Im September 2012 hatten wir erstmalig vom Amt für Soziale Dienste erfahren, dass das Fachverfahren OK.JUG des Jugendamtes keine Möglichkeit bietet, Zugriffsrechte auf einzelne Fälle zu beschränken. Deshalb konnten die Anforderungen des Sozialdatenschutzes, auch innerhalb eines Leistungsträgers sicherzustellen, dass Sozialdaten nur denen für die Verarbeitung der sensiblen Daten Befugten zugänglich sein dürfen, nicht erfüllt werden. Wir wiesen das Jugendamt mehrfach auf diesen Verstoß hin und forderten die Beseitigung der Mängel (siehe hierzu 38. Jahresbericht, Ziffer 8.3). Die Senatorin für Soziales, Jugend, Frauen, Integration und Sport hat inzwischen eine Leistungsbeschreibung für das Nachfolgeprodukt erstellt und das Vergabeverfahren gestartet. Die Leistungsbeschreibung lag uns zeitnah vor und definierte grundsätzlich einen angemessenen Standard zur Umsetzung datenschutzrechtlicher Anforderungen. Dennoch teilten wir der senatorischen Dienststelle einige Fragen, Wünsche zur Gewichtung einzelner Funktionen und besondere Anforderungen mit. Dazu gehörten beispielsweise die Klärung der Zulässigkeit für geplante Zugriffe aus externen Registern (Ausländerzentralregister, Bundeszentralregister), der Zulässigkeit der Einrichtung eigener Register wie eines zentralen Sorgerechtsregisters und Urkundenregisters, eine höhere Gewichtung für das Vorhandensein einer zentralen Benutzer- und Rechteverwaltung und die Prüfung einer datenschutzgerechten Durchführung des Supports, insbesondere die Möglichkeit einer revisionssicheren Protokollierung von Fernwartungszugriffen durch die Wartungsfirma. Darüber hinaus wiesen wir auf die Notwendigkeit der Bereitstellung geeigneter Verfahren zur Gewährleistung einer echten Anonymisierung sensibler Daten, beispielsweise zur Durchführung des Controllings, hin. Außerdem muss zur Auswertung von Hilfeketten technisch sichergestellt werden, dass die dafür erforderlichen Einwilligungserklärungen und gegebenenfalls Schweigepflichtentbindungen im System abgebildet werden. Die Senatorin für Soziales, Jugend, Frauen, Integration und Sport hat uns die Berücksichtigung unserer Hinweise für das weitere Verfahren zugesagt.

8.5 Vergabe von Mitteln des Europäischen Sozialfonds (ESF)

Im November 2015 hatten wir uns an die Verwaltungsbehörde für den Europäischen Sozialfonds beim Senator für Wirtschaft, Arbeit und Häfen gewandt, weil wir verschiedene Anfragen und Beschwerden zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus Mitteln des Europäischen Sozialfonds (ESF) finanzierte Maßnahmenträger für

Maßnahmen nach dem Sozialgesetzbuch II und Beratungsstellen für Empfängerinnen und Empfänger von Arbeitslosengeld II erhalten hatten. Dadurch entstanden bei uns Zweifel an der Zulässigkeit des derzeit praktizierten Verfahrens der Verarbeitung von personenbezogenen Daten der Teilnehmerinnen und Teilnehmer beziehungsweise Klientinnen und Klienten im Zusammenhang mit den Berichtspflichten für den Europäischen Sozialfonds. Beispielsweise war uns berichtet worden, dass die ESF-Verwaltungsbehörde zum Zweck der Prüfung die Einsichtnahme in personenbezogene Teilnehmerakten und Bestätigungen der Arbeitslosen über die erhaltenen Beratungsleistungen verlangte. Zudem wurde von den Trägern verlangt, alle Teilnehmerunterlagen zwanzig Jahre aufzubewahren und für die Prüfbehörde zur Einsicht bereitzuhalten. Diese Anforderungen hatten zu Folge, dass die Beratungsstellen keine anonymen Beratungen mehr anbieten konnten. Zudem deckten sich diese Anforderungen nicht mit den Informationen für die Betroffenen in einem von der ESF-Behörde zur Ausgabe durch die Träger erstellten Hinweisblatt mit Informationen zum Datenschutz.

Von Seiten der ESF-Behörde wurde uns erläutert, dass diese Anforderungen zwischenzeitlich Voraussetzung für die Mittelvergabe durch den ESF geworden seien, sodass die Prüfbehörde keine Möglichkeit mehr habe, datenschutzfreundlichere Lösungen umzusetzen. Die Prüfungen in personenbezogener Form lägen nicht im Eigeninteresse der Prüfbehörde; es werde lediglich das umgesetzt, was von der Kommission gefordert werde. Um jedoch sicherzustellen, dass trotzdem alle Hilfeempfänger das Angebot in Anspruch nehmen könnten, sei mit den Beratungsstellen vereinbart worden, dass eine anonyme Beratung von bis zu zehn Prozent von der Prüfbehörde akzeptiert werde.

Wir forderten, sowohl für die Maßnahmenträger und Beratungsstellen als auch für die Betroffenen eine vollständige Transparenz hinsichtlich der Datenverarbeitung herzustellen und das Informationsblatt für die Teilnehmerinnen und Teilnehmer entsprechend zu überarbeiten. Obwohl eine Überarbeitung des Informationsblatts bereits im Januar 2016 von der ESF-Prüfbehörde zugesagt worden war, wurde uns von der ESF-Behörde trotz mehrfacher Aufforderung bisher kein neuer Entwurf vorgelegt. Dass dadurch in der Praxis die Unsicherheiten bei Trägern und Betroffenen fortbestehen, zeigen entsprechende Anfragen, die uns weiterhin erreichen.

8.6 Bevollmächtigung und Einwilligungserklärung im Schwerbehindertenverfahren

Im Berichtsjahr meldete sich das Amt für Versorgung und Integration Bremen und nahm Bezug auf einen Vorgang aus dem Jahr 2009, in dem die damalige Senatorin für Arbeit, Frauen, Jugend, Gesundheit und Soziales unsere Rechtsauffassung zur datenschutzrechtlichen Zulässigkeit der Bevollmächtigung eines Dritten zur Abgabe der

erforderlichen Einwilligungs- und Schweigepflichtentbindungserklärungen im Schwerbehindertenverfahren erbeten hatte. Im Jahr 2009 hatten wir im Einklang mit der damals herrschenden Meinung in der Literatur die Position vertreten, dass die datenschutzrechtliche Einwilligungserklärung als höchstpersönliches Recht nicht durch Dritte erteilt werden kann, eine Bevollmächtigung dafür also nicht möglich ist. Auf Initiative der Landesarbeitsgemeinschaft in Betreuungsangelegenheiten wurde das Thema im Berichtsjahr erneut aufgegriffen, da diesbezüglich eine Inkompatibilität mit den gesetzlichen Wertungen im Betreuungsrecht gesehen wird.

Nach einer erneuten vertieften Befassung mit dem Thema stellten wir fest, dass diese Thematik mittlerweile in der Literatur differenzierter betrachtet wird. Zwar wird zum Teil weiterhin an der strengen Auffassung festgehalten, wonach eine Vertretung für die Abgabe einer Einwilligungs- und Schweigepflichtentbindungserklärung aufgrund der Höchstpersönlichkeit nicht zulässig ist. Diese Auffassung erscheint jedoch inkonsequent, da eine entsprechende Vertretung durch sorgeberechtigte Eltern und gesetzliche Betreuer nicht infrage gestellt wird. Die vereinzelt vertretene Gegenauffassung bewertet die Einwilligungserklärung ohne weitere Anforderungen als vertretbar. Die vermittelnde Auffassung unterteilt auch die höchstpersönlichen Verfahrenshandlungen in solche, die der Natur der Sache nach vertretbar sind, und solche, die nur persönlich ausgeführt werden können, wie beispielsweise, sich ärztlichen oder psychologischen Untersuchungsmaßnahmen zu unterziehen. Nach dieser Auffassung kann auch das Recht zur Abgabe einer datenschutzrechtlichen Einwilligungserklärung auf Dritte übertragen werden, wenn diese explizit und hinreichend bestimmt von den Betroffenen dazu legitimiert wurden.

Angesichts dieser veränderten Lage scheint es uns nicht mehr sachgerecht, Bevollmächtigungen kategorisch auszuschließen. Vor dem Hintergrund der Einführung des Instituts der Vorsorgevollmacht erscheint uns die vermittelnde Auffassung zeitgemäß. Die Erteilung einer Vorsorgevollmacht hat nach dem Gesetz Vorrang vor der gesetzlichen Betreuung. Folgte man der Gegenauffassung, die eine Bevollmächtigung für die Erteilung einer datenschutzrechtlichen Einwilligung ausschließt, würde dies zu einem Wertungswiderspruch im Hinblick auf die gesetzlich normierte Vorrangstellung der Vorsorgevollmacht führen. Die Vorsorgevollmacht begründet den Ausnahmefall eines gesetzlich zugelassenen Vertreterhandelns in Aufgabenkreisen, die grundsätzlich höchstpersönlicher Natur sind wie die gesundheitliche Fürsorge, die körperliche Unversehrtheit, die Selbstbestimmung, die Aufenthaltseinschränkung und die Aufenthaltsbestimmung. Sie muss also eine umfassende Vertretung beinhalten können, um dem vom Gesetzgeber angestrebten Ziel gerecht werden zu können, rechtliche Betreuung – soweit möglich – zu verhindern. Diesem Gedanken würde es widersprechen, müsste bei einem bestimmten Personenkreis auch bei Vorliegen einer umfassenden Vorsorgevollmacht

allein für die Abgabe von datenschutzrechtlichen Einwilligungs- und Schweigepflichtentbindungserklärungen ein Betreuer bestellt werden. Der Grundsatz der Subsidiarität der Betreuung würde damit unterlaufen. Eine Versagung der Möglichkeit, im Rahmen einer Vorsorgevollmacht oder auch generell eine Vollmacht für die Abgabe von datenschutzrechtlichen Einwilligungen zu erteilen, würde die Selbstbestimmung der Betroffenen einschränken, stellt doch auch die Entscheidung für die Bevollmächtigung eines Dritten zur Abgabe von datenschutzrechtlichen Einwilligungserklärungen eine Form der Ausübung des Rechts auf informationelle Selbstbestimmung dar.

Dem Amt für Versorgung und Integration und dem Senator für Wirtschaft, Arbeit und Häfen haben wir mitgeteilt, dass bei der Annahme einer Vertretungsbefugnis in der Praxis sichergestellt werden muss, dass die jeweilige Vorsorgevollmacht beziehungsweise Generalvollmacht die Bevollmächtigung zur Abgabe von Einwilligungs- und Schweigepflichtentbindungserklärungen auch tatsächlich umfasst. Finden sich in der schriftlich erteilten Vollmacht dazu keine weiteren Anhaltspunkte, weil diese lediglich für alle Angelegenheiten oder für andere konkret aufgelistete Sachverhalte erteilt wurde, kann zunächst nicht davon ausgegangen werden, dass auch datenschutzrechtliche Erklärungen umfasst sein sollen. In diesem Fall trifft das Amt für Versorgung und Integration eine Pflicht zur Ermittlung, die in der Akte dokumentiert werden sollte. Das Amt für Versorgung und Integration hat signalisiert, diese Anforderungen zukünftig umzusetzen.

8.7 Anforderung von Personalausweiskopien

Durch Anfragen von Bürgerinnen und Bürgern hatten wir erfahren, dass vom Amt für Soziale Dienste bei der Beantragung von Sozialleistungen (zum Beispiel Grundsicherung, Elterngeld) die Antragstellerin beziehungsweise Antragsteller regelmäßig zur Übersendung von Kopien ihrer Personalausweise aufgefordert werden. Wir teilten dem Amt für Soziale Dienste mit, dass dieses Verfahren nicht zulässig ist, da die Anforderung einer Personalausweiskopie zur Feststellung der Identität einer Person weder geeignet noch erforderlich ist. Bei der Vorlage einer Kopie kann zum einen ein gewisses Fälschungsrisiko nicht ausgeschlossen werden. Zum anderen ist eine Identitätsprüfung, soweit diese für erforderlich gehalten wird, durch Vorlage und Sichtabgleich des Ausweises mit der vorlegenden Person möglich. Zur Kontrolle der Personalien können Mitarbeiterinnen und Mitarbeiter des Sozialleistungsträgers die Vorlage eines gültigen Passes oder Personalausweises verlangen. Die Mitarbeiterin beziehungsweise der Mitarbeiter kann über diese Identitätsprüfung einen Vermerk für die Akte anfertigen. Sollten beim Leistungsträger im Zuge der Bearbeitung Zweifel an der Identität der Antragstellerin beziehungsweise des Antragstellers aufkommen, so wäre eine erneute Prüfung durch Vorlage des Ausweises möglich. Dieses datensparsame Verfahren ist zum Zweck der Identitätsprüfung ausreichend und verhindert, dass weitere im Ausweis enthaltene nicht erforderliche Daten gespeichert

werden. Darüber hinaus wäre es gerade in Zweifelsfällen auch die geeignetere Vorgehensweise zur Identitätsfeststellung. Ein Rückgriff auf die Kopie würde nicht zu neuen Erkenntnissen führen. Wir wiesen in dem Zusammenhang auf ein Schreiben des Bundesministeriums des Inneren vom 29. März 2011 hin, wonach die Anfertigung von Personalausweiskopien nur unter sehr engen Voraussetzungen zulässig ist:

- Die Erstellung einer Kopie muss erforderlich sein. Dabei ist insbesondere zu prüfen, ob nicht die Vorlage des Personalausweises oder des Reisepasses und gegebenenfalls die Anfertigung eines entsprechenden Vermerks ausreichend sind.

- Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden.

- Die Kopie muss als solche erkennbar sein.

- Daten, die nicht zu Identifizierungszwecken benötigt werden, können und sollen von den Betroffenen auf der Kopie geschwärzt werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangsnummer und Seriennummer. Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen.

- Die Kopie ist von der Empfängerin beziehungsweise vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist.

- Eine automatisierte Speicherung der Passdaten/Ausweisdaten ist nach dem Passgesetz und dem Personalausweisgesetz unzulässig.

Wir baten das Amt für Soziale Dienste, die regelmäßige Anforderung von Kopien bei der Beantragung von Sozialleistungen unverzüglich einzustellen und die bereits angeforderten Kopien zu vernichten beziehungsweise zu löschen. Das Amt für Soziale Dienste teilte uns mit, dass unsere Rechtsauffassung dort geteilt werde und die Fachabteilung der Senatorin für Soziales, Jugend, Frauen, Integration und Sport als Aufsichtsbehörde gebeten worden sei, diese in den bestehenden Verfahrensvorgaben umzusetzen. Die senatorische Behörde entschied daraufhin, eine umfassende Regelung zu schaffen, die auch die Zulässigkeit der Anforderung von Kopien von Aufenthaltstiteln umfasst, für die die oben genannten Anforderungen im Wesentlichen entsprechend gelten. In dem uns von der senatorischen Behörde übersandten Entwurf für eine fachliche Mitteilung "Umgang mit Pässen und Personalausweisen im Rahmen der Identitätsprüfung sowie der Umgang mit Aufenthaltstiteln" sahen wir unsere Anforderungen hinreichend berücksichtigt.

8.8 Jugendberufsagentur

Unsere Beratungstätigkeiten in Bezug auf den Aufbau einer Jugendberufsagentur (JBA) in Bremen und Bremerhaven gingen 2017 in das vierte Jahr. Nachdem wir im Juli 2014 aus der

Presse von entsprechenden Planungen erfahren hatten, wandten wir uns an die damalige Senatorin für Bildung und Wissenschaft. Da bei diesem Projekt datenschutzrechtliche Fragen eine zentrale Rolle spielen, baten wir um frühzeitige Beteiligung bei Strukturentscheidungen mit Datenschutzrelevanz. Im Februar 2015 fand diesbezüglich eine erste Besprechung mit Vertretern der Partner der Jugendberufsagentur statt. Bei diesen handelt es sich um die Senatorin für Bildung und Wissenschaft, das Amt für Soziale Dienste, den Magistrat Bremerhaven, den Senator für Wirtschaft, Arbeit und Häfen, die Agentur für Arbeit Bremen und das Jobcenter Bremen. In der Besprechung wurde mitgeteilt, dass die JBA Anfang Mai 2015 ihre Arbeit aufnehmen sollte.

Bei der Jugendberufsagentur handelt es sich um eine Kooperation der oben genannten Partner mit gegebenenfalls weiteren Stellen im Rahmen ihrer bisherigen Aufgaben und Zuständigkeiten mit dem Ziel, durch Abstimmung der Maßnahmen bessere Vermittlungs- und Beratungserfolge bei den 15 bis 25-jährigen zu erzielen. Die Jugendberufsagentur ist keine Stelle mit eigener Rechtsfähigkeit, sodass sie auch keine verantwortliche Stelle im Sinne des Datenschutzrechts sein kann, sondern die Datenverarbeitung der einzelnen Partner nur im Rahmen der für sie jeweils geltenden datenschutzrechtlichen Grundlagen erlaubt ist. An der Entwurfsfassung der Verwaltungsvereinbarung über die Zusammenarbeit im Rahmen einer Jugendberufsagentur in der Freien Hansestadt Bremen kritisierten wir, dass dazu aufgefordert wurde, das Denken in Zuständigkeiten und Abgrenzungen durch die Wahrnehmung einer gemeinsamen Verantwortung zu überwinden. Bei den einzelnen Aufgabenfestlegungen wurden in der Verwaltungsvereinbarung zum Teil keine klaren Verantwortlichkeiten für die einzelnen Partner festgelegt, sondern die Jugendberufsagentur in nicht korrekter Weise wie eine selbständige Behörde behandelt. Zudem sollten Informationen über die jungen Menschen regelmäßig an alle Partner weitergegeben werden, auch ohne dass die Weitergabe zur Aufgabenerfüllung erforderlich sein musste. Die kritisierten Passagen der Verwaltungsvereinbarung wurden geändert.

Mitte April 2015 erhielten wir einen ersten Entwurf der von den jungen Menschen zu unterzeichnende Einwilligungserklärung. Der Vorstellung einiger Partner der Jugendberufsagentur, wonach unabhängig von der Ausgestaltung der Zusammenarbeit in der Jugendberufsagentur regelmäßig alle durch die Partner der Jugendberufsagentur erhobenen Daten allen Partnern zur Verfügung gestellt werden sollten, traten wir entgegen, weil eine Datenvorratshaltung ohne Erforderlichkeitsprüfung im Einzelfall nicht mit dem Recht auf informationelle Selbstbestimmung zu vereinbaren ist. In einer wirksamen datenschutzrechtlichen Einwilligungserklärung müssen die zugrunde liegenden Datenflüsse vollständig und korrekt in einer für die Betroffenen verständlichen Form beschrieben werden. Zudem dürfen keine Datenverarbeitungen zum Gegenstand einer Einwilligungserklärung gemacht werden, die bereits gesetzlich erlaubt sind. Die Tatsache, dass die Zusammenarbeit der Partner in der Jugendberufsagentur und die damit im Zusammenhang

stehenden Datenverarbeitungen nicht abschließend festgelegt und dokumentiert worden waren, macht eine ständige und weiter fortdauernde Überarbeitung der Einwilligungserklärung erforderlich.

Im Dezember 2016 wurde durch eine Änderung des Bremischen Schuldatenschutzgesetzes die Möglichkeit zur Speicherung von Daten von, auch ehemaligen, Schülerinnen und Schülern im Alter von 15 bis 25 Jahren bei der Senatorin für Kinder und Bildung und dem Magistrat Bremerhaven geschaffen. Ebenso wurde die Befugnis zur Datenübermittlung an die Partner der Jugendberufsagentur bei Erforderlichkeit für Vermittlung, Beratung oder Förderung eingefügt und die Grundlage für eine aufsuchende Beratung bei fehlenden Informationen geschaffen.

Mitte August 2017 unterrichtete uns die Senatorin für Kinder und Bildung über die Planungen zum Aufbau eines "Kerndatensystems Jugendliche" bei der Bundesagentur für Arbeit. Dabei handelt es sich um eine gemeinsame Datenbank für alle Partner aller Jugendberufsagenturen im Bundesgebiet, in der die Daten aller jungen Menschen in Deutschland zwischen 15 und 25 Jahren fortlaufend gesammelt werden sollen. Die Datenbank soll den trägerübergreifenden und medienbruchfreien vollständigen Informationsaustausch zwischen Schule, Sozialleistungsträgern und weiteren Partnern ermöglichen und vielfältige Auswertungsmöglichkeiten schaffen. Sie soll ab Ende 2018 zum Einsatz kommen, zunächst im Rahmen eines Pilotprojekts unter Beteiligung der Länder Bremen, Hamburg, Saarland und Rheinland-Pfalz. Die beteiligten Länder sollen dafür einen Auftrag an die Bundesagentur für Arbeit zur Pilotierung und Bereitstellung der Datenbank erteilen. Von Seiten der Bundesagentur für Arbeit soll in diesem Zusammenhang auf die Schaffung von Rechtsänderungen hingewirkt werden, die den Einsatz der Datenbank zukünftig regelt.

