39. 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 2016. Redaktionsschluss für die Beiträge war der 31. Dezember 2016.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Gegen die informationelle Fremdbestimmung: Datenschutz in Europa und Bremen

Im Mai 2016 wurde die Europäische Datenschutzgrundverordnung (siehe hierzu 38. Jahresbericht, Ziffern 1.1 bis 1.4, 15.2 und 17.2; 37. Jahresbericht, Ziffern 17.2 und 19.3; 36. Jahresbericht, Ziffern 1. und 22.2 sowie 35. Jahresbericht, Ziffern 1.2, 18.3 und 18.9) verabschiedet. Ab 25. Mai 2018 gilt sie direkt in ganz Europa. Nur dort, wo sie dies zulässt, haben die mitgliedstaatlichen Gesetzgeber noch Regelungsspielräume.

Damit brach für die Gesetzgeber in Bund und Ländern datenschutzpolitisch gesehen die spannendste Zeit seit dem Volkszählungsurteil an. Im Jahr 1986 hatte das Bundesverfassungsgericht entschieden, dass in das Grundrecht auf informationelle Selbstbestimmung nur durch Gesetze rechtmäßig eingegriffen werden darf, sofern die Betroffenen nicht in Datenverarbeitungen eingewilligt haben. Damit hatte das Urteil einen großen Kodifizierungsschub in Bund und Ländern zur Folge. Zu Recht hatte sich deshalb das Staatsarchiv Bremen für die entsprechenden Akten interessiert, die sich noch im Keller in unserem Dienstgebäude in Bremerhaven befunden hatten.

Vor dem Hintergrund der Datenschutzgrundverordnung müssen die mitgliedstaatlichen Gesetzgeber nun alle damals und seitdem entstandenen Datenverarbeitungsregelungen auf den Prüfstand stellen (siehe hierzu 38. Jahresbericht, Ziffer 1.4 "Da kommt was auf uns zu. Oder: Was der Landesgesetzgeber nach Erlass der Datenschutzgrundverordnung entscheiden muss.") Die datenschutzpolitische Diskussion, die die EU-Kommission im Januar 2012 mit dem Entwurf für die Datenschutzgrundverordnung begonnen hatte, geht also in die nächste Runde. Vermutlich auch deshalb, weil die Gesetzgeber in den Ländern deutlich mehr Gestaltungsspielräume haben, als dies beim Bundesgesetzgeber der Fall ist, unterscheiden sich die Diskussionen auf Bundesebene und auf Länderebene.

1.1 Datenschutz in Bremen nach Verabschiedung der Datenschutzgrundverordnung

Das Land Bremen reagierte sofort auf die Verabschiedung der Datenschutzgrundverordnung: Durch Beschluss vom 28. Juni 2016 bat der Senat die Senatskommissarin für den Datenschutz um die Erarbeitung eines Gesetzesentwurfs zur Ablösung des Bremischen Datenschutzgesetzes und die Senatskanzlei und die Ressorts um Überprüfung aller Fachgesetze im Hinblick auf die Datenschutzgrundverordnung (DSGVO). An der in diesem Zusammenhang eingesetzten ressortübergreifenden Arbeitsgruppe nimmt die Landesbeauftragte für Datenschutz und Informationsfreiheit teil. Daneben berät sie die Senatsressorts wie bei allen anderen Gesetzgebungsvorhaben auch bilateral.

Was die datenschutzpolitische Richtung der bremischen Gesetzgebung anbelangt, ergibt sich die Gelegenheit, **ein bremisches Profil der informationellen Selbstbestimmung in Europa** zu entwickeln. In diesem Sinne hatte ich im letzten Jahresbericht die Hoffnung geäußert, der bremische Gesetzgeber ergreife die Chance, den durch die DSGVO eröffneten gesetzgeberischen Spielraum im Sinne des durch die Europäische Grundrechtecharta geforderten höchstmöglichen Grundrechtsschutzes zu nutzen (siehe 38. Jahresbericht, Ziffer 1.4). Der Senat vertrat in seiner Stellungnahme zum 38. Jahresbericht die Auffassung, "dass der verbliebene gesetzgeberische Spielraum genutzt werden sollte, um einen hohen Grundrechtsschutz zu erhalten". Die ausgesprochen positiven Erfahrungen im begonnenen Prozess ermutigen mich, die semantische Abweichung allein als diplomatische Zurückhaltung und Vermeidung von stilistisch fragwürdigen Superlativen zu interpretieren. Dies stimmt zuversichtlich für die informationelle Selbstbestimmung im Land Bremen.