Wir rieten der Senatorin für Kinder und Bildung von der Teilnahme am Pilotprojekt "Kerndatensystem Jugendliche" dringend ab, da gegen die Umsetzung dieses Projekts erhebliche datenschutzrechtliche Bedenken bestehen. Die dort vorgesehenen Datenverarbeitungen sind bislang weder durch Gesetz noch durch die für die Jugendberufsagenturen Bremen und Bremerhaven verwendeten Einwilligungserklärungen gedeckt. Wir sehen in dem Vorhaben, alle jungen Menschen im Alter von 15 bis 25 Jahren mit einer Historie ihrer Daten lückenlos in einem einzigen IT-System zentral zu speichern, ohne dass dies zur Förderung, Beratung oder Vermittlung der jungen Menschen erforderlich ist, eine unzulässige Vorratsdatenspeicherung. Zudem sehen wir keine Möglichkeit, im Wege der Auftragsverarbeitung durch das Land Bremen einen Auftrag an die Bundesagentur für Arbeit zum Betrieb einer Datenbank für eine gemeinsame Datenhaltung aller Partner auf Ebene des Bundes und der Länder zu erteilen. Auch steht ein solches Vorhaben im Widerspruch zur bremischen Verwaltungsvereinbarung, in der festgelegt ist, dass jeder

Partner in seinen eigenen Systemen arbeitet und keine gemeinsame Datenhaltung erfolgen soll.

8.9 Bewohner- und Quartiersmanagementsoftware für Flüchtlingsunterkünfte

Im Frühjahr 2016 wurde von der Senatorin für Soziales, Jugend, Frauen, Integration und Sport eine Software zum Bewohner- und Quartiersmanagement, also zur zentralen Erfassung von Flüchtlingen und zur Verwaltung von Flüchtlingsunterkünften, eingeführt. Diese Software dient der Verwaltung von Unterkünften für Flüchtlinge im Hinblick auf die zentrale Erstaufnahme, Belegungsplanung und Kapazitätskontrolle. Mit dem Programm sollen sowohl die zentralen Erstaufnahmeeinrichtungen als auch die dezentralen Aufnahmeeinrichtungen wie Notunterkünfte und Übergangswohnheime unterstützt werden. Jede Bewohnerin und jeder Bewohner erhält nach Aushändigung eines Aufklärungsbogens und Einwilligungsbogens in der jeweiligen Muttersprache eine Ausweiskarte, auf der ausschließlich die Kartennummer gespeichert ist. Durch Auflegen der Karte werden unter anderem die Zutrittskontrolle, die Essensausgabe und die Warenausgabe verwaltet. Für die bei der Anstalt öffentlichen Rechts Dataport gespeicherten Daten gibt es ein umfangreiches Berechtigungskonzept.

Von unserer Seite bestanden erhebliche datenschutzrechtliche Bedenken, die im Laufe der Zeit zum Teil schon durch Änderungen des Programms beseitigt wurden. Andere datenschutzrechtliche Aspekte befinden sich noch im Abklärungsprozess. Unter anderem kritisierten wir die Speicherfrist von fünf Tagen für Aktionen, wie das Betreten und das Verlassen des Quartiers, die die Erstellung eines Bewegungsprofils der Bewohnerinnen und Bewohner ermöglichen. Es gab keine Rechtsgrundlage für das Speichern der Aktionen für einen derartig langen Zeitraum. Als Grund für diese Speicherung wurde das Notfallmanagement angeführt. Es sollte im Katastrophenfall schnell festgestellt werden können, wer sich aktuell in der Unterkunft befindet. Wir kritisierten, dass für diesen Zweck die Speicherung der letzten Aktion ausreichen würde. Anfang 2017 konnten wir zunächst eine Reduzierung der Speicherfrist auf drei Tage und im Herbst 2017 die alleinige Speicherung der letzten Aktion erreichen.

Weiterhin bemängeln wir, dass die Tatsache der Essenausgabe bei den einzelnen Personen gespeichert wird. Wir sehen weder eine Rechtsgrundlage noch eine Erforderlichkeit für eine solche Datenspeicherung. Als Grund für die derzeitige Praxis wurde erläutert, dass diese Daten zur Abrechnung und Bestellung des Essens erforderlich seien. Diese Argumentation finden wir nicht einleuchtend, da für die Erreichung dieser Zwecke eine Speicherung ohne Personenbezug ausreicht. Das Ressort prüft, ob eine solche Speicherung auch anonym erfolgen kann.

Das Programm sah vor, auch für die Mitarbeiterinnen und Mitarbeiter, Ehrenamtliche und Sicherheitsangestellten die Anwesenheit im Quartier festzuhalten. Aus datenschutzrechtlicher Sicht sind Daten von Mitarbeiterinnen und Mitarbeitern nicht in einem Fachverfahren abzuspeichern. Die Senatorin für Soziales, Jugend, Frauen, Integration und Sport stellte den verschieden Institutionen bisher frei, dieses Modul zu nutzen. Eine aktuelle Überprüfung ergab, dass das Mitarbeitermodul von keiner Institution genutzt wird. Es wird daher derzeit abgeklärt, ob dieses Modul künftig nicht mehr angeboten wird, um die datenschutzrechtlichen Bedenken auch für die Zukunft auszuschließen.

Die Speicherung von Gesundheitsdaten innerhalb des Programms wurde im Laufe der Zeit in Bremen deutlich eingeschränkt. Aktuell wird nur noch ein Ankreuzfeld zur Gehbehinderung und zur bestehenden Schwangerschaft angeboten. Diese beiden Merkmale sind für die Auswahl der Unterbringung von erheblicher Bedeutung. Datenschutzrechtliche Bedenken bestehen jedoch bei einer Freitextangabemöglichkeit "andere Behinderungen". Dort besteht die Möglichkeit wichtige Diagnosen zu hinterlegen. Aufgrund der Nicht-Beherrschbarkeit dieses Feldes und der Möglichkeit, Gesundheitsdaten zu hinterlegen, die nicht für die Unterbringung relevant sind, wird derzeit vom Ressort überprüft, ob dieses Feld, für den Zugriff der jeweiligen Leitung der Unterkunft beschränkt werden kann. Möglicherweise sind die Angaben einer besonderen Behinderung für die Verteilung oder Versorgung der Bewohnerinnen und Bewohner wichtig, aber nicht jede Mitarbeiterin oder jeder Mitarbeiter muss auf dieses Datum Zugriff haben. Auch für die Angabe der Religion wird auf unseren Anstoß hin überprüft, ob nicht eine Zugriffsbeschränkung der Leitung ausreichend sein könne. Eine Antwort auf diese Alternative steht derzeit noch aus.

Von uns wurde des Weiteren kritisiert, dass die Verwandtschaftsverhältnisse der Personen innerhalb des Programms gespeichert werden, da nicht jeder offen legen möchte, mit wem er verwandt ist. Diese Datenerhebung sei jedoch wichtig, um bei einem Umzug einer Familie eine ausreichend große Wohnung für alle Familienmitglieder zu finden. Die Speicherung beziehe sich nur auf die Kernfamilie und ausschließlich auf die Daten, die die Bewohnerin beziehungsweise der Bewohner selbst angegeben habe, sodass unsere datenschutzrechtlichen Bedenken in Bezug auf diesen Punkt ausgeräumt wurden.

Offene Punkte sind unter anderem noch die Löschroutinen der vorhandenen Datensätze. Unserer Ansicht nach sind die Daten zu löschen, sobald sie nicht mehr erforderlich sind. Zum Thema Löschung der Daten ist das Ressort aber aufgrund von mangelnden Ressourcen noch nicht tätig geworden, aber das Problem ist bereits erkannt und werde in naher Zukunft gelöst werden.

Aus unserer Sicht ist es datenschutzrechtlich lobenswert, dass innerhalb des Programms ein Nachrichtenmodul zur Verfügung gestellt wird, sodass die verschiedenen Träger und

Einrichtung in Eilfällen bei Aufnahme oder Übernahme neuer Bewohnerinnen und Bewohner nicht in Gefahr laufen, ungesicherte E-Mails zu verschicken, sondern in einem gesicherten Umfeld innerhalb des Programms mit einem geschlossen Empfängerkreis Informationen austauschen können.

8.10 Umgang mit Protokollen und Tonaufzeichnungen in WiN-Foren

Im Berichtsjahr wandte sich ein Bürger mit der Beschwerde an uns, dass sein Name in den Protokollen eines WiN-Forums niedergeschrieben worden sei und bat uns um Durchsetzung seines Löschungsbegehrens. WiN steht für "Wohnen in Nachbarschaften" und damit ist ein seit dem Jahr 1998 laufendes, das Bund-Länder-Programm "Soziale Stadt" ergänzendes kommunales Finanzierungsprogramm. In elf Gebieten in Bremen ist als Anlaufstelle vor Ort jeweils ein Quartiersmanagement eingesetzt. Die jährlich pro Gebiet zur Verfügung stehenden Fördermittel werden auf den öffentlichen Sitzungen der lokalen Foren einvernehmlich vergeben. Mit dem Amt für Soziale Dienste Bremen als unserem Ansprechpartner entwickelten wir eine Handreichung zum Qualitätsmanagement betreffend den Datenschutz, die der Klarstellung datenschutzrechtlicher Fragen im Zusammenhang mit der Umsetzung sozialraumbezogener Programme in den sogenannten WiN-Gebieten dient. Als Ergebnis lässt sich festhalten, dass Namen von Bürgerinnen und Bürgern nur in den Protokollen aufgenommen werden dürfen, wenn eine Einwilligung vorliegt. Eine Einwilligung jeder am WiN-Forum teilnehmenden Person ist auch zur Tonaufzeichnung der jeweiligen Sitzung erforderlich. Wir empfahlen, vor der Tonaufnahme schriftliche Einwilligungen, zum Beispiel durch eine Einwilligungserklärung in Verbindung mit einer Anwesenheitsliste, einzuholen und nach Erstellung des Protokolls die Tonaufzeichnung sofort zu löschen.

9. Beschäftigtendatenschutz

9.1 Beschäftigtendatenschutz nach DSGVO und BDSG-neu

Wenn ab Ende Mai 2018 die Datenschutzgrundverordnung (DSGVO) anwendbar ist, gilt dies auch für den Beschäftigtendatenschutz. Dazu gehört insbesondere die Einhaltung der in Artikel 5 DSGVO enthaltenen Datenschutzgrundsätze Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Für die Einhaltung dieser Grundsätze ist nach Artikel 5 Absatz 2 DSGVO die Arbeitgeberin beziehungsweise der Arbeitgeber verantwortlich und muss dessen Einhaltung nachweisen können (Rechenschaftspflicht). Die Grundsätze ziehen sich wie ein roter Faden durch die gesamte DSGVO. Auch die in den Artikeln 14 und 15 DSGVO geregelten erweiterten Informationspflichten der Arbeitgeberinnen und Arbeitgeber gegenüber ihren Bewerberinnen oder Bewerbern und Beschäftigten bedeuten Verbesserungen für den Beschäftigtendatenschutz. So muss die Arbeitgeberin oder der Arbeitgeber die Beschäftigten

beispielsweise über Datenübermittlungen an Drittstaaten, also Länder außerhalb der Europäischen Union, über die Speicherfristen der vom ihm verarbeiteten Daten und über ihre Rechte unterrichten.

Nach Artikel 88 Absatz 1 DSGVO können die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen (Betriebsvereinbarungen, Dienstvereinbarungen und Tarifverträge) "spezifische Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten" bei Datenverarbeitungen im Beschäftigungskontext vorsehen. Dies gilt nach Erwägungsgrund 155 der DSGVO auch für die Bedingungen, unter denen eine Einwilligung im Beschäftigungskontext wirksam sein könnte. Nach Artikel 88 Absatz 2 DSGVO müssen solche Regelungen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe und die Überwachungssysteme am Arbeitsplatz umfassen.

Der Bundesgesetzgeber hat inzwischen mit § 26 Absatz 1 Bundesdatenschutzgesetz-neu (BDSG-neu) eine derartige Rechtsvorschrift geschaffen. Damit wurde einerseits der bisher geltende § 32 Absatz 1 Bundesdatenschutzgesetz (BDSG) übernommen. Andererseits erhält diese Vorschrift auch die Erlaubnis, dass erforderliche Beschäftigtendaten zur Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag oder einer Betriebsvereinbarung oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten verarbeitet werden dürfen. Zudem regelt § 26 Absatz 2 BDSG-neu die Bedingungen, unter denen eine Einwilligung im Beschäftigungskontext wirksam sein kann (rechtlicher oder wirtschaftlicher Vorteil oder Arbeitgeberinnen beziehungsweis Arbeitgeber und Beschäftigte verfolgen gleichgelagerte Interessen). Unabhängig davon muss die Arbeitgeberin oder der Arbeitgeber nach Artikel 7 Absatz 1 DSGVO nachweisen können, dass die betroffene Person in eine Datenverarbeitung eingewilligt hat. Des Weiteren wiederholt § 26 Absatz 3 BDSG-neu die Ausnahmen in Artikel 9 Absatz 2 Buchstabe b DSGVO zur Verarbeitung besonderer Kategorien von Daten.

Darüber hinaus muss die Arbeitgeberin oder der Arbeitgeber nach § 26 Absatz 5 BDSG-neu geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Artikel 5 DSGVO dargelegten Grundsätze für die Verarbeitung personenbezogener Beschäftigtendaten eingehalten werden. Lediglich für die Verarbeitung besonderer Kategorien von Daten verweist § 26 Absatz 2 letzter Satz BDSG-neu auf § 22 Absatz 2 BDSG-neu. Danach sind die dort konkret aufgeführten angemessenen und spezifischen Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Grundsätzlich sollten die dort genannten Maßnahmen jedoch generell bei der Verarbeitung von Beschäftigtendaten zu treffen sein. In diesem Zusammenhang sei auf das Kurzpapier

"Beschäftigtendatenschutz"[1] der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder verwiesen.

9.2 Zugriff auf Personalaktendaten

Bei der Feuerwehr Bremen bearbeiten die 18 Wachabteilungsleiterinnen und Wachabteilungsleiter und deren Stellvertreterinnen oder Stellvertreter in den sechs Feuerwachen auch Personalangelegenheiten, beispielsweise Beurteilungen, Stellungnahmen, Vermerke und persönliche Notizen. Die genannten Funktionsträgerinnen und Funktionsträger werden häufig in wechselnden Schichten auf allen Feuerwachen eingesetzt und verfügen über keinen eigenen Zugang zu einem Rechner. Sie melden sich auf jeder Wache immer mit dem gleichen Passwort und denselben für alle gültigen und gleichen Zugangsdaten an. Das einheitliche und vermeintlich geheime Passwort war allen bekannt. Insoweit hatte jede Funktionsträgerin und jeder Funktionsträger Zugriff auf sämtliche Daten einschließlich der genannten sensiblen Personalaktendaten. Um einen Mindestdatenschutz herzustellen, verwendeten einige Beschäftigte private USB-Sticks (Speichersticks), wobei derartige Sticks, auf denen Personaldaten gespeichert waren, bereits verlorengegangen sind oder vergessen wurden.

Wir wiesen die Feuerwehr Bremen auf die datenschutzrechtliche Mangelhaftigkeit dieser Praxis hin. Diese erklärte die Defizite mit der notwendigen Sicherstellung ununterbrochener Aufrechterhaltung des Dienstbetriebs in den Feuerwachen. Das für alle geltende Passwort sei das Erstanmeldekennwort gewesen. Wenn dies bisher nicht geändert worden sei, widerspreche dies der als Dienstanweisung eingeführten IT-Benutzerordnung. Seit 2014 sei eine Basissoftware zur Personalverwaltung eingeführt worden, deren Implementierung Ende 2017 abgeschlossen sein werde. Kurzfristig sei der Zustand nunmehr dahingehend verbessert worden, dass den Angehörigen des vorgenannten Personenkreises persönliche Profile zugeordnet worden seien, sodass personenbezogene Daten nunmehr innerhalb dieses mit einem individuellen Passwort zu sichernden Profils zu verarbeiten seien. Bezüglich der USB-Sticks sei in der IT-Nutzerordnung eindeutig geregelt, dass die Nutzung privater Sticks und die Mitnahme dienstlicher Daten untersagt sei. Soweit dies im Einzelfall tatsächlich passiert sei, könne es nicht mit der Absicht gerechtfertigt werden, einen Mindestdatenschutz zu sichern.

Auf weitere Nachfragen erklärte die Feuerwehr Bremen, sie beabsichtige in Abstimmung mit ihrem behördlichen Datenschutzbeauftragten, eine zusätzliche Software zu installieren, die es ermöglichen werde, unterschiedlichen USB-Geräten den Zugriff auf die USB-Schnittstellen an einem dezidierten Endgerät zu erlauben und andere zu sperren. Mit dem Abschluss der Arbeiten werde bis Herbst 2017 gerechnet.

[1] https://www.datenschutz.bremen.de/sixcms/media.php/13/DSK_Nr14_Besch%E4ftigtendatenschutz.pdf

9.3 Aufzeichnung von Telefongesprächen

Wir erhielten den Hinweis, dass nicht nur die bei der Notrufnummer eingehenden Telefongespräche, sondern darüber hinaus sämtliche bei der Feuerwehr Bremen über die Amtsnummer eingehenden Telefongespräche aufgezeichnet und über einen längeren Zeitraum gespeichert werden. Insoweit wurde das Recht am gesprochenen Wort der über die Amtsnummer anrufenden Personen und der die Gespräche entgegennehmenden Beschäftigten verletzt. Die unbefugte Aufnahme des nicht öffentlich gesprochenen Wortes auf einen Tonträger ist nach § 201 Strafgesetzbuch strafbewehrt (Verletzung der Vertraulichkeit des Wortes). Auf Nachfrage erklärte die Behörde, erst auf unsere Anfrage hin habe sie feststellen müssen, dass die über die Amtsnummer eingehenden Gespräche in der Tat aufgezeichnet wurden. Dies halte sie nicht für erforderlich und habe die zuständige Firma mit der unverzüglichen Änderung dieses Zustandes beauftragt.

9.4 Telefondatenerfassung über den Nebenanschluss

Dem Eigenbetrieb Seestadt Immobilien des Magistrats der Stadt Bremerhaven obliegt die Telefonkostenabrechnung. Zur Klärung ungewöhnlich hoher Telefonkosten forderte ein Beschäftigter des Magistrats von Seestadt Immobilien über den Telekommunikationsanbieter einen Einzelverbindungsnachweis für den entsprechenden Zeitraum an. Nach der Übergabe der Übersicht an Seestadt Immobilien verkürzte der Magistratsbeschäftigte, der Berufsgeheimnisträger im Sinne des § 203 Strafgesetzbuch ist, die Zielnummern derart, dass ein Bezug auf einzelne angerufene Personen nicht mehr herstellbar war. Nachdem eine Klärung der hohen Telefonkosten nicht erreichbar war, erhielt der Beschäftigte von seiner Fachbehörde Einzelverbindungsnachweise seines Nebenanschlusses ohne verkürzte Zielnummern über die entsprechenden Zeiträume. Der Beschäftigte monierte uns gegenüber, dass diese zusätzlichen Dokumente ohne seine Einwilligung offensichtlich vom Telefonanbieter an Seestadt Immobilien übermittelt und an seine Fachbehörde weitergeleitet worden seien. Seestadt Immobilien erklärte, die Beantragung des Einzelnachweises sei von ihr nicht beantragt worden; entsprechende Einzelnachweise würden dort auch nicht vorliegen. Nach der Veränderung des Abrechnungsverfahrens für private Ferngespräche im Jahr 2011 sei eine Differenzierung der getätigten Verbindungen nicht mehr erforderlich. In diesem Einzelfall sei der gewünschte Nachweis nur als Einzelfall aus dem Datenbestand der Telefonanlage ermittelt und dem Beschäftigten im geschlossenen Umschlag übermittelt worden.

Der Telefonanbieter erklärte auf Nachfrage, er habe für den mit dem Magistrat abgeschlossenen Telekommunikationsvertrag die Erstellung eines ungekürzten Einzelverbindungsnachweises nach § 99 Telekommunikationsgesetz (TKG) beantragt. Der gesamte Einzelverbindungsnachweis umfasse den gesamten Rufnummernbereich der

Stadtverwaltung und werde ihr seit dem Vertragsabschluss monatlich zur Verfügung gestellt. Das veränderte Abrechnungsverfahren privater Ferngespräche beim Magistrat habe nicht zur Abbestellung des Einzelverbindungsnachweises geführt.

Zwischenzeitlich stellte sich heraus, dass der zusätzliche Einzelverbindungsnachweis aufgrund eines Missverständnisses zwischen dem Telefonanbieter und der Fachbehörde zur Verfügung gestellt worden war. Danach hatte die Fachbehörde den Telefonanbieter lediglich um Stellungnahme zu den hohen Kosten gebeten, nicht jedoch um die Vorlage des Einzelverbindungsnachweises für diesen Nebenanschluss.

Wir baten Seestadt Immobilien, die monatlichen Einzelverbindungsnachweise über den gesamten Rufnummernbereich des Magistrats mit sofortiger Wirkung abzubestellen, bisher noch vorliegende Einzelverbindungsnachweise unverzüglich zu vernichten oder die entsprechenden personenbezogenen Daten unverzüglich zu löschen. Seestadt Immobilien bestätigte die Umsetzung dieser Maßnahmen.

9.5 Schweigepflichtentbindungserklärung für Arbeitgeber

Ein Arbeitgeber verlangte von einem Beschäftigten, der aus gesundheitlichen Gründen seine Tätigkeit nicht versah, eine Schweigepflichtentbindungserklärung gegenüber dessen behandelndem Arzt. Begründet wurde dies damit, der Arbeitgeber wolle lediglich Informationen erbitten, ob und in welchem Maße der Beschäftigte ohne gesundheitsgefährdende Risiken im Unternehmen eingesetzt werden könne. Zudem wurde der Beschäftigte darauf hingewiesen, zur Abgabe einer Schweigepflichtentbindungserklärung sei er nach arbeitsvertraglichen Grundsätzen verpflichtet. Zusätzlich war der Beschäftigte bereits vom Betriebsarzt untersucht worden; das Ergebnis dieser Untersuchung lag dem Arbeitgeber vor. Auf unsere Anfrage hin vertrat der Arbeitgeber die Auffassung, es sei arbeitsvertragliche Nebenpflicht des Beschäftigten, mit dem Arbeitgeber in Kontakt zu treten, wenn es um künftige Einsatzfähigkeiten gehe. Aus diesem Grund sei die Schweigepflichtentbindungserklärung verlangt worden.