1.2 Gefahr der Absenkung des bisherigen Datenschutzniveaus auf der Bundesebene

Auf Bundesebene ist diese Zuversicht leider nicht angebracht. Dort ist ein heftiger Streit darüber entbrannt, welche Regelungsspielräume die Datenschutzgrundverordnung (DSGVO) lässt und wie die verbleibenden Spielräume auszufüllen sind. Interessant für die informationelle Selbstbestimmung der Menschen im Land Bremen ist dabei vor allem die Frage, welchen datenschutzrechtlichen Regeln künftig Datenverarbeitungen durch Unternehmen, Verbände und Vereine unterliegen werden. Dies entscheidet sich auf Bundesebene, weil dem Bund die betreffende Gesetzgebungszuständigkeit zusteht.

Seit Verabschiedung der Datenschutzgrundverordnung steht die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in engem Kontakt mit dem Bundesministerium des Innern. Unsere Stellungnahme enthält starke Kritik am ersten "geleakten" Entwurf eines "Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680", dessen Versendung an die Länder zumindest ein Bundesministerium widersprochen hatte (siehe hierzu: https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen02.c.730.de) Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder wendet sich unter anderem dagegen, dass im "geleakten" Entwurf der Grundsatz der Zweckbindung als eines der zentralen Prinzipien des Datenschutzrechts missachtet und die in der DSGVO verankerten Rechte der Betroffenen auf Information und Auskunft verletzt werden. Am 23. November 2016 wurde der erste offizielle Referentenentwurf des Bundesministeriums des Innern zu einem Artikelgesetz mit dem Kurznamen "Datenschutz-Anpassungs- und Umsetzungsgesetz EU" an die Länder und Verbände mit Stellungnahmefrist zum

7. Dezember 2016 übersandt. Auch dieser Entwurf begegnet massiven grundrechtlichen Bedenken, von denen hier nur einige beispielhaft genannt werden.

1.2.1 Datenminimierungsgrundsatz steht nicht zur Disposition des Bundesgesetzgebers!

Der datenschutzpolitischen Einschätzung des Gesetzesentwurfs sei hier eine Bemerkung zum Prinzip der Datenminimierung vorangestellt, das das wahllose Sammeln von Daten verhindert. Die Datenminimierung war auf dem Nationalen IT-Gipfel am 16. und 17. November 2016 in Saarbrücken als Prinzip des Grundrechtsschutzes in Misskredit gebracht und als Hemmschuh für Big-Data-Geschäftsmodelle diabolisiert worden. Glücklicherweise steht die Aushebelung dieses Prinzips seit Verabschiedung der Datenschutzgrundverordnung (DSGVO) nicht mehr zur Disposition der Mitgliedstaaten und findet sich daher auch nicht im Entwurf des Bundesministeriums des Innern! Artikel 5 der DSGVO formuliert das Prinzip der Datenminimierung als einen der unhintergehbaren Grundsätze für die Verarbeitung personenbezogener Daten. Die Datenverarbeitung muss "dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein". Die Verletzung der Pflicht zur Datenminimierung kann nach Artikel 83 DSGVO mit "Geldbußen von bis zu 20.000.000 Euro oder im Fall eines Unternehmens von bis zu 4 Prozent seines gesamten weltweit erzielten Jahresumsatzes (..) je nachdem, welcher der Beträge höher ist", geahndet werden.

1.2.2 Geplante Zweckänderungsbefugnisse für Private verstoßen gegen die Datenschutzgrundverordnung

Der Entwurf des Bundesministeriums des Innern räumt Privaten in § 23 Absatz 2 des "BDSG-neu" (Bundesdatenschutzgesetz-neu), das den Artikel 1 des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU, darstellt, weitreichende Befugnisse ein, personenbezogene Daten in einem anderen Kontext zu verwenden als sie erhoben wurden. Was die datenschutzpolitische Einordnung anbelangt fügen sich diese Regelungen in das auf dem genannten IT-Gipfel verkündete Projekt ein, Datenschutzstandards abzusenken und auf rechtliche Beschränkungen für Big-Data-Geschäftsmodelle zu verzichten. So wird die Bundeskanzlerin mit der Äußerung zitiert: "Die Datenschutzgrundverordnung (DSGVO) ist eine Verordnung, aber der Minister de Maizière weist immer wieder darauf hin, dass es eine Vielzahl unbestimmter Rechtsbegriffe gibt, bei denen wir jetzt aufpassen müssen, dass wir es nicht wieder so restriktiv machen, dass das Big-Data-Management dann doch nicht möglich wird. Insofern wird die nationale Umsetzung nochmal sehr interessant werden und