Daraufhin erklärten wir dem Arbeitgeber, dass die Schweigepflichtentbindungserklärung nicht zur Nebenpflicht des Beschäftigten, mit seinem Arbeitgeber in Kontakt zu treten, gehört. Vielmehr reicht es regelmäßig aus, sofern dies im Einzelfall erforderlich sein sollte, den Beschäftigten aufzufordern, sich bei seiner Hausärztin beziehungsweise seinem Hausarzt zulässigerweise verlangte Informationen geben zu lassen und diese an den Arbeitgeber weiterzuleiten. Ebenso können diese Informationen im Rahmen des Betrieblichen Eingliederungsmanagements unter eventueller Beteiligung des Betriebsärztlichen Dienstes eingeholt werden, sofern der Beschäftigte dem zustimmt. Der

Arbeitgeber versicherte uns, zukünftig entsprechend zu verfahren und keine Schweigepflichtentbindungserklärungen mehr zu verlangen.

9.6 Überwachung mit einem Ortungssystem

Die Fahrzeuge eines Transportunternehmens waren mit Global Positioning System (GPS; deutsch Globales Positionsbestimmungssystem) ausgestattet. Uns erreichten Befürchtungen, dass die Fahrerinnen und Fahrer dadurch einer mehr oder weniger lückenlosen Kontrolle ausgesetzt seien. Auf Anfrage erklärte das Unternehmen, eine lückenlose Überwachung der Beschäftigten erfolge nicht. Diese sei nicht Zweck des Ortungsverfahrens. Vielmehr würden die Daten nur fahrzeugbezogen und nicht beschäftigtenbezogen und nur zur Fuhrparkoptimierung, Routenplanung und insbesondere zur Auftragsverwaltung und Auftragsbearbeitung genutzt. Kein Fahrzeug sei einer oder einem bestimmten Beschäftigten zugeordnet. Je nach Schicht, konkreten Aufträgen und Verfügbarkeit werde ein anderes Fahrzeug genutzt. Außerdem teilte uns das Unternehmen mit, die Daten würden nach Abschluss der Auftragsabwicklung beziehungsweise nach Ablauf der Gewährleistungspflichten oder Regressansprüchen gelöscht. Auf Nachfrage bei dem Betreiber des Verfahrens erklärte uns das Unternehmen, es sei eine Löschfrist von 90 Tagen festgelegt worden. Dies war dem Unternehmen bisher nicht bekannt.

Daraufhin legten wir dem Unternehmen dar, dass für die vorgenannten Zwecke eine Frist von 90 Tagen zur Löschung der Ortungsdaten nicht angemessen ist, zumal die fahrzeugbezogenen Daten ohne unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einzelnen Fahrerinnen und Fahrern zugeordnet werden können. Deshalb verlangten wir eine automatische Löschung nach einem Monat.

Daraufhin erklärte das Unternehmen, der Betreiber des Verfahrens könne diesen nach einer bestimmten Zertifizierung festgelegten Standardwert nur mit erheblichen regelmäßigen Kosten auf einen Monat reduzieren. Das Unternehmen schlug vor, eine Dienstanweisung zu erlassen, wonach die zugriffsberechtigen Beschäftigten lediglich bis zu 30 Tagen auf die Ortungsdaten zurückblicken dürfen. Daraufhin verwiesen wir auf § 3 a Bundesdatenschutzgesetz, wonach die Auswahl und Gestaltung von Datenverarbeitungssystemen an den Grundsätzen der Datenvermeidung und Datensparsamkeit auszurichten sind. Dies ist ein wesentlicher Bestandteil einer Vorabkontrolle, insbesondere die Möglichkeit, Systeme anzuschaffen, in denen automatische Löschfristen unterschiedlichen Verarbeitungssituationen oder Verarbeitungszwecken ohne besonderen Aufwand angepasst werden können. Nach diesem Hinweis informierte uns das Unternehmen, es habe sich mit dem Betreiber des Verfahrens geeinigt, die automatische Löschfrist auf einen Monat festzulegen.

9.7 Lückenlose Überwachung durch das Flottenmanagement

Ein Transportunternehmen sah in einer Betriebsvereinbarung vor, dass die Ortungsdaten für insgesamt 20 verschiedene Zwecke im Rahmen des Flottenmanagements verarbeitet werden (beispielsweise für Tourenplanung und Tourenberechnung, Vereinfachung der Kommunikation, Kostenersparnis, Kraftstoffreduzierung, Aufenthaltsnachweise, Erhöhung des Sicherheitsstandards zum Schutz der Beschäftigen, Einhaltung von Reaktionszeiten und Verbesserung der ökologischen Verträglichkeit des Fuhrparks).

Wir erklärten dem Unternehmen, dass die Verarbeitung der Ortungsdaten oder Beschäftigtendaten für die Vielzahl der genannten Zwecke einer lückenlosen Überwachung der Beschäftigten gleichkam. Daher vereinbarten wir nach einem längeren Austausch mit dem Unternehmen, die Zwecke auf ein angemessenes Maß zu reduzieren, und zwar zur Vereinfachung und Optimierung der Tourenplanung und Tourenberechnung, Erhöhung des Sicherheitsstandards zum Schutz der Beschäftigten, Senkung der Kfz-Kosten unter anderem durch Unterstützung von Wartungsprozessen und Instandhaltungsprozessen und zur Einführung eines elektronischen Fahrtenbuches.

9.8 Veröffentlichung von Fotos und Namen

Ein Kreditinstitut hängte in den Schaufenstern seiner Filialen Plakate mit Fotos sowie Vornamen und Zunamen von Beschäftigten aus. Außerdem lagen in den Filialen Flyer mit gleichen Daten der Beschäftigten aus. Zudem wurden bei Online-Banking und der elektronischen Kommunikation (Mailings) die gleichen Daten der Beraterinnen und Berater sowie deren Unterschriften regelmäßig auf den Bildschirmen der häuslichen Rechner oder Smartphones der Kundinnen und Kunden angezeigt. Auf Anfrage erklärte das Institut, es stärke damit die individualisierte Kommunikation ihrer Beschäftigten mit den Kundinnen und Kunden. Die Veröffentlichung der Beschäftigtendaten erfolge nur mit vorheriger Zustimmung der Beschäftigten. Die uns vorgelegte Einverständniserklärung entsprach jedoch nicht den Anforderungen an eine wirksame Einwilligung, wie sie nach § 4 a Absatz 1 Satz 1 Bundesdatenschutzgesetz vorgeschrieben ist. Insbesondere befand sich beim mit "Ja" anzukreuzenden Kästchen der Hinweis, mit der Zustimmung werde der Servicegedanke des Kreditinstituts unterstützt. Beschäftigte erklärten uns hierzu, sie hätten die Einwilligungen erteilen müssen, weil dies vom Unternehmen erwartet worden sei und sie ansonsten in den Verdacht hätten geraten können, "den Servicegedanken" des Arbeitgebers nicht zu unterstützen. Zumindest befürchteten sie für den Fall der Verweigerung einer Einwilligung Nachteile im weiteren Beschäftigungsverhältnis. Nach einem Beschluss des Bundesverfassungsgerichts aus dem Jahr 2006, befinden sich Arbeitnehmerinnen und Arbeitnehmer typischerweise in einer Situation der strukturellen Unterlegenheit, sodass grundsätzlich Zweifel an einer wirksamen Einwilligung im Beschäftigungsverhältnis

bestehen. Dies teilten wir dem Institut mit und baten, die entsprechenden Aushänge in den Schaufenstern und die Flyer zu entfernen sowie die Bilder, Namen und Unterschriften der betroffenen Beschäftigten aus den Mailings und den Internet-Banking-Portalen zu löschen. Der Vorstand des Bankinstituts unterrichtete uns darüber, dass unverzüglich eine entsprechende Anordnung im Unternehmen erlassen worden sei.

10. Videoüberwachung

10.1 Es ist nicht alles, wie es scheint

Die Zahl der Kameramodelle steigt. Die Gewöhnung auch: Videoüberwachung wird ständig ausgeweitet. An allen Ecken und Enden werden Kameras installiert. In jedem erdenklichen Kontext: Videoüberwachung soll gegen Vandalismus, Terroranschläge, abgefahrene Autospiegel und zu viele Menschen in engen Unterführungen helfen. Videoüberwachung soll zeigen, dass der Wolf durchs Land zieht, misst Besucherströme in Warenhäusern und erfasst "natürlich" auch noch die Kinder im Schlaf. Der Gesetzgeber reagiert und erlässt Gesetze, um die Videoüberwachung noch weiter zu "verbessern" (siehe hierzu 39. Jahresbericht, Ziffern 1.2.5, 13.7 und 18.8). "Verbessern" meint "Ausdehnen". Dabei sind wir noch lange nicht am Ende der Fahnenstange angelangt, obwohl schon jetzt die Dunkelziffer der Kameras vermutlich sehr hoch ist. Längst kann kein Mensch mehr die Bilderfluten auswerten. Das wird immer mehr in die "Hände" von Algorithmen gelegt. Nichts geschieht unbemerkt, nichts geht unter: Videoüberwachung ist der Gral, die Lösung für alles.

In den meisten Fällen ist Videoüberwachung erkennbar: Kameras hängen sichtbar allenthalben an Gebäuden, in Geschäften und Unterführungen, in der Straßenbahn, auf öffentlichen Plätzen. Erfasste Bereiche sollen mit entsprechenden Hinweisschildern gekennzeichnet werden. DIN 33450 beschreibt, wie das aussehen sollte. Das Schild zeigt eine Kamera, wie sie Fernsehjournalistinnen und Fernsehjournalisten vor sich haben. Keine Dome-Kamera, die den ungeübten Augen wie ein Dekorationselement erscheint. Aber Videoüberwachung erfolgt auch verdeckt: in Deckenplatten, Vogelnistkästen oder Feuermelder Imitaten. Der Elektronikfachhandel hält allerlei Gerätschaften bereit: Kameras im Schlüsselbund, in der Powerbank fürs Handy, im Feuerzeug, in der Uhr auf dem Tisch oder am Arm, im Bilderrahmen, in einer Wetterstation und im Kugelschreiber. Dazu noch die getarnte Wildkamera. Alles auch mit Bewegungssensor zu bekommen. Und mit Infrarotdioden, damit alles auch bei Dunkelheit funktioniert. Sichtbare Videoüberwachung durch eine Vielzahl von Kameras hat einen Gewöhnungseffekt, verdeckte weckt Misstrauen, in einigen Fällen Widerstand.

Der drückt sich auch in einer steigenden Zahl von Beschwerden bei der Landesbeauftragten für Datenschutz und Informationsfreiheit aus. Wir nehmen im Rahmen unserer Prüfungen

sehr oft Einsicht in Bilddaten aus der Videoüberwachung, sehen die erfassten Bereiche und Menschen, die sich in diesen Bereichen aufhalten (müssen). Wir sehen die Bildwinkel, die Lichtverhältnisse und stellen Fragen nach dem Zweck der Videoüberwachung. Sehr oft zeigt sich, dass die Kamerabilder so gut wie gar nicht dazu taugen, die Zwecke, für die sie erhoben werden, zu erreichen. Auch in solchen Fällen, in denen eine Videoüberwachung zulässig wäre. Zu häufig war ihre Anschaffung also eine Fehlinvestition, die Zeit und Geld gekostet, nichts gebracht und auch noch einen unerwünschten Kontakt mit der Datenschutzaufsichtsbehörde beschert hat.

10.2 Fähren

Wir stellten fest, dass Kameras auf den Fähren eines Unternehmens die gesamte Fläche erfassen, auf der die Beschäftigten die Fahrzeuge einweisen und die Fährgebühren kassieren. Insoweit wurden sämtliche Tätigkeiten der Beschäftigten mehr oder weniger lückenlos erfasst. Auf Anfrage erklärte die Geschäftsführung, Zwecke der Videoüberwachung seien die Überwachung des Fährverkehrs, die Erhöhung der Sicherheit der an Bord Beschäftigten, die Aufklärung von Regressansprüchen von Fahrgästen gegenüber dem Fährbetrieb und von durch Fahrgäste begangene Straftaten. Die Videodaten würden nicht für Leistungskontrollen und Verhaltenskontrollen, Leistungsvergleiche oder Leistungsbemessungen der Beschäftigten genutzt.

Wir baten die Geschäftsführung darzulegen, welche konkreten Gefährdungen der genannten Zwecke bisher eingetreten seien, die eine Videoüberwachung erforderlich machten. Dabei verwiesen wir auf die ständige Rechtsprechung des Bundesarbeitsgerichts, wonach eine lückenlose Überwachung der Beschäftigten einen unzumutbaren Überwachungsdruck darstellt und daher unverhältnismäßig ist. Die daraufhin genannten Beispiele konnten die Videoüberwachung nicht rechtfertigen. Eine vom Unternehmen zur Videoüberwachung mit dem Betriebsrat abgeschlossene Betriebsvereinbarung entsprach insbesondere hinsichtlich der Speicherung der Videodaten nicht den datenschutzrechtlichen Anforderungen. Letztendlich wurde mit dem Fährunternehmen vereinbart, dass die Videoüberwachung ausschließlich im Wege des Monitoring erfolgt und technische Maßnahmen getroffen werden, um eine Aufzeichnung auszuschließen. Die Kameras erfassen nunmehr nur die Bereiche, die der Schiffsführer aufgrund der Bauweise der Fähren und der Einschränkung von Blickwinkeln nicht ohne den Einsatz von Videokameras erkennen kann, um den ordnungsgemäßen und sicheren Betrieb der Fähren zu gewährleisten.

10.3 Restaurant

Hinweisen zufolge sollte ein Restaurant zwei Videokameras im Gastraum zur Kontrolle der Beschäftigten installiert haben. Dieses Restaurant hatte bereits im vorangegangenen Jahr

auf unsere Veranlassung Videokameras entfernt und gegen Bewegungsmelder ausgetauscht. Auf Anfrage erklärte der Geschäftsführer nunmehr, inzwischen seien diese Bewegungsmelder im Rahmen von Umbaumaßnahmen durch neue Bewegungsmelder ausgetauscht worden. Sie lösten keinen Alarm mehr aus, sondern dienten nur zur Abschreckung.

Bei einer Vorortprüfung konnte nicht mit Sicherheit festgestellt werden, um was für Geräte es sich bei den wie Kameras oder Kameraattrappen aussehenden Geräten tatsächlich handelte. Der Geschäftsführer erklärte, es handele sich um Kameraattrappen. Seine Beschäftigten sollten dies nicht erfahren, weil nur so Diebstahlsdelikten vorgebeugt werden könne. Da auch die Vortäuschung einer ständigen Überwachung Beschäftigter rechtswidrig ist, verlangten wir den Abbau der Geräte, der inzwischen erfolgt ist.

10.4 Eiscafékette

Im Berichtsjahr wurden wir darauf hingewiesen, dass in mehreren Filialen einer Eiscafékette sowohl im Innenbereich als auch im Außenbereich zahlreiche Videokameras installiert seien, die augenscheinlich eine Überwachung von Gästen sowie Beschäftigten ermöglichten. Auf unsere Anfrage hin bestätigte uns die Geschäftsführung die Installation etlicher Kameras in den einzelnen Filialen. Aufgrund der Vielzahl von Kameras an verschiedensten Standorten in den Filialen führten wir eine Vorortprüfung durch, um die Kamerastandorte in Augenschein zu nehmen und die aufgezeichneten Bilddaten einzusehen. Hierbei stellten wir fest, dass die Kameras sowohl die Verkaufstresen als auch Teilbereiche der Sitzbereiche mit erfassten und alle Kamerabilder rund um die Uhr aufgezeichnet wurden. In unserem Prüfbericht teilten wir dem Geschäftsführer mit, dass Cafés während der Öffnungszeiten typischerweise Orte sind, an denen sich die Kundinnen und Kunden zur Erholung und Entspannung aufhalten und dabei Kontakte pflegen, essen, trinken, sich ungezwungen miteinander unterhalten oder einfach nur für sich allein "chillen" möchten. Daher ist eine Videoüberwachung der in Cafés und Gaststätten eingerichteten Sitzplätze durchweg ausgeschlossen. Auch handelt es sich bei Cafés und Gaststätten allgemein um Orte, an denen sich die Kundinnen und Kunden nicht nur kurz aufhalten und sie weisen auch kein erhöhtes Gefährdungspotenzial auf, um eine Aufzeichnung im bisherigen Umfang rechtfertigen zu können.

Letztlich konnten wir die Geschäftsführung davon überzeugen, dass eine Aufzeichnung der Videodaten rund um die Uhr nicht erforderlich sei. Es wurde uns mitgeteilt, dass nunmehr eine Aufzeichnung der Daten nur noch nach Geschäftsschluss stattfinde. Auf diesen Umstand soll in den einzelnen Filialen künftig durch deutlich sichtbare Hinweisschilder hingewiesen werden. Zwischenzeitlich wurde uns schriftlich bestätigt, dass die Umsetzung der weiteren von uns im Prüfbericht geforderten Maßnahmen erfolgt sei. In Bezug auf die in den Thekenbereichen installierten Kameras konnten wir erreichen, dass die

Erfassungswinkel verschiedener Kameras angepasst wurden, sodass die Überwachung der Mitarbeiterinnen und Mitarbeiter nicht mehr möglich ist. Außerdem wurde eine im Lagerbereich einer Filiale angebrachte Kamera abmontiert, da mit ihr eine Überwachung der Mitarbeiterinnen und Mitarbeiter möglich gewesen wäre.

10.5 Großbaustelle

Mehrere aufgebrachte Bürgerinnen und Bürger beschwerten sich im Berichtsjahr fast zeitgleich über Videokameras, die auf einem Baustellengelände installiert worden waren. Nach Auffassung der Bürgerinnen und Bürger war aufgrund der Wahl der Kamerastandorte zu befürchten, dass die unmittelbar angrenzende Straße, der Fußweg sowie Parkplätze überwacht würden.

Bei unserer Vorortsichtung konnten wir die verantwortliche Stelle für das Bauvorhaben ermitteln und feststellen, dass an drei mobilen Beleuchtungsmasten je eine Dome-Kamera installiert war. Durch Bauart der Kamera und Anordnung der Beleuchtungsmasten auf dem Baustellengelände war durch bloße Inaugenscheinnahme nicht auszuschließen, dass unmittelbar an die Baustelle angrenzende, öffentlich zugängliche Bereiche (Fußweg, Straße und Parkplätze) mit überwacht werden konnten. Das galt ebenso für Häuser und Vorgärten, die der Baustelle auf der anderen Straßenseite direkt gegenüberliegen und für die auf der Baustelle tätigen Handwerker. Die verantwortliche Stelle teilte uns auf unsere schriftlichen Anfragen hin mit, dass keine öffentlichen Bereiche mit erfasst würden, da diese ausgeblendet würden und auch bei einer Einsicht in die aufgezeichneten Daten im Nachgang nicht wieder sichtbar gemacht werden könnten. Eine Aufzeichnung der erfassten Bereiche würde ausschließlich außerhalb der Arbeitszeiten durchgeführt. Während der Arbeitszeit sei die Kamera zur Eigensicherung in das Innere des Turms gerichtet, wodurch eine Erfassung der auf der Baustelle tätigen Handwerker ausgeschlossen sei. Des Weiteren sei es durch diese Kameraausrichtungen nicht möglich, Livebilder vom Baufortschritt bereitzustellen. Eine Aufzeichnung der erfassten Bilder würde nur außerhalb der Arbeitszeiten durchgeführt und nach 72 Stunden automatisch wieder gelöscht. Anhand der übersandten Unterlagen sowie der zur Verfügung gestellten Screenshots (Bildschirmausdrucke) der einzelnen Kameraerfassungsbereiche konnten wir feststellen, dass tatsächlich keine öffentlich zugänglichen Bereiche von den Kameras erfasst werden und somit kein Verstoß gegen datenschutzrechtliche Vorschriften festzustellen war.

10.6 Straßenzüge mit Wohnhäusern

Durch eine Eingabe wurden wir darauf aufmerksam gemacht, dass im April 2017 Panoramaansichten aller Straßen Bremerhavens im Auftrag des Vermessungs- und Katasteramts Bremerhaven angefertigt werden sollten. Diese Aufnahmen sollten

verwaltungsintern durch verschiedene Behörden Bremerhavens genutzt werden, soweit dies erforderlich ist, um Vor-Ort-Besichtigungen durch Mitarbeiterinnen und Mitarbeiter von Behörden und damit Dienstgänge und Dienstzeit zu sparen. Auf unsere Nachfrage erfuhren wir, dass die Aufnahmen durch ein privates Unternehmen, das sich dem von der Geodatenwirtschaft formulierten "Datenschutz-Kodex" unterworfen hatte, angefertigt werden sollten. Der Stadt Bremerhaven und ihren hundertprozentigen Tochtergesellschaften sollten die Aufnahmen im Rahmen einer mit diesem Unternehmen abgeschlossenen Lizenzvereinbarung dauerhaft, aber nicht exklusiv und nicht übertragbar zur internen Verwendung zur Verfügung gestellt werden. Der Zugang sollte über eine spezielle Hosting-Software des Unternehmens erfolgen, die unter Eingabe von Zugangsdaten den Zugriff auf die Panoramaansichten beim Unternehmen selbst ermöglicht, ohne dass die Stadt Bremerhaven selbst darüber verfügen kann. Da sich das Unternehmen verpflichtet hatte, Gesichter und Autokennzeichen vor der Zugriffsgewährung unkenntlich zu machen und vorab über die geplanten Aufnahmen im Internet und in der Nordseezeitung berichtet wurde, wobei auch die Möglichkeit benannt wurde, bei dem Unternehmen Widerspruch gegen die unverpixelte Ansicht des eigenen Hauses einzulegen, bestand für uns kein Anlass gegen die geplanten Aufnahmen einzuschreiten.

Wir sehen es weiterhin (siehe hierzu 33. Jahresbericht, Ziffer 1.1.3) kritisch, dass der "Datenschutz-Kodex" für Geodatendienste keine generelle Verpflichtung zur Ermöglichung eines Vorabwiderspruchs für betroffene Bürgerinnen und Bürger beinhaltet. Auch müsste zumindest bei einer Veröffentlichung von Aufnahmen, wenn also nicht nur die Einsichtnahme durch einen geschlossenen Benutzerkreis wie hier vorgesehen ist, ein Widerspruch auch hinsichtlich der unverpixelten Darstellung weiterer personenbezogener Abbildungen möglich sein. So sollten zum Beispiel nicht nur Gesichter, sondern auch ganze Personen verpixelt werden können. Aus diesen und weiteren Gründen wurde der "Datenschutz-Kodex" auch nicht durch die Aufsichtsbehörden als Verhaltensregel im Sinne von § 38 a Bundesdatenschutzgesetz anerkannt.

11. Kreditwirtschaft und Auskunfteien

11.1 Kundenfragebogen bei der Wertpapierberatung

Das Wertpapierhandelsgesetz in der bis zum 2. Januar 2018 geltenden Fassung differenzierte im Hinblick auf den Datenerhebungsumfang wie auch die Folgen fehlender Erkenntnisse über kundenseitige Verhältnisse deutlich zwischen verschiedenen Formen denkbarer Wertpapierdienstleistungen. Es sah vor, dass Kreditinstitute und andere Wertpapierdienstleister in Fällen einer Anlageberatung oder Finanzportfolioverwaltung die erforderlichen Informationen zu Kenntnissen/Erfahrungen, zu Anlagezielen und zu den finanziellen Verhältnissen der Kundinnen und Kunden erheben durften, aber auch mussten.

Im Falle der Nichtermittelbarkeit dieser Informationen im erforderlichen Umfang durfte der Wertpapierdienstleister nämlich keine eigenen Empfehlungen hinsichtlich etwaiger Anlagemöglichkeiten oder hinsichtlich etwaiger Möglichkeiten der Finanzportfolioverwaltung abgeben. Bei anderen Wertpapierdienstleistungen als Anlageberatung und Finanzportfolioverwaltung war dem Dienstleister lediglich eine Ermittlung der Kenntnisse/Erfahrungen seiner Kundinnen und Kunden im Hinblick auf die gewünschte Wertpapierdienstleistung vorgeschrieben. Sollten diese Kenntnisse/Erfahrungen nicht in Erfahrung gebracht werden können, musste der Wertpapierdienstleister seine Kundschaft lediglich darüber informieren, dass er nicht beurteilen könne, ob die ausgewählte Wertpapierdienstleistung für sie angemessen sei. Unrichtige oder unvollständige Informationen seitens der Kundinnen und Kunden führten grundsätzlich zu einer Haftungsentlastung beim Wertpapierdienstleister, falls er wegen fehlerhafter Beratung haftbar gemacht werden sollte.

Um die benötigten Kundeninformationen zur Erbringung von Wertpapierdienstleistungen einzuholen, setzten alle Kreditinstitute eines bestimmten Bankenfachverbands bundesweit einen einheitlichen Kundenfragebogen ein. An der inhaltlichen Gestaltung des Fragebogens hatte sich bereits im Jahr 2008 die Kritik der Datenschutzaufsichtsbehörden entzündet. Bei den zu beantwortenden Fragen fehlte nämlich die vorstehend beschriebene, im Gesetz angelegte deutliche Differenzierung zwischen den benötigten Informationen für Anlageberatung und Finanzportfolioverwaltung einerseits und den benötigten, begrenzteren Informationen für andere Wertpapierdienstleistungen andererseits. Zudem enthielt der Kundenfragebogen den unzutreffenden Hinweis, dass eine Anlageberatung bei unvollständigen Angaben der Kundin oder des Kunden (etwa zu seinen finanziellen Verhältnissen) gesetzlich untersagt sei.

In der Folgezeit drängten wir gemeinsam mit der baden-württembergischen Datenschutzaufsichtsbehörde immer wieder auf eine Abänderung des Kundenfragebogens. Da sich aber schon früh neue europäische Rechtsvorgaben für die Finanzmärkte abzeichneten, die eine Anpassung (auch) des Wertpapierhandelsgesetz durch die mitgliedstaatlichen Gesetzgeber erforderlich machen würden, und nicht auszuschließen war, dass von diesen Änderungen auch die Vorschriften erfasst würden, die die Kundendatenerhebung bei den Wertpapierdienstleistungen regelten, sahen wir von einer Anordnung ab und erklärten uns mit einem Abwarten auf diese gesetzlichen Änderungen einverstanden. Andernfalls hätten die Kundenfragebögen möglicherweise kurzfristig mehrfach angepasst werden müssen. Unerwartet ließ sich dann allerdings der deutsche Gesetzgeber mehrere Jahre bis kurz vor Ablauf der europäischen Umsetzungsfrist Zeit, die deutschen Finanzmarktvorschriften einschließlich des Wertpapierhandelsgesetzes an die europäischen Rechtsvorgaben anzupassen. Erst Ende Juni 2017 war mit dem Erlass des Zweiten Finanzmarktnovellierungsgesetzes (Bundestagsdrucksache 18/10936), das

zahlreiche Änderungen in vielen einzelnen Fachgesetzen zusammenfasste, absehbar, welchen Inhalt auch das neue, künftig geltende Wertpapierhandelsgesetz (Inkrafttreten am 3. Januar 2018) und damit auch seine die Kundendatenerhebung regelnden Vorschriften haben würden.

Nachdem das künftig geltende Wertpapierhandelsgesetz die bisherige Differenzierung im Kundendatenerhebungsumfang je nach Wertpapierdienstleistung fortschrieb, reagierte der Bankenfachverband zügig und legte eine Neufassung des Fragebogens vor, die unserer bisherigen datenschutzrechtlichen Kritik am Kundenfragebogen vollumfänglich und überzeugend Rechnung trug. Was lange währt, wird endlich gut.

11.2 Kontoeröffnungen des Amtsvormunds für sein Mündel

Durch die Mitteilung einer Mitarbeiterin des Jugendamts wurden uns datenschutzrechtliche Schwierigkeiten im Zusammenhang mit Kontoeröffnungen des Jugendamts für Mündel bei einem Kreditinstitut bekannt. Das Jugendamt kann in besonderen familiären Situationen durch Beschluss des Familiengerichts zum Amtsvormund für eine minderjährige Person, das sogenannte Mündel, bestellt werden. Die mit der Vormundschaft des Jugendamts verbundenen Aufgaben werden durch eine Mitarbeiterin oder einen Mitarbeiter des Jugendamts wahrgenommen. Die Aufgabenbetrauung dieser Jugendamtsbeschäftigten erfolgt förmlich und ist somit klar und rechtssicher dokumentiert. Obwohl die gesetzliche Formulierung im Sozialgesetzbuch VIII insoweit missverständlich ist, ist nach allgemeiner Rechtsauffassung allein das Jugendamt als Behörde Vormund und damit der alleinige gesetzliche Vertreter des Mündels. Hingegen werden selbstverständlich nicht die für das Jugendamt handelnden Beschäftigten als Privatpersonen gesetzliche Vertreter des Mündels. Zur Aufgabenstellung des Amtsvormunds "Jugendamt" gehört auch die sogenannte Vermögenssorge für das Mündel. In Wahrnehmung der Vermögenssorge kann das Jugendamt durch die handelnden Mitarbeiterinnen und Mitarbeiter für das Mündel bei Bedarf ein Konto bei einem Kreditinstitut eröffnen.

Ein hiesiges Kreditinstitut führte nun bei solchen Kontoeröffnungen durch Mitarbeiterinnen und Mitarbeiter des Jugendamts für Mündel Personenidentifizierungen bei diesen Amtsmitarbeiterinnen und Amtsmitarbeitern durch. Zur Begründung berief es sich auf die Identifizierungspflichten des Geldwäschegesetzes. Zwecks Durchführung der Identifizierung forderte das Kreditinstitut also von den Jugendamtsbeschäftigten die Vorlage des privaten Personalausweises. Sodann durchforstete es seinen Datenbestand auf das Vorhandensein von Daten aus Bankverträgen der Betreffenden als Privatkundinnen und Privatkunden und verknüpfte diese gegebenenfalls mit den Kontovertragsdaten des Mündels. Schließlich übernahm das Kreditinstitut persönliche Daten der Beschäftigten des Jungendamts unter der Rubrik "gesetzlicher Vertreter" (insbesondere Name und Privatanschrift) in den seitens des

Mündels auszufüllenden Kontoeröffnungsbogen. Letzteres hatte zur Folge, dass dem Mündel mit Aushändigung der Kontoeröffnungsunterlagen persönliche Daten der betreffenden Mitarbeiterinnen und Mitarbeiter des Jugendamts bekannt wurden, datenschutzrechtlich gesprochen also eine Datenübermittlung durch das Kreditinstitut an das Mündel stattfand. Da bei Ausübung der Amtsvormundschaft durch die Jugendamtsbeschäftigten mitunter erhebliche Konflikte mit dem Mündel und eventuell auch dessen Angehörigen auftreten können, war diese Mitteilung des Namens und der Wohnanschrift geeignet, zu einer massiven Gefährdung der betreffenden Mitarbeiterinnen und Mitarbeiter des Jugendamts zu führen.

Dieser Gefährdung ließ sich schon durch Nichteintrag der persönlichen Daten der Amtsmitarbeiterin oder des Amtsmitarbeiters in den Kontoeröffnungsunterlagen begegnen. Gleichwohl warf das Vorgehen des Kreditinstituts die Grundfrage auf, ob das durchgeführte Personenidentifikationsverfahren gegenüber einer beziehungsweise einem Staatsbediensteten, der jederzeit nachprüfbar durch einen familiengerichtlichen Beschluss, einen dokumentierten behördlichen Auftrag und schließlich seinen Amtsausweis ausgewiesen sowie jederzeit ermittelbar ist und bei der Kontoeröffnung unmittelbar eine staatliche Aufgabe wahrnimmt, angebracht und gesetzgeberisch gewollt sein kann.

Das Geldwäschegesetz schreibt vor, dass Kreditinstitute insbesondere bei der Begründung von Geschäftsbeziehungen ihre *Vertragspartner* und gegebenenfalls die *für diese auftretenden Personen* zu identifizieren haben. Die näheren Regelungen des Geldwäschegesetzes zu Art und Weise der Identifizierung unterscheiden danach, ob eine natürliche Person oder eine juristische Person zu identifizieren ist. Nur bei der Identifizierung von natürlichen Personen ist eine Ausweiskontrolle und eine entsprechende Erfassung persönlicher Daten, wie Geburtsdatum et cetera, erforderlich. Bei juristischen Personen hingegen können und müssen andere Angaben erhoben und überprüft werden. Der nach dem Geldwäschegesetz zu identifizierende Vertragspartner des Kreditinstituts ist das Mündel selbst, auch wenn es aufgrund seiner Minderjährigkeit nicht alleine einen Vertrag mit dem Kreditinstitut über die Kontoeröffnung abschließen kann, sondern der Mithilfe seines Vormunds als seines gesetzlichen Vertreters bedarf. Die tatsächlich die Kontoeröffnung durchführenden Jugendamtsbeschäftigten hingegen sind nicht Vertragspartner, daher also auch nicht als Vertragspartner zu identifizieren. So bleibt die Frage, ob die Mitarbeiterinnen und Mitarbeiter des Jugendamts als "für den Vertragspartner auftretende Person" zu identifizieren sind. Dabei ist zu berücksichtigen, dass sie nicht als Privatperson tätig werden, sondern lediglich als "Teil" des Jugendamts als gesetzlichen Vertreters des Mündels. Das Jugendamt wiederum ist eine rechtlich unselbständige Behörde der Freien Hansestadt Bremen. Die Freie Hansestadt Bremen selbst ist eine juristische Person des öffentlichen Rechts. Rechtlich zutreffen kann es daher nur, die juristische Person "Freie Hansestadt Bremen" selbst durch ihr Jugendamt als die "für den Vertragspartner auftretende Person" im

Sinne des Geldwäschegesetzes zu betrachten. Zur Anwendung kommen können daher nur die Identifizierungsregelungen für juristische Personen. Dieses Ergebnis deckt sich mit der steuerrechtlichen Vorgabe der sogenannten Kontenwahrheit. Nach einem Anwendungserlass des Bundesministeriums für Finanzen zur Abgabenordnung müssen Kreditinstitute nämlich dann keine Legitimationsprüfung durchführen, sind also von der Verpflichtung, sich über die Person und Anschrift des Kontoverfügungsberechtigten Gewissheit zu verschaffen, befreit, wenn insbesondere ein Fall der Amtsvormundschaft gegeben ist. Im Übrigen ist mit der Identifizierung der Freien Hansestadt Bremen nach den Identifizierungsvorgaben für juristische Personen auch völlig dem Zweck des Geldwäschegesetzes, Finanzen und Finanzströme zuordenbar und kontrollierbar zu machen, genügt.

Nachdem wir das Kreditinstitut angeschrieben und auf die eintretende Gefährdung der Mitarbeiterinnen und Mitarbeiter des Jugendamts hingewiesen und unsere Rechtsbedenken gegenüber der praktizierten Personenidentifizierung der Jugendamtsbeschäftigten geltend gemacht hatten, reagierte das Kreditinstitut sofort und gestaltete seine Datenverarbeitungsprozesse so um, dass in Amtsvormundschaftsfällen als handelnde Person die Freie Hansestadt Bremen durch das Jugendamt aufgenommen und kein Personendatensatz für die Jugendamtsbeschäftigten mehr angelegt wird. In den Kontoeröffnungsunterlagen erscheint für das Mündel in der Rubrik "gesetzlicher Vertreter" zutreffend lediglich das Jugendamt mit seinem Dienstsitz.

11.3 Fragwürdiger Bestandsschutz für Scoringverfahren

Über die Notwendigkeit, die Regelung des § 28 b Bundesdatenschutzgesetz (BDSG) zum sogenannten Scoring zu novellieren, hatten wir im letzten sowie vorletzten Jahresbericht (siehe hierzu 39. Jahresbericht, Ziffer 14.4 und 38. Jahresbericht, Ziffer 13.6) bereits berichtet. Obwohl das im Auftrag der Bundesregierung erstellte, Mitte 2014 vorgelegte Scoringgutachten erheblichen Reformbedarf aufgezeigt und die Verbraucherschutzministerkonferenz im Mai 2015 in einem einstimmigen Beschluss Handlungsbedarf des Gesetzgebers festgestellt hatte, wurde die bestehende defizitäre Regelung in der 18. Legislaturperiode des Bundestages gesetzgeberisch bestätigt. Der Gesetzgeber schuf nämlich mit § 31 Absatz 1 im neuen Bundesdatenschutzgesetz (BDSG-neu) eine Vorschrift zum Scoring, die nahezu unverändert die bisherige Regelung aufrechterhält. Wie wenig der Gesetzgeber dabei den Schutz der von Scoringverfahren betroffenen Personen im Sinn hatte, zeigt die amtliche Überschrift der Vorschrift in bemerkenswerter Ehrlichkeit. Sie lautet: "Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften". Der Zweck der neuen Vorschrift, nämlich Aufrechterhaltung der Scoringsysteme deutscher Wirtschaftsauskunfteien und Absicherung der ungehinderten Verwertbarkeit ihrer Scoringprodukte durch Online-Händler und andere Auskunfteienkunden,

hätte kaum deutlicher formuliert werden können. Ob dem nationalen Gesetzgeber hiermit Erfolg beschieden ist, wird sich erst noch zeigen müssen. Es sprechen gewichtige Gründe dafür, dass die Vorschrift mit der Datenschutzgrundverordnung (DSGVO) unvereinbar ist, also schlicht gegen europäisches Recht verstößt.

Die DSGVO enthält eine eigenständige Definition des Begriffs "Profiling", unter den das Scoring fällt, sowie Erläuterungen zu Zulässigkeitsvoraussetzungen des Profilings in Erwägungsgrund 71 Unterabsatz 2 sowie Erwägungsgrund 72. Bereits dies spricht für die Absicht einer europaweiten Rechtsvereinheitlichung und gegen die Zulässigkeit einer individuellen mitgliedstaatlichen Vorschrift, die Scoring als Unterfall des Profilings eigenständig begrifflich definiert und eigenständig Voraussetzungen des Scorings festlegt. Zwar greift die Scoringvorschrift des § 31 Absatz 1 BDSG-neu die Festlegungen der DSGVO zum Profiling teilweise auf und wiederholt sie; zugleich normiert sie aber auch eigene Zulässigkeitskriterien und beschränkt den Anwendungsbereich des Scorings entgegen Artikel 4 Ziffer 4 DSGVO auf Vertragsverhältniszusammenhänge. Auch Erwägungsgrund 72 Satz 2, in dem eine Schaffung von Leitlinien zum Profiling durch den Europäischen Datenschutzausschuss als Option vorgesehen ist, und daneben die Verhandlungen zwischen Rat, der Europäischen Kommission und dem Europäischen Parlament zur DSGVO belegen, dass der europäische Gesetzgeber das Profiling späteren, näheren europäischen Regelungen überlassen wollte.

Dementsprechend fehlt in der DSGVO auch eine Ermächtigung für mitgliedstaatliche Gesetzgeber zum Erlass rein nationaler Scoringvorschriften. Die Gesetzesbegründung zu § 31 BDSG-neu schweigt sich bezeichnenderweise zur europarechtlichen Ermächtigungsgrundlage dieser Vorschrift aus (siehe hierzu Bundestagsdrucksache 18/11325, Seite 101 zu § 31). Die fehlende Regelungsbefugnis der Mitgliedstaaten war im dritten Referentenentwurf eines neuen Bundesdatenschutzgesetzes erkannt worden und führte zu einem Verzicht auf einen Scoringparagrafen. Im vierten Referentenentwurf, der in die Kabinettsfassung und damit in die letztlich verabschiedete Fassung mündete, fand sich hingegen erneut, unter welcher Einflussnahme auch immer, die nunmehrige Scoringvorschrift.

Insbesondere Artikel 22 Absatz 2 Buchstabe b DSGVO, der mitgliedstaatliche Regelungen zulässt, ist keine Ermächtigung für den Erlass des § 31 Absatz 1 BDSG-neu. Artikel 22 DSGVO befasst sich nämlich mit der ausschließlich auf automatisierten Datenverarbeitungsprozessen ohne menschliches Zutun beruhenden *Entscheidungsfindung* gegenüber betroffenen Personen, hingegen nicht mit den die Entscheidungsfindung lediglich vorbereitenden automatisierten Datenverarbeitungsprozessen wie beispielsweise dem Profiling. Dementsprechend sind die Mitgliedstaaten auch nur befugt, vom Verbot automatisiert generierter Entscheidungsfindung Ausnahmen zuzulassen. Das in § 31

Absatz 1 BDSG-neu geregelte Scoring der Auskunfteien stellt aber selbst keine Entscheidungsfindung dar, sondern ist vielmehr nur Grundlage und Vorbereitung der Entscheidungsfindung der Online-Händler und anderer Kundinnen und Kunden von Auskunfteien über Vertragsabschlüsse mit betroffenen Personen.

Auch die Artikel 85 fortfolgende (ff.) DSGVO, die in bestimmten Bereichen mangels gemeinsamer europäischer Standards beziehungsweise europäischer Kompetenzen den Mitgliedstaaten Regelungsspielräume eröffnen, kommen als Grundlage für den Erlass der Scoringvorschrift nicht in Betracht. Zwar regelt der Gesetzesabschnitt des BDSG-neu, dem § 31 zugehört, laut Überschrift wie auch Gesetzesvorwort "Besondere Verarbeitungssituationen" (Teil 2, Kapitel 1, Abschnitt 2), soll also die Artikel 85 ff. DSGVO umsetzen (§ 26 BDSG-neu den Artikel 88 DSGVO; §§ 27, 28 BDSG-neu den Artikel 89 DSGVO; § 29 BDSG-neu den Artikel 90 DSGVO). Scoring, als Unterfall des Profilings, ist aber lediglich eine Form einer Datenanalyseanwendung, einerlei in welcher Lage beziehungsweise unter welchen Umständen es eingesetzt wird. Es ist damit gerade keine "besondere Datenverarbeitungssituation" im Sinne der Artikel 85 ff. DSGVO.