auch die Auslegung dann in den Gerichten."[1] In dieses Bild passt, dass der Katalog der Zweckänderungsmöglichkeiten für nicht öffentliche Stellen im Vergleich zum ersten, "geleakten" Entwurf des Bundesministeriums des Inneren sogar noch deutlich ausgeweitet wurde. Die gegenwärtig geltenden Regeln des Bundesdatenschutzgesetzes (BDSG) zugrunde gelegt stellen die geplanten Zweckänderungsbefugnisse damit deutliche Verschlechterungen des Datenschutzniveaus in Deutschland dar. Sofern sie verabschiedet würden, wäre Privaten die zweckändernde Datenverarbeitung in deutlich größerem Maße erlaubt als dies derzeit der Fall ist.

Gleichzeitig verstoßen die geplanten Regelungen gegen die Datenschutzgrundverordnung, die in Artikel 5 Absatz 1 Nummer 5 die Zweckbindung als eines der fundamentalen Prinzipien für die Verarbeitung personenbezogener Daten bestimmt und vorschreibt, dass personenbezogene Daten für "festgelegte, eindeutige und legitime Zwecke erhoben werden" müssen und "nicht" in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Stattdessen werden im Entwurf zum BDSG-neu Zweckänderungen pauschal erlaubt, ohne dass eine Auseinandersetzung mit den Folgen für die Betroffenen stattfinden würde, und ohne dass gesetzgeberische Vorkehrungen für den Schutz der Betroffenen getroffen würden.

Damit kollidieren die vorgeschlagenen Regelungen mit dem letztlich verabschiedeten Normtext der Datenschutzgrundverordnung, der der Möglichkeit zu zweckändernden Weiterverarbeitungen strenge Grenzen setzt. Zwar wären nach dem ursprünglichen Entwurfstext der EU-Kommission zu Artikel 6 Absatz 4 Satz 1 DSGVO Datenverarbeitungen auch zu einem Zweck, der nicht mit dem ursprünglichen Zweck vereinbar ist, erlaubt gewesen, wenn auf die zweckändernde Datenverarbeitung einer der in dieser Regelung genannten fünf Gründe zugetroffen hätte. Die Verfolgung berechtigter Interessen gehörte übrigens nicht hierzu. In den Trilogverhandlungen übernahm der Rat der Europäischen Union die Kommissionsformulierung und fügte ihr einen Satz an, nach dem die Weiterverarbeitung für nicht konforme Zwecke sogar schon dann rechtmäßig gewesen wäre, wenn sie durch denselben Verantwortlichen erfolgt wäre und dessen berechtigte Interessen oder die berechtigten Interessen eines Dritten die Interessen der betroffenen Person überwogen hätten. Wie die verabschiedete Fassung des Artikels 6 Absatz 4 DSGVO belegt, folgte der europäische Gesetzgeber aber weder dem ursprünglichen Kommissionvorschlag noch dem Vorschlag des Rates. Stattdessen ist die zweckändernde Weiterverarbeitung nach der DSGVO nur zulässig, wenn die Zwecke der ursprünglichen Datenverarbeitung und der zweckändernden Weiterverarbeitung kompatibel sind, wenn die Betroffenen in die zweckändernde Weiterverarbeitung eingewilligt haben, oder wenn sie sich im Rahmen einer speziellen mitgliedstaatlichen Rechtsnorm oder EU-Rechtsnorm halten, die zum Schutz der

[1] https://netzpolitik.org/2016/angela-merkel-hat-gehoert-dass-sie-datenschutz-jetzt-datensouveraenitaet-nennen-soll/

in Artikel 23 Absatz 1 genannten elementaren Gemeinwohlbelange unabdingbar erforderlich ist.