Auch Artikel 6 Absätze 2, 3 DSGVO sind als Regelungsermächtigung für § 31 BDSG-neu nicht tragfähig. Denn sie ermächtigen nationale Gesetzgeber nicht zu einer "Präzisierung" der Verarbeitungsbefugnis aus Artikels 6 Absatz 1 Buchstabe f DSGVO, auf die das Scoring der Wirtschaftsauskunfteien allein gestützt werden kann. Zulässig sind vielmehr lediglich mitgliedstaatliche Regelungen entweder bei einer "Erforderlichkeit der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt" (Artikel 6 Absatz 1 Buchstabe c DSGVO oder bei einer "Erforderlichkeit der Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse beziehungsweise in Ausübung öffentlicher Gewalt" (Artikel 6 Absatz 1 Buchstabe. e DSGVO; diese beiden Verarbeitungsgrundlagen sind nach ihrer Entstehungsgeschichte und der Systematik (siehe etwa die Regelung der Aufsichtszuständigkeit in Artikel 55 Absatz 2 DSGVO) primär also auf Datenverarbeitungen zur Staatsaufgabenerfüllung gemünzt. Weder gibt es aber eine rechtliche Verpflichtung der Wirtschaftsauskunfteien zum Scoring noch erfüllen Wirtschaftsauskunfteien mit dem Scoring Staatsaufgaben. Scheinbar soll allerdings mit der Gesetzesbegründung zu § 31 BDSG-neu suggeriert werden, dass es ein öffentliches Interesse am Scoring gebe. Dort heißt es, Verbraucher vor Überschuldung zu schützen, liege sowohl im Interesse der Verbraucher selbst als auch der Wirtschaft. Die Ermittlung der Kreditwürdigkeit und die Erteilung von Bonitätsauskünften bildeten das Fundament des deutschen Kreditwesens und damit auch der Funktionsfähigkeit der Wirtschaft.

Bezogen auf das Scoring der Wirtschaftsauskunfteien ist diese Gesetzesbegründung bei näherem Hinsehen weder unter dem Aspekt "Verbraucherüberschuldungsschutz" noch unter dem Aspekt "Funktionsfähigkeit der Wirtschaft" von Substanz. Schon die Rechtsformen der

deutschen Wirtschaftsauskunfteien mit Scoringangebot belegen, dass diese Akteure des Privatwirtschaftsverkehrs mit Gewinnerzielungsabsicht sind und folgerichtig auch mit ihrem Datenprodukt "Scoring" ausschließlich rein private erwerbswirtschaftliche Zwecke verfolgen, mitnichten jedoch gemeinnützige Ziele oder gar ein öffentliches Interesse. Hieran ändert auch das Ermöglichen einer Beschleunigung von Geschäftsabschlüssen auf Kreditbasis im Privatwirtschaftsverkehr nichts. Geschäftszweck der Auskunfteien ist es insbesondere nicht, Verbraucherinnen und Verbraucher vor Überschuldung zu schützen. Die unter § 28 b BDSG etablierten, gängigen Scoringverfahren, die Regelungsgegenstand des § 31 BDSG-neu sind, sind weder dafür konzipiert noch geeignet, einen individuellen Überschuldungsschutz zu bewirken. Drei der vier als Hauptauslöser einer Überschuldung bei natürlichen Personen geltenden Gründe, nämlich Arbeitsplatzverlust, Trennung sowie Krankheit, sind individuelle, oftmals unvorhersehbar eintretende Lebensumstände, die nicht Gegenstand der Scoringverfahren der Auskunfteien sind und es ihrem Wesen nach nicht sein können. Scoringverfahren blenden zudem gerade die individuelle, tatsächliche Finanzsituation Betroffener aus und bieten anstelle dessen eine rein statistische, vergleichsgruppenbezogene Finanzeinschätzung. Sie haben also mit einer individuellen Ermittlung der Kreditwürdigkeit einer natürlichen Person wenig zu tun. Anders als es die Gesetzesbegründung wohl suggerieren möchte, sind Kreditwürdigkeitsermittlung und Bonitätsauskunftserteilung auch nicht gleichzusetzen mit Scoring im Sinne der etablierten Modelle deutscher Auskunfteien. Scorewerte der Auskunfteien waren bei ihrer Etablierung im deutschen Markt im Wesentlichen lediglich als Ergänzung der aus Einzelbonitätsinformationen bestehende Bonitätsauskunft durch eine zusätzliche gruppenstatistische Wahrscheinlichkeitsaussage zwecks Standardisierung und Beschleunigung der Entscheidung bei scorewertabrufenden Unternehmen gedacht. Kreditwürdigkeitsermittlung und Bonitätsauskunft hängen also mitnichten von einer Aufrechterhaltung der erst 2010 eingeführten Scoringregelung des BDSG ab. Verbraucherüberschuldungsschutz ist und bleibt eine staatliche Aufgabe, der nicht mit Scoringregelungen für private Unternehmen Rechnung getragen werden kann. Schließlich kann die bisherige Regelung des Scoringverfahrens, welches neben seiner massiven Fehleranfälligkeit, seiner fragwürdigen Prognosegüte, seiner weitgehenden Unkontrollierbarkeit vor allem Diskriminierungspotenzial für ganze Wohngebietsbevölkerungen aufweist, aufgrund dieser gesamtgesellschaftlich unerwünschten möglichen Konsequenzen kaum als dem öffentlichen Interesse dienlich bezeichnet werden. § 31 Absatz 1 BDSG-neu dient also wie erwähnt im Wesentlichen dem Interesse der Wirtschaftsauskunfteien an der Aufrechterhaltung ihrer Scoringsysteme und der Verwertbarkeit des Scoringprodukts durch abrufende Unternehmen.

Soweit § 31 Absatz 1 BDSG-neu unverändert – nunmehr im Vergleich mit der gestrichenen Gesetzesbegründung der ersten beiden Referentenentwürfe lediglich unausgesprochen –

auf eine behauptete Regelungskompetenz aus einer "Zusammenschau der Artikel 6 Absatz 4 und Artikel 23 Absatz 1 Buchstabe e DSGVO" gestützt werden soll, würde auch diese Begründung nicht überzeugen. Dort wo die DSGVO dem nationalen Gesetzgeber Regelungsspielräume eröffnen wollte, sind diese nämlich klar benannt.

Zur Problematik der fehlenden Befugnis zum Erlass des § 31 Absatz 1 BDSG-neu tritt die weitere Problematik hinzu, dass die Vorschrift auch inhaltlich nicht geglückt ist. Sie knüpft an die "Verwendung" eines Wahrscheinlichkeitswertes an und lässt eine Verwendung nur unter bestimmten Voraussetzungen zu. Die "Verwendung" ist nach Artikel 4 Ziffer 2 DSGVO ein definierter Teilschritt der Datenverarbeitung, der beispielsweise vom Erheben oder Bereitstellen von Daten zu unterscheiden ist. Adressaten der Vorschrift sind also ihrem Wortlaut nach diejenigen, die Scorewerte verwenden. Sprachlich können hiermit nur Stellen gemeint sein, die einen zumeist nicht selbst errechneten Scorewert im Rahmen von anstehenden Vertragsentscheidungen als Entscheidungshilfe heranziehen wollen, also beispielsweise Online-Händler. Inhaltlich regelt § 31 in Absatz 1 BDSG-neu aber Anforderungen an die Erstellung beziehungsweise die Berechnung des Scorewertes. Diese inhaltlichen Rechtspflichten sollen also den Ersteller des Scorewertes treffen. Anstatt aber unmissverständlich an die Erstellung des Wahrscheinlichkeitswertes anzuknüpfen, knüpft die Vorschrift, wie gesagt, an die Verwendung eines Wahrscheinlichkeitswertes an. Konsequenz hieraus ist, dass der Verwender nur dann einen Scorewert heranziehen dürfen soll, wenn der Ersteller des Scorewertes die inhaltlichen Vorgaben an die Erstellung beachtet hat. Die Einhaltung der inhaltlichen Vorgaben zur Erstellung des Scorewertes kann aber derjenige, der einen Scorewerte verwenden will, ganz offenkundig überhaupt nicht kontrollieren. Die Umstände und Details der Erstellung der Scorewerte bei einer Auskunftei sind dem Scorewertabnehmer nicht bekannt und können ihm nicht bekannt werden, da diese Umstände als Geschäftsgeheimnis der Auskunfteien behandelt werden.

11.4 Artikel-29-Gruppe zum Profiling (Scoring)

Die Artikel-29-Gruppe ist ein unter der Datenschutzrichtlinie (RL 95/46/EG) etabliertes Gremium aller europäischen Datenschutzbehörden und bestimmter EU-Institutionen mit Beratungsfunktion. Sie hat am 3. Oktober 2017 in einem Arbeitspapier (Working Paper, kurz: WP, Nummer 251) Leitlinien vorgelegt, mit denen die neuen Regelungen der Datenschutzgrundverordnung zum Profiling – sowie daneben zur automatisierten Entscheidungsfindung – erläutert werden sollen. Der Begriff des Profiling schließt nach seiner rechtlichen Definition in der Datenschutzgrundverordnung (Artikel 4 Ziffer 4) grundsätzlich das sogenannte Scoring, wie es deutsche Wirtschaftsauskunfteien einsetzen, ein. Die Leitlinien beziehungsweise "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" sind online abrufbar unter folgendem Link: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 .

11.5 Richtlinien des Europarats zu Big Data

Der Europarat, eine aus 47 Vertragsstaaten bestehende internationale europäische Organisation neben der Europäischen Union, zu deren bekanntestem Übereinkommen die europäische Menschenrechtskonvention zählt und deren bekanntestes Organ der Europäische Gerichtshof für Menschenrechte in Straßburg ist, legte zu Beginn des Berichtsjahres eine Richtlinie zum Schutz der Einzelnen bei der Datenverarbeitung in einer Big-Data-Welt vor ("Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data" vom 23. Januar 2017; T-PD [2017] 01). Diese Richtlinie ergänzt die aus dem Jahr 1981 stammende Konvention Nummer 108 zum Schutz der Einzelnen bei automatisierter Verarbeitung personenbezogener Daten. Sie wendet sich insbesondere auch an Datensammler wie beispielsweise Wirtschaftsauskunfteien und spricht neun Empfehlungen für die Nutzung von Big-Data-Anwendungen zur Vermeidung von negativen Auswirkungen auf die Menschenwürde, Menschenrechte und grundlegende Freiheiten aus. Dass neben einem weiteren Vertragsstaat lediglich Deutschland bei der Schlussabstimmung über die Annahme dieser Richtlinien für eine Ablehnung votierte, zeigt, dass trotz einiger gegenteiliger Lippenbekenntnisse auch in der 18. Legislaturperiode ein effektiver Schutz des informationellen Selbstbestimmungsrechts der Menschen nicht im Fokus des Regierungshandelns stand.

12. Mieterdatenschutz und Gewerbe

12.1 Mieterselbstauskünfte bei der Anbahnung von Mietverhältnissen

Die angespannte Lage auf dem Wohnungsmarkt führt auch in Bremen vermehrt zu datenschutzrechtlichen Verstößen bei der Anbahnung von Mietverhältnissen. Im vergangenen Jahr erreichten uns viele Eingaben von Wohnungssuchenden, von denen teils schon vor der Entscheidung, ob sie überhaupt eine Wohnung besichtigen dürfen, umfangreiche und damit häufig unzulässige Auskünfte über ihr Privatleben, ihre berufliche und finanzielle Situation sowie Einwilligungen in die Einholung von Auskünften bei aktuellen Vermieterinnen und Vermietern sowie Auskunfteien eingefordert wurden.

Die Eingaben richteten sich gegen verschiedene Maklerbüros und private Vermieterinnen und Vermieter. Wohnungsbaugesellschaften waren bisher nicht betroffen, was daran liegen könnte, dass wir an diese bereits im Jahr 2014, die am 27. Januar 2014 von den Aufsichtsbehörden für den nicht öffentlichen Bereich beschlossene Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten, mit der Bitte um Beachtung versandt hatten.

12.2 Kopien der Personalausweise von Bewachungspersonal

Nach der Bewachungsverordnung müssen Bewachungsunternehmer der Gewerbebehörde Wachpersonen melden, bevor sie diese erstmals zu Bewachungsaufgaben einsetzen. Im Frühjahr des Berichtsjahres erhielten wir einen Hinweis eines Bewachungsunternehmers darauf, dass die zuständigen kommunalen Gewerbeämter in Bremen und Bremerhaven bei der Meldung auch die Vorlage einer Kopie des Personalausweises der jeweiligen Wachperson anforderten. Wir wandten uns an die Gewerbebehörden und erläuterten, dass wir gegen eine solche Vorgehensweise Rechtsbedenken hätten, weil es keine Rechtsgrundlage für eine solche Anforderung gebe.

Welche Unterlagen zwecks Nachweises der Zuverlässigkeit, der Volljährigkeit und der Befähigung der Wachperson bei der Meldung durch den Bewachungsunternehmer vorzulegen sind, regelt die Bewachungsverordnung nämlich ausdrücklich. Daneben kann beziehungsweise muss die Gewerbebehörde einige zusätzliche Informationen und/oder Auskünfte über die Wachperson einholen. Personalausweiskopien gehören aber nach diesen Vorschriften nicht zu den vorzulegenden Unterlagen.

Dem Bewachungsunternehmer war es nach der bis Juli des Berichtszeitraums geltenden Rechtslage auch gar nicht möglich, ohne eigenen Rechtsverstoß Kopien der Personalausweise seiner zu beschäftigenden Wachpersonen anzufertigen und der Gewerbebehörde vorzulegen. Das damals geltende Personalausweisgesetz erlaubte eine solche Kopieanfertigung grundsätzlich nicht. Dies war dem Gesetz eindeutig zu entnehmen. Dieses Verbot war auch sachlich begründet, denn im Unterschied zur beglaubigten Kopie besitzt eine einfache Kopie im allgemeinen Rechtsverkehr keinen Beweiswert hinsichtlich der Richtigkeit ihres Inhalts, sie hat rechtlich also nicht die Qualität einer Urkunde. Dies hat nicht zuletzt seinen Grund in der leichten Fälschbarkeit einer einfachen Kopie. Auch in der Begründung des Personalausweisgesetzes war das Kopierverbot ausdrücklich benannt. Eine spezielle Erlaubnisvorschrift fand sich im Bewachungsgewerberecht nicht. Mit der Anfertigung von Kopien des Personalausweises hätte sich der Bewachungsunternehmer daher unter Umständen sogar datenschutzaufsichtsbehördlicher Maßnahmen (siehe Urteil des Verwaltungsgerichts Hannover vom 28. November 2013, Aktenzeichen 10 A 5342/11) bis hin zur Einleitung eines Ordnungswidrigkeitsverfahrens wegen unerlaubter Erhebung, Speicherung und Übermittlung personenbezogener Ausweisdaten ausgesetzt. Nach zügiger Überprüfung unserer Einwände teilten uns die Gewerbeämter erfreulicherweise mit, dass sie keine Personalausweiskopien mehr anfordern würden.

Im Sommer des Berichtsjahres, also nach Abschluss unseres Verfahrens, sorgte der Bundesgesetzgeber allerdings für eine Rechtsänderung im maßgeblichen Paragrafen des

Personalausweisgesetzes (§ 20) und hob damit das bisherige generelle Kopierverbot auf. Die Vorschrift lautet nun wie folgt:

"(2) Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder datenverarbeitende Stelle dies nur mit Einwilligung der Ausweisinhaberin beziehungsweise des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt."

Zur Begründung dieser Gesetzesänderung führte der Gesetzgeber aus, die bisherige Regelung habe sich als nicht praxisgerecht erwiesen. Hinweise, worauf diese Erkenntnis beruht, finden sich in der Gesetzesbegründung nicht.

Bemerkt hat der Gesetzgeber zudem offensichtlich nicht, dass er mit dieser allgemeinen Regelung zur Ermöglichung von Personalausweiskopien sein ausdrückliches Hauptziel der Novellierung des Personalausweisgesetzes erheblich gefährdet. Dies bestand darin, die Nutzung der elektronischen Identifizierungsfunktion (eID-Funktion) des Personalausweises zu fördern. Diese Funktionalität war ursprünglich in den Personalausweis integriert worden, um gerade einen sicheren und zuverlässigen Nachweis der Identität auch in der elektronischen Kommunikation, insbesondere im Wirtschaftsverkehr, zu ermöglichen. Dass die aufwändigere elektronische Identifizierungsfunktion stärker genutzt werden wird, wenn nun die schlichte E-Mail-Zusendung einer einfachen Ausweiskopie beispielsweise im Online-Wirtschaftssektor rechtlich zulässig ist, ist wenig wahrscheinlich. Das bereits erwähnte Grundproblem einfacher Ausweiskopien, das darin besteht, dass sie im Unterschied zu beglaubigten Ausweiskopien zu einer zuverlässigen Nachweisführung völlig ungeeignet sind, und daher im allgemeinen Rechtsverkehr überhaupt keinen urkundlichen Beweiswert haben, gleichwohl aber den trügerischen Anschein der Verlässlichkeit und des wirksamen Identitätsnachweises erzeugen, wird dabei ja tatsächlich oft übersehen. Auch der Gesetzgeber hat dies wohl bei seiner Kopieerlaubnis nicht bedacht. Wie im Übrigen die gesetzliche Vorgabe erfüllt werden soll, dass die Ablichtung "eindeutig und dauerhaft" als Ablichtung erkennbar ist, verrät der Gesetzgeber ebenfalls nicht. In der Gesetzesbegründung ist hierzu die lapidare Erläuterung zu lesen, bei der Kopie könne einfach eine Schwarz-weiß-Erstellung erfolgen oder ein Kopievermerk angebracht werden. Beides ist zwar ohne weiteres möglich, angesichts der heutigen technologischen Möglichkeiten etwa der digitalen Bildbearbeitung oder der "Herausrechnung" von Dokumentenwasserzeichen, ist dies allerdings praktisch kaum ein wirksamer Schutz gegen eine spätere Entfernung der Kopiekennzeichnung. Die gesetzliche Vorgabe kann daher nur als praxisfern und

realitätsfern bezeichnet werden. Dazu, wie das öffentliche Interesse an verlässlichen, hoheitlichen Identifizierungsdokumenten gewahrt bleiben soll, wenn bei unterschiedlichsten privaten Stellen gegebenenfalls massenhaft Kopien von Personalausweisdokumenten in analoger oder digitaler Form gesammelt werden und sichere Kopiekennungen technisch sowie mit realisierbarem Aufwand kaum möglich sind, enthält das Gesetz keine Hinweise.

12.3 Keine Datenübermittlung über Reisegewerbekarteninhaber

Die Gewerbeordnung regelt neben den beiden Gewerbe(ausübungs)formen des sogenannten stehenden Gewerbes und des sogenannten Marktgewerbes auch das Reisegewerbe. Ein typisches Beispiel für das Reisegewerbe ist die Schaustellertätigkeit auf Jahrmärkten. Aber auch Handwerksleistungen können in Form des Reisegewerbes erbracht werden. Derjenige, der ein Reisegewerbe betreiben will, bedarf – abgesehen von einigen speziell geregelten Fällen – einer vorhergehenden Erlaubnis der Gewerbebehörde. Die Erlaubnis wird durch eine – stets mitzuführende – Reisegewerbekarte dokumentiert. Im Fall des "stehenden Gewerbes" sieht die Gewerbeordnung Pflichten des Gewerbeamtes zu Übermittlungen von bestimmten personenbezogenen Daten des Gewerbetreibenden aus seiner Gewerbeanzeige an weitere Behörden und Stellen vor, unter anderem auch an die Industrie- und Handelskammern oder Handwerkskammern. Hingegen enthält die Gewerbeordnung keine Regelung, die im Zusammenhang mit der Ausstellung einer Reisegewerbekarte eine Befugnis der Gewerbeämter zur Übermittlung von Daten des Reisegewerbekarteninhabers etwa an Kammern vorsieht.

Aufgrund eines Hinweises im Online-Angebot des stadtbremischen Gewerbeamtes, der vermutlich zwecks besserer Verständlichkeit recht allgemein gefasst war und daher in seiner Reichweite missverstanden werden konnte, sowie einiger zurückliegender Vorkommnisse in anderen Bundesländern im Zusammenhang mit Reisegewerbekartenausstellungen, hegte ein Reisegewerbetreibender die Befürchtung, dass es im Rahmen der Reisegewerbekartenausstellung auch in Bremen zu einer Datenübermittlung über Reisegewerbekarteninhaber etwa an die Handelskammer Bremen komme.

Zwecks Abklärung wandten wir uns an die stadtbremische Gewerbebehörde. Nachdem wir von dort – wie schon bei einem anderen Prüfanlass (siehe hierzu 38. Jahresbericht, Ziffer 5.11) – auch nach einer Erinnerung keine Auskunft erhalten hatten, wandten wir uns an die übergeordnete senatorische Wirtschaftsbehörde. Von dort aus wurde auf die angespannte Personalsituation des Gewerbeamtes hingewiesen, uns aber zugleich ein Bemühen um Nachforschung hinsichtlich dieser Frage und baldige Auskunftserteilung zugesagt. Tatsächlich erhielten wir wenig später die Nachricht, dass man keine Anhaltspunkte habe, dass es im Rahmen von Reisegewerbekartenausstellungen zu von der Gewerbeordnung nicht legitimierten Datenflüssen an andere Behörden oder Stellen

gekommen sei. Insoweit gehen wir momentan davon aus, dass die Befürchtungen des Reisegewerbekarteninhabers unbegründet waren.

12.4 Missachtung des datenschutzrechtlichen Auskunftsanspruchs

Beschwerden darüber, dass datenverarbeitende bremische Unternehmen unter Verstoß gegen das Bundesdatenschutzgesetz keine oder nur eine unzureichende Auskunft über gespeicherte personenbezogene Daten und deren Herkunft, über den Zweck der Speicherung und eine etwaige Datenweitergabe erteilt hätten, waren auch in diesem Berichtszeitraum wieder zu verzeichnen.

Für uns neu war das folgende auskunftsvermeidende Vorgehen zweier Unternehmen aus der Branche Reisevertragsvermittlung sowie Energielieferungsvertragsvermittlung: Nachdem die Beschwerdeführer die Unternehmen um Auskunft ersucht hatten, erhielten sie jeweils die Nachricht, dass ihre Daten aufgrund ihrer Anfrage unmittelbar gelöscht worden seien, man daher nunmehr keine Auskunft mehr erteilen könne. Ob die Unternehmen tatsächlich die Daten irreversibel und vollständig gelöscht hatten, wie behauptet, hätten wir im Zuge des aufsichtsbehördlichen Kontrollverfahrens vor Ort überprüfen müssen. Aus Kapazitätsgründen konnten wir dies jedoch nicht leisten. Somit blieb uns lediglich die Möglichkeit einer Sanktionierung der Auskunftsverweigerung im Wege eines Bußgeldverfahrens. Dem ursprünglichen Anliegen der Antragsteller, Auskunft zu erhalten, war damit aber nicht Rechnung getragen. Dies ist eine auch für uns unbefriedigende Situation.

An unseren begrenzten Kontrollkapazitäten wird sich auch unter Geltung der Datenschutzgrundverordnung (DSGVO) nichts ändern. Allerdings sieht die DSGVO wesentlich höhere Bußgeldgrenzen vor. Zudem schreibt sie ausdrücklich vor, dass verhängte Bußgelder eine abschreckende Wirkung entfalten sollen. Derartige Verstöße begründen künftig also ein noch höheres Ahndungsrisiko für die datenverarbeitenden Stellen.

13. Verkehr und Umwelt

13.1 Personenbezogene Daten in automatisierten und vernetzten Fahrzeugen

Bei Fahrzeugen geht der Trend seit vielen Jahren hin zum Einsatz von immer mehr elektronischen Steuergeräten. Diese müssen häufig Daten auswerten, um funktionsfähig zu sein, und produzieren, speichern und übermitteln selbst Daten. Bei der Nutzung und Übermittlung solcher Daten muss die informationelle Selbstbestimmung gewahrt bleiben. Um dies zu erreichen, bedarf es sowohl technischer als auch rechtlicher Maßnahmen. Im

Folgenden geben wir einen Überblick über den derzeitigen Stand der Bemühungen, die technische Entwicklung im Automobilbereich in ein erforderliches (datenschutz-)rechtliches Gewand einzukleiden.

13.1.1 Änderung des Straßenverkehrsgesetzes

Der Bundestag stimmte Ende März des Berichtsjahres für eine Änderung des Straßenverkehrsgesetzes, die eine rechtliche Grundlage für die Verwendung von hochautomatisierten und vollautomatisierten Fahrfunktionen im Straßenverkehr schaffen soll und umfangreiche Datenspeicherungen und Übermittlungspflichten zur Klärung der Verantwortlichkeit bei Autounfällen regelt.

Der Gesetzentwurf war von den unabhängigen Datenschutzbehörden des Bundes und der Länder in der Entschließung "Gesetzentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!" vom 16. März 2017 (siehe hierzu Ziffer 16.4 dieses Berichts) zu Recht kritisiert worden. Auch die danach veränderte Fassung lässt datenschutzrechtlich leider viele Fragen offen. Auch wenn die Frist für die Speicherung unfallfreier Fahrten von drei Jahren auf sechs Monate verkürzt wurde, ist die Halterin beziehungsweise der Halter eines Fahrzeugs mit hochautomatisierten oder vollautomatisierten Fahrfunktionen weiterhin verpflichtet, auf Vorrat für sechs Monate im Fahrzeugspeicher die durch ein Satellitennavigationssystem ermittelten Positionsangaben und Zeitangaben aufzuzeichnen, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführerin beziehungsweise Fahrzeugführer und dem hochautomatisierten oder vollautomatisierten System erfolgt. Eine derartige Speicherung muss auch erfolgen, wenn die Fahrzeugführerin oder der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische Störung des Systems auftritt. Hierdurch kann ein Bewegungsprofil für das Fahrzeug und die in der Regel überschaubare Anzahl von Nutzerinnen und Nutzern wie bei einem elektronischen Fahrtenschreiber erstellt werden. Eine solch lange Speicherdauer ist zur Klärung der Haftung bei Unfällen nicht erforderlich, da stattdessen der Halterin beziehungsweise dem Halter auch die Pflicht zur Sicherung der Daten nach einem Unfall hätte auferlegt werden können, verbunden mit einer Beweislastverteilung, die die Nichtaufklärbarkeit der Verantwortlichkeit zu Lasten der Halterin oder des Halters beziehungsweise der Fahrzeugführerin oder des Fahrzeugführers gehen lässt. Dadurch hätte die erforderliche Speicherdauer stark reduziert werden können, ohne dass berechtigte Interessen der Halterin oder des Halters oder anderer Unfallbeteiligter beeinträchtigt worden wären. Hierfür wäre auch ohne Festlegung irgendeiner Speicherdauer oder Speicherverpflichtung eine entsprechende Beweislastverteilung zuungunsten der Halterin oder des Halters beziehungsweise der Fahrzeugführerin oder des Fahrzeugführers ausreichend gewesen. Damit genügt die getroffene Regelung nicht den Grundsätzen der Erforderlichkeit der Datenverarbeitung und der Datensparsamkeit und hindert durch die

getroffenen gesetzlichen Vorgaben die Umsetzung des in der Datenschutzgrundverordnung vorgesehenen Prinzips des Datenschutzes durch Technikgestaltung ("Data Protection by Design") in hochautomatisierten und vollautomatisierten Fahrzeugen.

Zu begrüßen ist zwar, dass in dem geänderten Gesetzentwurf zumindest eine Verordnungsermächtigung aufgenommen wurde, die viele offen gebliebene datenschutzrechtliche Details erfasst, nämlich die technische Ausgestaltung und den Ort des Speichermediums sowie die Art und Weise der Speicherung, den Adressaten der Speicherpflicht und Maßnahmen zur Sicherung der gespeicherten Daten gegen unbefugten Zugriff bei Verkauf des Kraftfahrzeugs. Leider ist offen, ob und wann von dieser Verordnungsermächtigung Gebrauch gemacht wird und ob die so geschaffenen Regelungen datenschutzkonform sein werden.

13.1.2 Datenverarbeitung beim Betrieb eines Fahrzeugs

Neben dem Zweck der Klärung der Haftungsfrage bei Unfällen, an denen hochautomatisierte oder vollautomatisierte Fahrzeuge beteiligt sind, kann eine Datenverarbeitung im Fahrzeug und gegebenenfalls die Übermittlung dieser Daten an Dritte auch zu anderen Zwecken erfolgen. Steuerungsgeräte verarbeiten Fahrzeugstatusinformationen, wie zum Beispiel Radumdrehungszahl, Geschwindigkeit, Bewegungsverzögerung, Querbeschleunigung, Anzeige geschlossener Sicherheitsgurte oder auch Umgebungszustände, wie zum Beispiel Temperatur, Regensensor oder Abstandssensor. Die Verarbeitung vieler Daten im Fahrzeug ist erforderlich, um bestimmte Funktionen zu gewährleisten. Da diese Daten personenbeziehbar sind, bedarf es aber nicht nur für ihre Erhebung sondern auch dann, wenn diese Daten längerfristig gespeichert oder gar an Dritte übermittelt werden, einer wirksamen Rechtsgrundlage.

Gegenwärtig ist vielfach unklar, welche Daten zu welchen Zwecken in Fahrzeugen gespeichert und an wen übermittelt werden. Eine von mehreren Aufsichtsbehörden der Länder durchgeführte Umfrage bei Werkstätten verdeutlichte, dass selbst den Werkstätten nicht bekannt war, welche Daten bei einer durch sie durchgeführten Inspektion aus dem Fahrzeugspeicher ausgelesen und an den jeweiligen Hersteller übermittelt werden. Gleichzeitig wächst die Begehrlichkeit Dritter, wie zum Beispiel von Versicherungen oder App-Entwicklern, Zugriff auf die durch Fahrzeugführer bei der Nutzung ihrer Fahrzeuge produzierten Daten zu erhalten. Die vom Bundesministerium für Verkehr und digitale Infrastruktur eingesetzte Ethikkommission zum automatisierten und vernetzten Fahren forderte in ihrem Bericht vom Juni 2017, die Autonomie und Datenhoheit der Verkehrsteilnehmerinnen und Verkehrsteilnehmer sicherzustellen. In diesem Zusammenhang finden bereits seit mehreren Jahren Gespräche zwischen dem Verband der Automobilindustrie und den unabhängigen Datenschutzaufsichtsbehörden der Länder und

des Bundes statt. Hierbei entstand am 26. Januar 2016 eine gemeinsame Erklärung, die die datenschutzrechtlichen Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge klarzustellen versuchte. Auf dieser Basis wird derzeit an einem Mustertext zur Datenverarbeitung im Fahrzeug gearbeitet, die Fahrzeugkäuferinnen und Fahrzeugkäufer über die in ihren Fahrzeugen verarbeiteten Daten und ihre diesbezüglichen Rechte in verständlicher Form aufklären soll. Da auch Hersteller an diesen Gesprächsrunden teilnehmen, steht zu hoffen, dass die informationelle Selbstbestimmung der Fahrerinnen und Fahrer im Sinne der von der Datenschutzgrundverordnung als unhintergehbares Grundprinzip angesehenen Privacy by Design schon bei der Produktion von Fahrzeugen beachtet wird.

13.1.3 Kooperative intelligente Verkehrssysteme

Zur Entwicklung kooperativer intelligenter Verkehrssysteme werden derzeit Datenübermittlungsstandards entwickelt, mit deren Hilfe jedes Fahrzeug an andere Verkehrsteilnehmerinnen oder Verkehrsteilnehmer, an einen uneingeschränkten Empfängerkreis oder an Infrastruktureinrichtungen Mitteilungen verschicken kann. Solche Mitteilungen können in kurzen, regelmäßigen Abständen erfolgen (sogenannte Cooperative Awareness Messages – CAMs) oder nur ausgelöst durch bestimmte Ereignisse (sogenannte Decentralized Environmental Notification Messages – DENMs). Auf diese Weise sollen die Verkehrssicherheit erhöht und die Unfallgefahr reduziert werden. Auch können so verkehrslenkende Maßnahmen ergriffen werden, die für einen besseren Verkehrsfluss und damit auch für eine umweltfreundlichere Verkehrsausübung sorgen können. Diese Mitteilungen können unter anderem vor Verkehrshindernissen warnen, Geisterfahrer melden, auf Bremslichter voranfahrender Fahrzeuge automatisch reagieren und abbremsen oder auf Einsatzfahrzeuge der Feuerwehr oder Polizei aufmerksam machen. Auch könnten Lastkraftwagen zu Konvois zusammengekoppelt werden.

Aufgabe der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es in diesem Zusammenhang, darauf aufmerksam zu machen, dass schon bei der Entwicklung entsprechender Programme sichergestellt werden muss, dass diese Mitteilungen nicht abgefangen und zur Erstellung von Bewegungsprofilen zweckentfremdet werden können. Eine erste Untersuchung, ob die bisher zum Einsatz kooperativer intelligenter Verkehrssysteme entwickelten Standards den datenschutzrechtlichen Anforderungen genügen, wurde im Juli des Berichtsjahres durch die Artikel-29-Gruppe mit einem 51-seitigen Gutachten mit dem Titel "Processing personal data in the context of C-IST" abgeschlossen. Hierin wird deutlich, dass insbesondere die in kurzen Abständen verschickten Mitteilungen (CAMs), die auch Angaben zu Position, Geschwindigkeit, Fahrtrichtung, Länge und Breite eines Fahrzeugs enthalten, problematisch bleiben. Diese Mitteilungen werden zwar mit pseudonymen Schlüsselzertifikaten signiert, bei denen der Signaturschlüssel in

regelmäßigen Abständen gewechselt wird. Aufgrund der oben genannten dynamischen und statischen Informationen kann das betreffende Fahrzeug aber auch nach einem Signaturschlüsselwechsel wieder eindeutig identifiziert und damit dessen Route verfolgt werden. Diese datenschutzrechtliche Problematik ist weiterhin ungelöst. Um bereits im Rahmen der Entwicklung sicherzustellen, dass datenschutzrechtliche Vorgaben mitbedacht werden, um Kosten für eine Nachbesserung zu vermeiden und Risiken für die informationelle Selbstbestimmung bei diesem wichtigen Zukunftsthema zu reduzieren, bieten wir für diesbezügliche Vorhaben in Bremen an, frühzeitig vor der Einrichtung von Teststrecken, der Umsetzung von Logistikkonzepten oder bei Forschungsvorhaben zur Weiterentwicklung technischer Konzepte beim automatisierten oder autonomen Fahren aus datenschutzrechtlicher Sicht zu beraten.

13.2 Feuerstättenbeschau in Kleingärten

Ein Vorstandsmitglied eines Kleingartenvereins wandte sich an uns mit der Frage, ob der Kleingartenverein berechtigt oder sogar verpflichtet sei, Namen und Anschriften der Pächterinnen und Pächter an den Bezirksschornsteinfeger weiterzugeben, wenn die Pächterinnen und Pächter auf ihrer Parzelle einen Ofen betreiben. Der Verein hatte bereits mit einem Rundschreiben alle Pächterinnen und Pächter darüber informiert, dass sie verpflichtet seien, einmal jährlich den Ofen durch den Schornsteinfeger reinigen zu lassen und dass alle vier Jahre eine Feuerstättenbeschau durchzuführen sei. Der Kleingartenverein vermutete nämlich, dass vielen Pächterinnen und Pächtern diese Pflicht nicht bekannt sei. Da der Kleingartenverein davon ausging, dass immer noch nicht alle Pächterinnen beziehungsweise Pächter ihrer Verpflichtung freiwillig nachgekommen waren, stellte sich ihm die Frage, ob er zu weiteren Maßnahmen gegenüber den Behörden verpflichtet sei und ob eine Übermittlung der Namen und Anschriften der Pächterinnen und Pächter zu diesem Zweck "unbefugt" sei und damit gegen die Vereinssatzung verstoßen würde. Bei der Klärung dieser Frage wurde uns deutlich, dass die Gewährleistung des Brandschutzes in Kleingärten aufgrund der hier vorherrschenden Pachtverhältnisse schwierig ist:

Grundsätzlich trifft die Eigentümerin oder den Eigentümer eines Grundstücks oder Raums nach dem Schornsteinfeger-Handwerksgesetz die Verpflichtung, fristgerecht entsprechende Reinigungen, Überprüfungen und Schornsteinfegerarbeiten zu veranlassen. Da die Vereinsmitglieder regelmäßig nicht Eigentümerinnen und Eigentümer der Kleingärten sind, sondern diese nur gepachtet haben, trifft sie diese Pflicht nicht direkt. Auch sofern der Verein nicht selbst Eigentümer der Parzellen sein sollte, kann er aber zur Übermittlung der Daten der Parzellenpächterinnen und Parzellenpächter berechtigt sein, wenn er von der Eigentümerin oder dem Eigentümer hierum gebeten wurde. Die Tätigkeit des Schornsteinfegers dient der Abwehr der Brandgefahr als einer Gefahr für die öffentliche Sicherheit. Daher kann der Kleingartenverein sich hier auf das Bundesdatenschutzgesetz

stützen, wenn er auf Ersuchen der Eigentümerin oder des Eigentümers die Übermittlung der notwendigen Daten der Parzellenpächterinnen und Parzellenpächter vornimmt. Eine solche Übermittlung kann nicht wirksam durch die Satzung des Vereins ausgeschlossen werden.

Sofern der Verein bisher nicht von der Eigentümerin oder dem Eigentümer zur Übermittlung der Daten seiner Pächterinnen und Pächter aufgefordert wurde, und sich sorgt, dass wegen nicht vorgenommener Schornsteinfegerarbeiten Brandgefahr im Kleingartengebiet besteht, kann er zumindest in allgemeiner Form an die Eigentümerinnen und Eigentümer herantreten und diese darauf aufmerksam machen, dass die Feuerstättenbeschau im Kleingartengebiet nicht vollständig beziehungsweise ordnungsgemäß durchgeführt wird. Dann obliegt es den Eigentümerinnen und Eigentümern, hier Abhilfe zu schaffen. Im Rahmen dieses Hinweises dürfen aber noch nicht die Daten der Pächterinnen und Pächter übermittelt werden. Sofern die Eigentümerin oder der Eigentümer sich weigert den Pflichten nachzukommen, verbleibt noch die Möglichkeit einer Meldung an die zuständige Behörde. Hier schlugen wir vor, am besten zunächst den Bezirksschornsteinfeger anzusprechen. Um zukünftig eine Übermittlung transparent zu machen, empfahlen wir, bei Abschluss von Pachtverträgen festzulegen, dass die Daten der Pächterinnen und Pächter zur Gewährleistung der Feuerstättenbeschau und der Kehrpflicht an die Eigentümerin oder den Eigentümer übermittelt werden dürfen.

14. Internationales und Europa

14.1 Verarbeitung von Fluggastdaten

Am 6. Juni 2017 beschloss der Bundestag das Gesetz zur Umsetzung der Richtlinie (EU) 681/2016 über die Verwendung von Fluggastdatensätzen (Passenger Name Records – PNR) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Dieses sogenannte Fluggastdatengesetz (FlugDaG) regelt die Übermittlungspflicht für 20 verschiedene Kategorien von Fluggastdaten durch Luftfahrtunternehmen an das Bundeskriminalamt. Danach muss die Übermittlung 24 bis 48 Stunden vor dem Flug erfolgen und ist zu dem Zeitpunkt zu wiederholen, an dem sich alle Fluggäste an Bord eines von einem deutschen Flughafen abfliegenden Flugzeugs befinden und dies nicht mehr verlassen können. Andere Unternehmen, die an der Buchung von Flügen beteiligt sind, müssen Fluggastdaten an die Luftfahrtunternehmen so rechtzeitig übermitteln, dass diese ihren eigenen Übermittlungspflichten rechtzeitig nachkommen können. Insoweit geht das Fluggastdatengesetz über die Vorgaben der Richtlinie hinaus. Das Fluggastdatengesetz verpflichtet zudem auch zur Übermittlung der Fluggastdaten bei innereuropäischen Flügen und nicht nur bei Flügen von Drittstaaten in die Europäische Union (EU) und umgekehrt. Diese Erweiterung des Anwendungsbereichs ergibt sich ebenfalls nicht aus der EU-Richtlinie selbst, sondern geht auf einen EU-Ratsbeschluss vom

18. April 2016 zurück. Das Bundeskriminalamt pflegt diese Daten in ein Fluggastdaten-Informationssystem ein, das der Verhütung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität dienen soll. Vor der Ankunft eines Luftfahrzeugs auf einem deutschen Flughafen oder vor dem Abflug eines Luftfahrzeugs von einem deutschen Flughafen führt das Bundeskriminalamt einen automatischen Abgleich mit Mustern und Datenbeständen durch, die der Fahndung oder Ausschreibung von Personen oder Sachen dienen. Hierdurch sollen Personen identifiziert werden, die entweder bereits bestimmte Straftaten begangen haben oder von denen aufgrund der Übereinstimmung mit einem Muster die Begehung bestimmter Straftaten in nächster Zeit erwartet wird.

In seiner Stellungnahme vom 31. März 2017 setzte sich das Plenum des Bundesrats über die Empfehlung des federführenden Ausschusses für Innere Angelegenheiten und des Rechtsausschusses vom 20. März 2017 hinweg, in der diese die Berücksichtigung der anstehenden Entscheidung des Europäischen Gerichtshofs (EuGH) zum Abkommen zwischen Kanada und der EU zur Übermittlung von Fluggastdatensätzen bei den Beratungen im Bundestag empfohlen hatten. Die übereilte Umsetzung der EU-Richtlinie wird es erforderlich machen, das Fluggastdatengesetz, welches in Teilen noch nicht einmal in Kraft getreten ist, grundrechtekonform abzuändern. Denn der EuGH hat in seinem Gutachten vom 26. Juli 2017 (Aktenzeichen 1/15) Grundsätze aufgestellt, die mit verschiedenen Regelungen in dem Fluggastdatengesetz und auch der ihm zugrunde liegenden EU-Richtlinie nicht vereinbar sind. So dürfte ein Teil der Bedenken zur hinreichenden Bestimmtheit auch hinsichtlich einzelner in § 2 Absatz 2 FlugDaG und im Anhang I der Richtlinie (EU) 681/2016 genannten Fluggastdaten gelten, so zum Beispiel bezüglich der allgemeinen Hinweise (Nummer 16), der erweiterten Fluggastdaten (Nummer 8), der Angaben zum Vielflieger-Eintrag (Nummer 12) und zum Reisebüro und deren Sachbearbeitern (Nummer 13), sowie der Daten zum gesamten Reiseverlauf (Nummer 11). Nicht hinreichend bestimmt dürften auch die eine Datenverarbeitung rechtfertigenden Straftatbestände für schwere Kriminalität sein. Hier verweist § 4 Absatz 1 Nummer 6 FlugDaG lediglich auf den Katalog an strafbaren Handlungen im Anhang II der Richtlinie (EU) 681/2016, die mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht sind. Dieser Katalog lässt aber die hiervon erfassten nationalen Straftatbestände nicht immer zweifelsfrei erkennen. So bleibt zum Beispiel unklar, was alles unter "Cyberkriminalität", "Umweltkriminalität" oder "Korruption" zu fassen ist. Da im Fluggastdatengesetz und der diesem Gesetz zugrunde liegenden EU-Richtlinie für die Verarbeitung sensibler Daten strengere Regelungen gelten als in dem Fluggastdatenabkommen zwischen der EU und Kanada sind die Ausführungen des EuGH hierzu nicht übertragbar. Allerdings setzt das deutsche Fluggastdatengesetz die EU-Richtlinie hier nur unzureichend um, da das deutsche Fluggastdatengesetz nicht – wie in der EU-Richtlinie vorgesehen – bereits die Übermittlung sensibler Daten durch die

Luftfahrtunternehmen verbietet, sondern nur eine Löschungspflicht für bereits übermittelte sensible Daten vorsieht. Selbst wenn mit dem EuGH davon ausgegangen würde, dass die Verarbeitung von Fluggastdaten zur Grenzkontrolle zulässig ist, bleibt fraglich, ob dies auch für innereuropäische Flüge innerhalb des Schengen-Raums gilt. In jedem Fall sehen das Fluggastdatengesetz und die EU-Richtlinie hierzu genauso wie das Fluggastdatenabkommen zwischen der EU und Kanada für die Fluggastdaten eine überlange Speicherfrist von fünf Jahren vor. Erforderlich ist nach Ansicht des EuGH nur eine Verarbeitung zu Zwecken der Grenzkontrolle und Sicherheitskontrolle bei Ausreise und Einreise. Während des Aufenthalts im Inland dürfen die PNR-Daten dagegen – außer in hinreichend begründeten Eilfällen – nur nach vorheriger Kontrolle durch ein Gericht verwendet werden. Ein Abgleich nach Mustern dürfe dann nicht erfolgen. Nach Ausreise seien alle Fluggastdaten unverzüglich zu löschen, sofern nicht in konkreten Fällen objektive Anhaltspunkte dafür gegeben seien, dass von bestimmten Fluggästen auch nach ihrer Ausreise eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und schwerer Kriminalität im Inland ausgehen könnte. Auch die Regelung im Fluggastdatengesetz zur Übermittlung der PNR-Daten an Drittstaaten genügt nicht den Anforderungen des EuGH, der eine solche Übermittlung nur dann für zulässig erklärt, wenn in dem Drittstaat ein gleichwertiges Schutzniveau der Grundfreiheiten und Grundrechte gewährleistet ist. Zudem dürfte es unzulässig sein, dass andere Behörden nach dem Fluggastdatengesetz PNR-Daten auch zur Verfolgung von anderen Straftaten als dem Terrorismus und schwerer Kriminalität verwenden dürfen. Auch fehlt im Fluggastdatengesetz eine Regelung, die das erforderliche Recht auf individuelle Information der Fluggäste im Falle der Verarbeitung der sie betreffenden PNR-Daten während ihres Aufenthalts im Inland oder nach ihrer Ausreise oder bei Weitergabe der PNR-Daten an andere Behörden gewährleistet.

Entgegen der am 18. Oktober 2017 geäußerten vorläufigen Auffassung der Europäischen Kommission besteht daher aufgrund des Gutachtens des EuGH sehr wohl ein rechtliches Erfordernis, die EU-Fluggastdaten-Richtlinie und damit auch das deutsche Umsetzungsgesetz zu überarbeiten, damit diese zukünftig zumindest grundrechtskonform sind. Insofern wäre eine entsprechende, von Bremen unterstützte Stellungnahme des Bundesrats wichtig, die die in der Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9. November 2017 "Keine anlasslose Vorratsspeicherung von Reisedaten" (siehe hierzu Ziffer 16.8 dieses Berichts) formulierten Argumente aufgreifen könnte.

14.2 Koordinierte Prüfung des internationalen Datenverkehrs

Nachdem wir im Frühjahr 2016 bereits verschiedene Bremer Unternehmen im Rahmen des "Safe Harbor – Auskunftsersuchens" angeschrieben hatten (siehe hierzu 39. Jahresbericht,

Ziffer 16.1), fand Ende des Jahres 2016 eine deutschlandweite, koordinierte Prüfung des internationalen Datenverkehrs statt, welche im Frühjahr 2017 ausgewertet wurde. Ziel war es einerseits, den jeweiligen verantwortlichen Stellen einen Anlass zu geben, in eigener Zuständigkeit zu prüfen, ob und in welchem Umfang personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter oder der Kundinnen und Kunden in ein Drittland übermittelt werden. Andererseits konnten wir erkennen, inwiefern datenschutzrechtliche Voraussetzungen für die Übermittlung personenbezogener Daten in Drittländer beachtet werden. Deutschlandweit wurden von den verschiedenen Datenschutzaufsichtsbehörden insgesamt 500 Unternehmen angeschrieben.

In Bremen schrieben wir 16 zufällig ausgewählte Unternehmen an und baten sie um Auskunft. In dem dreiseitigen Fragebogen behandelten die ersten beiden Abschnitte Fragen des Datentransfers in die Vereinigten Staaten von Amerika (USA) und in sonstige Drittstaaten, während sich der dritte Abschnitt auf die konkreten Arten von Übermittlungen (wie beispielsweise Datenübermittlungen im Rahmen der Fernwartung oder des Supports sowie durch die Nutzung von Cloud-Computing-Diensten) bezog. Der vierte und letzte Abschnitt behandelte die Rolle der oder des betrieblichen Datenschutzbeauftragten. Unter den von uns angeschriebenen Unternehmen waren nicht nur große international tätige Konzerne, sondern auch kleine und mittlere Unternehmen, da diese erfahrungsgemäß besonders häufig auf Leistungen von Cloud-Computing-Anbietern (zum Beispiel in Form von "Software as a Service") zurückgreifen. Die Erfahrungen aus den Beratungen insbesondere im Nachgang des "Safe Harbor – Auskunftsersuchens" zeigen, dass sich manche verantwortliche Stellen nicht bewusst sind, dass sie personenbezogene Daten in Drittländer wie beispielsweise die USA übermitteln. Die Verabschiedung des EU-U.S. Privacy Shield (siehe hierzu Ziffer 14.3 dieses Berichts) erschien deshalb als sinnvoller Zeitpunkt für eine bundesweit einheitliche Prüfung des internationalen Datenverkehrs.

Die Auswertung ergab, dass lediglich sieben der angeschriebenen Bremer Unternehmen Daten in die USA übermittelten. Bei vier dieser Unternehmen fand zusätzlich noch eine Übermittlung in weitere Drittländer statt. Jedes der Unternehmen konnte eine gültige Rechtsgrundlage für die Datenübermittlung vorweisen, wobei der sogenannte Standardvertrag als häufigstes Instrument genannt wurde (gefolgt vom EU-U.S. Privacy Shield und der Einwilligung nach § 4 c Absatz 1 Bundesdatenschutzgesetz). Der häufigste Grund für die Datenübermittlung war die Nutzung von Cloud-Office-Diensten und Cloud-Speicher-Diensten. Trotz des guten Abschneidens der befragten Unternehmen behalten wir uns vor, auch weiterhin stichprobenartig den Umgang mit personenbezogenen Daten, insbesondere im Hinblick auf den internationalen Datentransfer, zu überprüfen.

14.3 EU-U.S. Privacy Shield

Der Datenschutzschild, welcher von der Europäischen Union und den Vereinigten Staaten von Amerika (EU-U.S. Privacy Shield) am 12. Juli 2016 verabschiedet worden ist, steht auch nach einer ersten Überprüfung durch die Europäische Kommission (EU-Kommission) Mitte September 2017 in der Kritik. So kommt die EU-Kommission zwar zu dem Schluss, dass der EU-U.S. Privacy Shield ordnungsgemäß funktioniere, grundlegende Kritikpunkte konnten aber dennoch nicht ausgeräumt werden. Eines der Hauptargumente, welches das Vorgängerabkommen Safe Harbor vor dem Europäischen Gerichtshof (EuGH) zu Fall brachte, waren die Erkenntnisse des Europäischen Parlaments über den anlasslosen und massenhaften Zugriff auf personenbezogene Daten durch amerikanische Geheimdienste. Ein solcher Zugriff ist nach wie vor nicht ausgeschlossen. Im Gegenteil deuten Äußerungen des aktuellen US-amerikanischen Präsidenten wie beispielsweise im Dekret vom 25. Januar 2017[2], welches die Datenschutzgarantien gegenüber nicht-amerikanischen Personen infrage stellt, darauf hin, dass die Lage unverändert ist. Die Tatsache, dass es auf amerikanischer Seite nach wie vor keine entsprechenden Gesetze oder ein völkerrechtliches Abkommen sondern lediglich schriftliche Zusagen der amerikanischen Regierung gibt, entkräftet diese Zweifel nicht. Ein weiterer Kritikpunkt ist die Ansiedlung der vom EuGH geforderten, aber nach wie vor nur kommissarisch eingesetzten Ombudsperson für die Rechte der Bürgerinnen und Bürger der Europäischen Union bei dem amerikanischen Außenministerium, wodurch die Unabhängigkeit dieser Person faktisch ausgeschlossen wird.

Inzwischen haben sich mehr als 2.500 Unternehmen zertifizieren lassen. Eine vom amerikanischen Handelsministerium erstellte Liste der zertifizierten Unternehmen kann online abgerufen werden.[3] Informationen sowie einheitliche Beschwerdeformulare zu dem EU-U.S. Privacy Shield haben wir auf unserer Homepage[4] veröffentlicht.

Es kann nicht ausgeschlossen werden, dass das EU-U.S. Privacy Shield das gleiche Schicksal erwartet, das im Jahr 2015 das Safe-Harbor-Abkommen ereilte. Sollte der EuGH auch dieses Instrument zur Übertragung von personenbezogenen Daten in die USA für ungültig erklären, darf ein Datentransfer in die USA auch auf dieser Grundlage nicht mehr stattfinden. Es ist deshalb ratsam, schon zum gegenwärtigen Zeitpunkt über andere Möglichkeiten des Datentransfers in die USA nachzudenken und technische Vorkehrungen zu treffen, die den Datenschutz nach europäischem Standard gewährleisten.

[2] https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united
[3] https://www.privacyshield.gov/list
[4] https://www.datenschutz.bremen.de/datenschutztipps/eu_u_s__privacy_shield-13632

14.4 e-Privacy-Verordnung

Nach den ursprünglichen Planungen der Kommission sollte gleichzeitig mit der Datenschutzgrundverordnung eine "e-Privacy-Reform" in Geltung gelangen. Begonnen hatte die Diskussion über eine Reform mit einem Vorschlag der Europäischen Kommission für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation – sogenannte e-Privacy-Verordnung) vom 10. Januar 2017. Die unmittelbar in allen Mitgliedstaaten geltende e-Privacy-Verordnung würde damit die bislang geltende sogenannte e-Privacy-Richtlinie (Richtlinie 2002/58/EG), ergänzt durch die sogenannte Cookie-Richtlinie (Richtlinie 2009/136/EG), ablösen. Eine Umsetzung in nationale Vorschriften wäre nicht erforderlich. Dementsprechend würden die Regelungen im Telemediengesetz (TMG) zum Datenschutz entfallen beziehungsweise mangels Vereinbarkeit mit EU-Recht nicht mehr anwendbar sein.

Mit der Mehrheit der Stimmen beschloss das EU-Parlament am 26. Oktober 2017 seine Position zur e-Privacy-Reform. Es hielt sich an die Empfehlung des Innenausschusses, die Verarbeitung von elektronischen Kommunikationsdaten streng zu reglementieren und das Recht der Nutzerinnen und Nutzer auf verschlüsselte Kommunikation und damit das Recht auf informationelle Selbstbestimmung zu stärken. Zum Redaktionsschluss befindet sich die Verordnung noch in der Entwurfsfassung und die Beratung beziehungsweise Trilog-Verhandlungen zwischen dem Europäischen Rat, der Europäischen Kommission und dem Europäischen Parlament stehen noch aus.

Mit der e-Privacy-Verordnung beabsichtigt der EU-Gesetzgeber, die Datenschutzgrundverordnung (DSGVO) im Bereich der elektronischen Kommunikation zu präzisieren und zu ergänzen. Die e-Privacy-Verordnung soll sich vor allem an Anbieter elektronischer Kommunikationsdienste, öffentlich verfügbarer Auskunftsdienste sowie an Softwareanbieter richten, die elektronische Kommunikation ermöglichen. Wie in der DSGVO ist auch in der Entwurfsfassung der e-Privacy-Verordnung das sogenannte Marktortprinzip verankert. Die e-Privacy-Verordnung würde somit auch für diejenigen Anbieter gelten, die sich mit ihren Angeboten an Nutzerinnen und Nutzer in der Europäischen Union (EU) richten. Würden also personenbezogene Daten beziehungsweise elektronische Kommunikationsdaten von Bürgerinnen und Bürgern der EU außerhalb der EU verarbeitet und hätte die verantwortliche Stelle ihren Sitz ebenfalls außerhalb der EU, so wären die Regelungen der e-Privacy-Verordnung gleichwohl anwendbar.

Die wesentlichen Regelungsinhalte der Entwurfsfassung betreffen insbesondere sogenannte Over-The-Top-Dienste (OTT-Dienste) wie Skype, Viber, Facetime oder WhatsApp, vernetzte Geräte und Maschinen (Machine-to-Machine-Kommunikation), Cookies, Offline-Tracking und

die Einwilligung in die Verwendung von E-Mail-Adressen zu Werbezwecken. Ziel soll es sein, ein einheitliches Schutzniveau für die Rechte und Freiheiten der europäischen Bürgerinnen und Bürger bei der Nutzung elektronischer Kommunikationsdienste sowie einen ungehinderten Datenverkehr zu erreichen. Dabei geht es nicht nur um den Schutz personenbezogener Daten, sondern auch um die Vertraulichkeit der Kommunikation. Grundsätzlich soll die Verarbeitung der elektronischen Kommunikationsdaten nur noch mit der Einwilligung der Nutzerinnen und Nutzer möglich sein. Zu den elektronischen Kommunikationsdaten zählen insbesondere nicht nur die Inhaltsdaten, sondern auch die Metadaten. Die Metadaten geben unter anderem Informationen über den Zeitpunkt und die Dauer der Kommunikation, den Standort sowie die Empfängerinnen und Empfänger der Nachricht. Werbeindustrie und Datenindustrie, die an der Verarbeitung und Analyse dieser Metadaten interessiert sind, um zum Beispiel personalisierte Werbung zu erstellen, lehnen den Verordnungsentwurf deshalb ab.

Weitere erhebliche Änderungen sind für den Einsatz von Cookies oder sonstigen Tracking-Methoden zu erwarten. Die Entwurfsfassung sieht für diesen Bereich das Verbot mit Erlaubnisvorbehalt vor. Demnach soll die Nutzung der Daten von Endgeräten nur erlaubt sein, wenn die Nutzerin oder der Nutzer eingewilligt hat. Überdies sollen die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen im Sinne des Artikels 25 DSGVO auch für den Einsatz von Cookies gelten. Das bedeutet konkret, dass die Do-Not-Track-Einstellungen von Browsern und Smartphone-Betriebssystemen ab Werk aktiviert sein müssen. Webbrowser übernehmen insofern die Rolle eines "Torwächters" und verhindern von Vornherein ein Speichern von Informationen in Endgeräten beziehungsweise den Zugriff darauf. Aus unserer Sicht müssten die Möglichkeiten der Einwilligungserteilung noch deutlich weiter gehen. Nutzerinnen und Nutzer sollten nicht nur eine pauschale und unspezifische Einwilligung über die Browsereinstellung erteilen können. Vielmehr sollte ein differenziertes Einwilligungsmanagement möglich sein, damit Nutzerinnen und Nutzer etwa entscheiden können, Cookies einer bestimmten Webseite zu akzeptieren, gleichzeitig jedoch die Cookies von Drittanbietern zu blockieren. Diese vorgeschlagene sogenannte "Cookie-Regelung" ist derzeit noch höchst umstritten. Während das Europäisches Parlament, der Europäische Datenschutzbeauftragte, Datenschutzaufsichtsbehörden und die Artikel-29-Gruppe für eine strengere Regelung und Umsetzung dieser Regelung plädieren, fordern Lobbyisten der Werbeindustrie und Datenindustrie und Verlage sowie teilweise auch der Europäische Rat eine Lockerung dieser Regelung.

Eine weitere wichtige Regelung der Entwurfsfassung ist das Verbot von Offline-Tracking, also das Verbot, Bewegungsprofile etwa durch Verfolgung der Bluetooth-Signale eines Smartphones zu erstellen. Diese soll nur erlaubt sein, sofern Nutzerinnen und Nutzer eingewilligt haben. Außerdem regelt die Entwurfsfassung die unerbetene Kommunikation.

Direktwerbung soll mittels elektronischer Kommunikationsdienste, insbesondere per E-Mail, grundsätzlich nur noch mit der Einwilligung der Nutzerinnen und Nutzer möglich sein. Eine Ausnahme erlaubt Direktwerbung nur bei bestehender Kundenbeziehung. Auf die Möglichkeit des Widerspruchs muss nach der geplanten Regelung klar und deutlich hingewiesen werden. Auch soll nach der Entwurfsfassung das Recht auf Verschlüsselung gestärkt werden. Danach müssen Anbieter von Kommunikationsdiensten sicherstellen, dass die verschlüsselte Kommunikation ihrer Nutzerinnen und Nutzer vor unbefugtem Zugriff geschützt wird. Nur die Nutzerinnen und Nutzer selbst sollen die Möglichkeit haben, die Inhalte zu entschlüsseln. Diese Regelung stellt einen eindeutigen Appell an die EU-Mitgliedstaaten dar, keine Gesetze zu erlassen, mit denen sie Anbieter von Kommunikationsdiensten zwingen können, die Vertraulichkeit und Integrität der Kommunikation ihrer Nutzerinnen und Nutzer zu schwächen.

Aus Sicht des informationellen Selbstbestimmungsrechts der Menschen in Europa ist die aktuelle Entwurfsfassung, die auch die Änderungen des EU-Parlaments einschließt, grundsätzlich zu begrüßen. Regelungsbedarf besteht vor allem noch für ein differenziertes Einwilligungsmanagement sowie für einzelne technische Anforderungen für die Umsetzung der Regelungen.

15. Beschwerden und Bußgelder

15.1 Beschwerden

Die Zahl der Beschwerden, die wir erhielten, erhöhte sich im Berichtsjahr im Vergleich zum Vorjahr erneut. Sie betrug insgesamt 281. Von diesen Beschwerden bezogen sich 252 auf die Einhaltung der datenschutzrechtlichen Anforderungen und 29 auf die Umsetzung der Bestimmungen des Bremer Informationsfreiheitsgesetzes durch die hierzu verpflichteten Stellen.

Im Bereich des Datenschutzes bezog sich fast die Hälfte der Beschwerden auf den Beschäftigtendatenschutz (53 Fälle), die Videoüberwachung (23 Fälle), die Telemedien (23 Fälle) und die Werbung (21 Fälle). Insbesondere in den Bereichen des Beschäftigtendatenschutzes und der Videoüberwachung war damit wie schon in den Vorjahren ein starker Anstieg der Zahl der Beschwerden festzustellen.

Einen deutlichen Zuwachs verzeichneten wir darüber hinaus auch bei den telefonischen Anfragen zu Datenschutz und Informationsfreiheit. Hier betrug die Zahl im Berichtsjahr 209. Bei diesen Anfragen handelt es sich zumeist um Anrufe von Bürgerinnen und Bürgern, die rechtliche oder technische Fragestellungen und Probleme betreffen und kurzfristig bereits am Telefon gelöst werden können.

15.2 Ordnungswidrigkeitsverfahren

Ein Unternehmen, das als Vermittler von Energieversorgungsverträgen tätig ist, gibt bereits seit mehreren Jahren wegen immer wiederkehrender Verstöße gegen das Bundesdatenschutzgesetz Anlass für datenschutzaufsichtsrechtliches wie ordnungswidrigkeitsrechtliches Einschreiten. Dabei handelte es sich bisher stets um Verstöße, die allein schon durch eine ordnungsgemäße Organisation der Geschäftsabläufe unschwer zu vermeiden gewesen wären. Nachdem wir gerade Ende des vergangenen Berichtszeitraums gegen das Unternehmen ein Bußgeld wegen Nichterteilung einer unsererseits geforderten Auskunft verhängt hatten, wurden wir in diesem Berichtszeitraum weiterer Rechtsverstöße gewahr, die einer Ahndung durch Bußgeld bedurften. So verhängten wir ein weiteres Bußgeld wegen Nichtbestellung einer beziehungsweise eines betrieblichen Datenschutzbeauftragten. Da das Unternehmen sodann in einem weiteren Fall neuerlich einem Betroffenen keine Datenauskunft erteilte und auch unser aufsichtsbehördliches Auskunftsersuchen neuerlich ignorierte, leiteten wir ein weiteres Bußgeldverfahren ein. Nun liegt uns bereits eine weitere Beschwerde eines Bürgers wegen Nichterfüllung seines Datenauskunftsanspruchs vor.

Wegen Nichterteilung einer Datenauskunft gegenüber einem Betroffenen, wahrheitswidriger Auskünfte uns gegenüber und schließlich Nichtbeachtung der Hinweispflicht auf das Werbewiderspruchsrecht leiteten wir im Berichtszeitraum ein Bußgeldverfahren gegen ein kleines Reisevermittlungsunternehmen ein. Obwohl die Beweislage eindeutig war, legte das Unternehmen gegen unseren Bußgeldbescheid Einspruch ein, ohne jedoch inhaltliche Einwände gegen unsere Tatvorwürfe zu erheben. Es steht zu vermuten, dass die Einspruchseinlegung lediglich in der Hoffnung erfolgte, bei der mündlichen Verhandlung vor Gericht die Bußgeldhöhe reduzieren zu können. Der weitere Verlauf des Bußgeldverfahrens bleibt abzuwarten.

Auch bei einem weiteren Ordnungswidrigkeitsverfahren, das wir ebenfalls wegen einer Verletzung des Datenauskunftsanspruchs einleiteten, steht derzeit eine gerichtliche Entscheidung über unseren Bußgeldbescheid aus. Betroffen ist ein Unternehmen, das sich auf Abmahnungen wegen angeblicher Verstöße gegen seine Filmurheberrechte im Internet spezialisiert zu haben scheint.

Eingeleitet wurde von uns auch ein Verfahren gegen ein Unternehmen, dessen Geschäftstätigkeit unter anderem darin besteht, unterstützend, zum Beispiel durch die Erstellung von Gutachten, an Rechtsanwaltskanzleien Juristen zu vermitteln. Ein Anwalt hatte sich in diesem Fall an uns mit der Beschwerde gewandt, dass er trotz seines Widerspruchs und der Aufforderung, seine Daten zu löschen weiterhin unerwünschte Werbeanschreiben von dem betreffenden Unternehmen erhielt. Unser Tatvorwurf besteht

darin, dass von dem Unternehmen unzulässig vorsätzlich Daten für Zwecke der Werbung verarbeitet werden, was eine Ordnungswidrigkeit darstellt. Ein Bußgeldbescheid wurde erlassen.

Im Hinblick auf die Verhängung eines Bußgeldes gegen die Geschäftsführerin eines Pflegeunternehmens wegen der Nichterteilung von richtigen und vollständigen Auskünften zur Videoüberwachung in dem Unternehmen, wogegen die Betroffene Einspruch eingelegt hatte (siehe hierzu 39. Jahresbericht, Ziffer 17.2), bestätigte das Amtsgericht das Vorliegen einer Ordnungswidrigkeit, reduzierte jedoch das von uns festgesetzte Bußgeld um die Hälfte.

Wegen Unterlassung der Bestellung einer oder eines betrieblichen Datenschutzbeauftragten, über die wir ebenfalls im 39. Jahresbericht, Ziffer 17.2 informiert hatten, erließen wir gegen den Geschäftsführer eines Unternehmens der Automobilbranche ebenfalls einen Bußgeldbescheid. Da der Betroffene gegen den Bescheid Einspruch einlegte, dem wir nicht abhelfen konnten, gaben wir den Vorgang zur weiteren Bearbeitung an die Staatsanwaltschaft ab. Mit einem gerichtlichen Verhandlungstermin ist in dieser Sache zu Beginn des Jahres 2018 zu rechnen.

Einen Bußgeldbescheid erließen wir auch gegen den Geschäftsführer eines Handelsunternehmens, in diesem Fall wegen unzulässiger Videoaufnahmen und der Nichtbestellung einer oder eines betrieblichen Datenschutzbeauftragten (siehe hierzu 39. Jahresbericht, Ziffer 17.2). Nachdem der Bescheid rechtskräftig geworden war, bezahlte der Betroffene das gegen ihn verhängte Bußgeld.

15.3 Zwangsmittel

Erneut wurden von uns in mehreren Fällen Zwangsmittelverfahren betrieben. Wie in den Vorjahren betrafen die Verfahren insbesondere die Nichterteilung von Auskünften. So weigerte sich in einem Fall eine Rechtsanwaltspartnerschaftsgesellschaft einem Auskunftsersuchen nachzukommen, das wir der Partnerschaft bereits mit einer Verfügung aus dem Jahr 2011 hatten zukommen lassen. Nachdem die Rechtsanwaltspartnerschaftsgesellschaft gegen unsere Verfügung geklagt hatte, hatte das Oberverwaltungsgericht diese im Jahr 2016 für rechtmäßig befunden. Da die Rechtsanwaltspartnerschaftsgesellschaft auch unserer trotz der Gerichtsentscheidung notwendig gewordenen Verfügung zur Erteilung der erforderlichen Auskünfte nicht nachkam, setzten wir ein Zwangsgeld in Höhe von 3.000 Euro fest, gegen das die Partnerschaft beim Verwaltungsgericht klagte. Die Klage ist aus unserer Sicht unbegründet. Die Entscheidung des Gerichts steht aber noch aus.

In einem anderen Fall baten wir ein Unternehmen des Feinkost- und Versandhandels um Auskunft zu der von ihm betriebenen Videoüberwachung und der Bestellung einer

beziehungsweise eines betrieblichen Datenschutzbeauftragten. Da wir die erbetenen Auskünfte zunächst nicht erhielten, erließen wir gegen den Geschäftsführer des Unternehmens eine Anordnung, uns die benötigten Auskünfte unverzüglich zu erteilen. Nachdem wir auch in der mit unserer Anordnung gesetzten Frist die Auskünfte nicht erhalten hatten, setzten wir ein Zwangsgeld in Höhe von 1.500 Euro fest. Der Geschäftsführer klagte gegen unsere Festsetzungsverfügung beim Verwaltungsgericht und begründete dies damit, dass uns die erforderlichen Auskünfte mit einem Schreiben seines Unternehmens kurz nach dem Erlass unserer Anordnung erteilt worden seien. Er konnte aber nicht belegen, dass uns dieses Schreiben, das wir tatsächlich erst vom Verwaltungsgericht als Anlage der Klageschrift erhielten, übersandt worden war. Für den Zugang einer empfangsbedürftigen Willenserklärung (Auskunft) Sorge zu tragen, obliegt nach allgemeinen Rechtsgrundsätzen dem Auskunftspflichtigen. Wir halten die Klage auch in diesem Fall für unbegründet und, da sich die angefochtene Zwangsgeldfestsetzung mittlerweile erledigt hat, nicht für zulässig. Die Entscheidung des Gerichts steht auch in dieser Sache noch aus.

In mehreren anderen Fällen wurden uns die erforderlichen Auskünfte erst erteilt, nachdem wir die Verhängung eines Zwangsgeldes angedroht hatten.

15.4 Einstellung von Bußgeldverfahren

Legt eine Betroffene beziehungsweise ein Betroffener bei der Verwaltungsbehörde, die den Bußgeldbescheid erlassen hat, fristgerecht Einspruch ein, so prüft die Behörde, ob sie den Bescheid aufrecht erhält oder zurücknimmt. Hält sie den Bußgeldbescheid aufrecht, übersendet die Behörde die Akten über die Staatsanwaltschaft an das Amtsgericht. Mit dem Eingang der Akten bei der Staatsanwaltschaft gehen die Aufgaben der Verfolgungsbehörde auf diese über. Die Staatsanwaltschaft legt die Akten der Richterin oder dem Richter beim Amtsgericht vor, wenn sie weder das Verfahren einstellt noch weitere Ermittlungen durchführt. Die Verwaltungsbehörde selbst kann das Bußgeldverfahren einstellen, wenn aufgrund der Zahlungsunfähigkeit der oder des Betroffenen das Bußgeld nicht einbringlich ist.

Aufgrund einer Anfrage einer Journalistin ermittelten wir, wie viele unserer Bußgeldverhängungen in den vergangenen Jahren wegen Einstellung des Bußgeldverfahrens durch die Staatsanwaltschaft oder das Gericht oder wegen Zahlungsunfähigkeit des Betroffenen erfolglos geblieben sind. Unsere Prüfung ergab, dass seit 2011 bei 26 Verfahren, in denen von uns Bußgeldbescheide erlassen worden waren, neun durch das Amtsgericht und zwei von uns selbst eingestellt worden waren. Soweit die Einstellung durch das Amtsgericht erfolgt war, hatte das Gericht die Begehung einer Ordnungswidrigkeit zwar bejaht, ihre Ahndung im Gegensatz zu uns jedoch nicht für geboten

erachtet. Die Gesamtsumme der auf diese Weise nicht realisierten Bußgelder beläuft sich auf circa 18.600 Euro.

16. Die Entschließungen der Datenschutzkonferenzen im Jahr 2017

16.1 Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 24. Januar 2017)

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (Bundesrat-Drucksache 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.

- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.

- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets – wie bislang – nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.

- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende

Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.

- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.

- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.

- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizeibehörden und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

16.2 Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 15. März 2017)

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesgesetzgeber auf, mit dem derzeit vorliegenden Gesetzentwurf der Bundesregierung "zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen" (Bundesrat-Drucksache 163/17) den Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtsicher und datenschutzkonform zu gestalten.

Die Schweigepflicht ist Grundlage des für die Berufsausübung notwendigen Vertrauensverhältnisses. Aber auch Berufsgeheimnisträger können heute nicht mehr wirtschaftlich agieren, ohne die moderne Informationstechnik und Kommunikationstechnik zu nutzen. Kaum ein Anwalt oder Arzt verfügt über das notwendige Spezialwissen, um diese Technik selbst zu warten und vor ständig neuen Bedrohungen abzusichern. Der vorliegende Gesetzentwurf will deshalb eine Praxis legalisieren, die aus Gründen der Praktikabilität längst etabliert ist.

Der strafrechtliche Schutz von Privatgeheimnissen soll die Beauftragung externer Dienstleister durch Berufsgeheimnisträger nicht länger erschweren. Im Gegenzug sollen diese Auftragnehmer künftig einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegen. Dennoch versäumt es der Gesetzentwurf, insbesondere mit der vorgeschlagenen Formulierung zu § 203 Strafgesetzbuch (StGB), klare Verhältnisse zu schaffen. Bisher sorgte unter Ärzten – und mitunter sogar Anwälten – der Umstand für Verwirrung, dass das, was datenschutzrechtlich legitim war, noch längst nicht strafrechtlich erlaubt sein musste. Was nach dem Gesetzentwurf nunmehr strafrechtlich erlaubt sein soll, könnte wiederum nach der neuen Europäischen Datenschutz-Grundverordnung mit empfindlichen Bußgeldern in Millionenhöhe sanktioniert werden. Denn es ist weder mit dem Schutzzweck von § 203 StGB vereinbar, noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen. Nicht absehbar ist zudem, ob die Zeugnisverweigerungsrechte und das Beschlagnahmeverbot in einem weiteren Gesetzgebungsverfahren entsprechend weitgehend auf alle denkbaren Dienstleister ausgeweitet werden, die an der Berufsausübung durch Berufsgeheimnisträger mitwirken.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dringt daher darauf, den Gesetzentwurf nachzubessern und die geplanten strafrechtlichen und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren. Es muss Berufsgeheimnisträgern möglich sein, externe Dienstleister zu Rate zu ziehen. Im Sinne der ungestörten Berufsausübung der Berufsgeheimnisträger und des Rechts auf informationelle Selbstbestimmung der Betroffenen sollten die Pflichten, die den Berufsgeheimnisträger dabei aus unterschiedlichen Rechtsgebieten treffen, aber soweit als möglich gleichlaufend ausgestaltet werden.

16.3 Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 16. März 2017)

Der "Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes" (Deutscher Bundestag-Drucksache 18/11326 und 18/11163; Bundesrat-Drucksache 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz (BKAG) und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.

Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.

Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen

und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante "Mitziehautomatik" erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

16.4 Gesetzentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 16. März 2017)

Die Bundesregierung hat im Januar 2017 einen Entwurf zur Novellierung des Straßenverkehrsgesetzes (Deutscher Bundestag Drucksache 18/11300) vorgelegt, um die Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen zu erlauben. Dabei sollen Fahrdaten aufgezeichnet werden, anhand derer bewertet werden kann, zu welchem Zeitpunkt das Auto jeweils durch den Fahrer oder durch eine "automatisierte Fahrfunktion" gesteuert wurde und wann ein Fahrer die Aufforderung zur Übernahme der Steuerung erhalten hat. Ebenfalls aufgezeichnet werden sollen Daten zu technischen Störungen automatisierter Fahrfunktionen. Mit den Daten soll sich nach einem Unfall klären lassen, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, regelt der Gesetzentwurf nicht.

Auf Verlangen der nach Landesrecht für Verkehrskontrollen zuständigen Behörden müssen die Fahrdaten diesen Behörden übermittelt werden. Die Fahrdaten sind auch Dritten zu übermitteln, wenn diese glaubhaft machen können, dass sie die Fahrdaten zur Geltendmachung, Abwehr oder Befriedigung von Rechtsansprüchen aus Unfällen benötigen. Unklar ist, wer die Daten übermitteln muss. Es bleibt ebenfalls unbestimmt, ob gegebenenfalls auch die Behörden Fahrdaten übermitteln dürfen.

Im Gesetzentwurf sind außerdem weder die Zwecke noch die zu übermittelnden Daten hinreichend konkretisiert. Weiterhin geht nicht hervor, wie die Integrität, Vertraulichkeit und Verfügbarkeit bei der Aufzeichnung und Übermittlung der Fahrdaten sichergestellt werden soll.

Sollte der Entwurf in der vorgelegten Form in Kraft treten, besteht in Kraftfahrzeugen mit hochautomatisierter oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber, die personenbezogene Profile bilden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Gesetzgeber zu einer dem datenschutzrechtlichen Bestimmtheitsgebot genügenden Novellierung des Straßenverkehrsgesetzes und zur Stärkung der Datenschutzrechte der Fahrer auf.

Sofern man eine Datenverarbeitung überhaupt für erforderlich hält, ist folgendes zu regeln:

- die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,
- die Bestimmung des für die Verarbeitung Verantwortlichen,
- die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,
- die Konkretisierung der Daten, die den nach Landesrecht zuständigen Behörden zu übermitteln sind,
- die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,
- eindeutige Festlegungen für die Trennung der Daten von den in den Fahrzeugdatenspeichern der Fahrzeuge gespeicherten Daten,
- die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,
- die Nennung des Adressaten für das Übermittlungsverlangen,

- die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und

- die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

16.5 Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 20. und 21. März 2017)

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen "abweichendes Verhalten" erkannt werden soll.[5]

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungstechniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und

[5] Siehe auch Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder "Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz".

konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder Bildaufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von Kfz-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von Kfz-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und es müssen angemessene und spezifische Regelungen zum Schutz der Grundrechte und Grundfreiheiten der Betroffenen vorgesehen werden. Hierzu gehören unter anderem eine normenklare Regelung für die Verwendung von Templates, zum Beispiel von Personen im Fahndungsbestand, für den Anlass zum Abgleich des Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.

Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

16.6 Göttinger Erklärung – Vom Wert des Datenschutzes in der digitalen Gesellschaft

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 20. und 21. März 2017)

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck dabei, das nationale Recht an die europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.

Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dies grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.

Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

"Datensouveränität" verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dies jedoch keinesfalls ersetzen.

Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Die Entwicklung datenschutzkonformer IT-Produkte und IT-Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

16.7 Umsetzung der Datenschutzgrundverordnung im Medienrecht

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 8. und 9. November 2017)

Das Inkrafttreten der Datenschutzgrundverordnung (DSGVO) und deren Geltungsbeginn im Mai 2018 verlangt eine Anpassung der medienrechtlichen Datenschutzbestimmungen an die neuen Vorgaben. Dabei muss dem hohen Stellenwert der Meinungs- und Informationsfreiheit sowie der Presse-, Rundfunk- und Medienfreiheit gemäß Artikel 5 Grundgesetz (GG) und Artikel 11 EU-Grundrechtecharta (GRCh) für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Artikel 1 in Verbindung mit Artikel 2 GG und dem Recht auf Schutz personenbezogener Daten gemäß Artikel 8 GRCh. Kollisionen der Schutzbereiche der Grundrechte sind im Sinne einer praktischen Konkordanz aufzulösen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist daher auf die Anpassungsklausel des Artikels 85 DSGVO hin. Danach können die Mitgliedstaaten Ausnahmen und Abweichungen von bestimmten Vorgaben der DSGVO normieren, wenn *"dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen".* Das sich daraus ergebende Regel-Ausnahme-Verhältnis bedeutet, dass die Vorgaben der DSGVO grundsätzlich auch auf sämtliche Verarbeitungen personenbezogener Daten zu grundrechtlich besonders geschützten journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angewendet werden sollen.

Bei der Umsetzung von Artikel 85 DSGVO gilt es insbesondere folgende Anforderungen zu beachten:

- Ausnahmen oder Abweichungen von der Anwendung der DSGVO auf die Verarbeitung personenbezogener Daten im journalistischen Bereich müssen notwendig sein, um freie Meinungsäußerung und Informationsfreiheit gemäß Artikel 11 GRCh sicherzustellen.

- Einen regelhaften Vorrang der Presse-, Rundfunk- und Medienfreiheit sieht die DSGVO nicht vor. Sie verlangt vielmehr, einen angemessenen Ausgleich zwischen den Grundrechten herzustellen, wenn diese in Widerstreit geraten (vergleiche 153. Erwägungsgrund der DSGVO).

- Die Grundsätze des Datenschutzes (Artikel 5 DSGVO) müssen hinreichend Beachtung finden. Jedenfalls steht es nicht im Einklang mit dem Recht auf Schutz personenbezogener Daten, wenn die Grundsätze des Datenschutzes im Journalismus in weitem Umfang ausgeschlossen werden. Eine Regelung kann keinesfalls als notwendig im Sinne der DSGVO angesehen werden, wenn sie zum Zwecke der Abwägung mit der Meinungsfreiheit und Informationsfreiheit die Transparenzrechte und Interventionsmöglichkeiten für betroffene Personen sowie Verfahrensgarantien über eine unabhängige Aufsicht missachtet.

- Über den eingeräumten Gestaltungsspielraum geht es hinaus, wenn die Verarbeitung personenbezogener Daten durch Hilfsunternehmen zu undifferenziert vom Geltungsbereich der DSGVO ausgenommen wird, ohne dass diese Aktivitäten unmittelbar der journalistischen Tätigkeit dienen. Die Reichweite der journalistischen Tätigkeit bedarf zudem einer Konkretisierung.

- Die künftige Aufsicht über den Datenschutz beim Rundfunk ist unabhängig auszugestalten. Sie bedarf wirksamer Abhilfebefugnisse bei Datenschutzverstößen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher für die Anpassung von Rundfunk-Staatsverträgen, Presse- und Mediengesetzen:

- Die gesetzlichen Anpassungen im Sinne des Artikels 85 DSGVO müssen konkret und spezifisch – bezogen auf die jeweiligen Normen und Vorgaben der DSGVO – Ausnahmen und Abweichungen regeln und diese begründen.

- Bei der Ausübung der jeweiligen Regelungskompetenz ist das europäische Datenschutzrecht zwingend zu beachten. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

16.8 Keine anlasslose Vorratsspeicherung von Reisedaten

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 8. und 9. November 2017)

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Gutachten vom 26. Juli 2017 (Gutachten 1/15) zum Fluggastdaten-Abkommen der Europäischen Union (EU) mit Kanada die langfristige Speicherung von Fluggastdaten (Passenger Name Records - PNR-Daten) sämtlicher Passagiere für nicht mit der Europäischen Grundrechtecharta vereinbar erklärt und seine Position zu anlasslosen Speicherungen personenbezogener Daten bekräftigt. Er erteilt damit einer anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage. Die Aussagen des EuGH sind nicht nur auf alle geltenden PNR-Instrumente übertragbar und stellen Anforderungen an die Anpassung des Fluggastdatengesetzes, sie betreffen auch die auf europäischer Ebene angestrebte Einrichtung eines Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS), die ebenfalls weitreichende anlasslose Speicherungen beabsichtigen.

Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu ermitteln, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen. Das gilt jedoch nicht für sensible Daten, die Rückschlüsse etwa auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder das Sexualleben ermöglichen. Der Übermittlungszweck rechtfertigt auch nicht automatisch die weitere Verwendung und Speicherung der Daten. Die übermittelten Daten haben vielmehr ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkreten Anhaltspunkte für geplante terroristische oder andere schwere Straftaten ergeben haben. In diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten.

Das Fluggastdatengesetz, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität umgesetzt wurde, geht insbesondere durch die Einbeziehung der innereuropäischen Flüge, die im Widerspruch zu dem Grundsatz des freien Personenverkehrs im Schengen-Raum steht, noch über den verpflichtenden Teil der Richtlinie hinaus.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sieht in den vom EuGH ausgesprochenen Feststellungen zur Rechtslage einen unverzichtbaren Maßstab für die Verordnungsvorschläge zur Einrichtung eines neuen Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS).

Mit dem EES sollen alle Ein- und Ausreisen sowie Einreiseverweigerungen von Drittstaatlern in die EU zentral erfasst und für mehrere Jahre gespeichert werden (einschließlich

biometrischer Identifizierungsmerkmale). Im ETIAS sollen zum Zwecke der Erleichterung der Grenzkontrollen vorab Daten von einreisewilligen visa-befreiten Drittstaatlern erhoben und ebenfalls für mehrere Jahre zentral gespeichert werden. In beiden Datenbanken sollen also Daten, die im Rahmen der Einreise und Grenzkontrolle erhoben werden, ebenso wie nach dem PNR-Abkommen, ohne konkreten Anlass zentral für einen langen Zeitraum vorgehalten werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hält dies nicht für vertretbar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert die jeweils zuständigen Gesetzgeber auf, zeitnah und konsequent sämtliche PNR-Instrumente der EU im Sinne der EuGH-Rechtsprechung nachzubessern, insbesondere das deutsche Fluggastdatengesetz.

Sie fordert die Bundesregierung zudem auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung der angestrebten Systeme EES und ETIAS einzusetzen.

17. Die Europäische und die Internationale Datenschutzkonferenz

Die Entschließungen der Europäischen Datenschutzkonferenz im Jahr 2017 stehen auf der Seite der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter https://www.bfdi.bund.de/DE/Infothek/Entschliessungen/EuDSK/_functions/EuDSK_table.html zur Verfügung. Informationen und Entschließungen der 39. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre, welche vom 25. bis 29. September 2017 in Hongkong stattgefunden hat, finden sich ebenfalls auf der Seite der Bundesbeauftragten für Datenschutz und Informationsfreiheit unter https://www.bfdi.bund.de/DE/Infothek/Entschliessungen/IntDSK/_functions/IntDSK_table.html.

18. Index

H

I

J

K

M

N

O

P

R

S

T

V

W

Z