Die Begründung des Referentenentwurfs scheint sich für alle in § 23 des Entwurfs vorgeschlagenen Regelungen auf Artikel 6 Absatz 4 DSGVO zu berufen, wenn behauptet wird, diese Norm sei eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 DSGVO genannten Ziele. Um welchen der in Artikel 23 Absatz 1 genannten zehn Gemeinwohlbelange es sich handelt, wird jedoch nicht erläutert. Schon hiermit verstößt der Entwurf gegen die sich aus der DSGVO ergebenden Konkretisierungsanforderungen an die mitgliedstaatlichen Gesetzgeber. Auch können nach Artikel 6 Absatz 4 DSGVO Zweckänderungen nur durch solche mitgliedstaatliche Rechtsvorschrift gerechtfertigt werden, die "in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt." Eine solche vorzuschlagen, ist dem Bundesministerium des Innern im Absatz 2 des Entwurfs nicht gelungen. Der Katalog der Zweckänderungsbefugnisse des § 23 Absatz 2 des Entwurfs für nicht öffentliche Stellen ist pauschal und uferlos. Artikel 23 DSGVO richtet sich an die Mitgliedstaaten und verleiht ihnen Befugnisse zur Schaffung von Gesetzen. Der Gesetzesentwurf des Bundesministeriums des Innern verwendet ähnliche oder gleich lautende Formulierungen im selben Abstraktionsgrad wie Artikel 23 DSGVO, um nicht öffentlichen Stellen Datenverarbeitungsbefugnissen zu verschaffen. Auch in dieser Hinsicht erfüllt der Gesetzesentwurf nicht die an mitgliedstaatliche Gesetzgeber gerichteten Konkretisierungsanforderungen der DSGVO, insbesondere nicht diejenigen im Sinne des Artikels 23 Absatz 2 DSGVO. Die Normsetzungsbefugnisse stehen gerade unter dem Vorbehalt, dass die abstrakt gefassten Befugnisse zur Schaffung von mitgliedstaatlichem Recht ausgefüllt und auf konkrete Gesetzgebungsmaterien zugeschnitten werden. Die bloße Umdefinition von Gesetzgebungsbefugnissen in Datenverarbeitungsbefugnisse unterliegt einem grundsätzlichen Denkfehler, entzieht sich der gesetzgeberischen Konkretisierungsaufgabe und verstößt damit gegen die DSGVO.

Die in der DSGVO genannten Voraussetzungen werden von den Nummern 1 bis 4 des § 23 Absatz 2 des Entwurfs also in keiner Hinsicht erfüllt. Diese Regelungen, auf deren Regelungsgehalt im Folgenden noch einmal näher eingegangen wird, müssen damit ersatzlos wegfallen, will der Bundesgesetzgeber nicht die Nichtigkeitserklärung durch den Europäischen Gerichtshof riskieren.

1.2.2.1 Geplante Zweckänderungsbefugnis zur Abwehr von Gefahren und zur Strafverfolgung streichen

Die Vorschrift des § 23 Absatz 2 Nummer 1 des Entwurfs für das BDSG-neu (Bundesdatenschutzgesetz-neu) schafft für nicht öffentliche Stellen, also für Private, die Befugnis zur zweckändernden Datenverarbeitung, wenn diese "zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist". Dies unterschreitet das gegenwärtige Datenschutzniveau und verstößt gegen die Datenschutzgrundverordnung.

In der Überschrift findet sich in eckigen Klammern der zutreffende Hinweis, dass es sich bei der vorgeschlagenen Formulierung um eine wörtliche Wiederholung der bis zum 31. August 2009 geltenden Fassung des § 28 Absatz 3 Nummer 2 BDSG-alt handelt. Misstrauen darüber, dass die alte und nicht die derzeit geltende Fassung verwendet wird, ist angebracht: Gegenwärtig gilt § 28 Absatz 2 Nummer 2 b) Bundesdatenschutzgesetz (BDSG), wonach es konstitutive Voraussetzung einer zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlichen Zweckänderung ist, dass zusätzlich "kein Grund zu der Annahme besteht, dass die oder der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat". Insofern unterschreitet die vorgeschlagene Regelung, der eine entsprechende Anforderung fehlt, definitiv das gegenwärtig geltende Datenschutzniveau und setzt sich über den nach einem langen Gesetzgebungsprozess gefundenen derzeit gültigen gesetzgeberischen Willen hinweg. Nummer 1 verknüpft Datenerhebungen nicht öffentlicher Stellen und öffentliche Sicherheitsinteressen. Hier besteht zusammen mit der genannten Absenkung der Zweckänderungsvoraussetzungen ein Zusammenhang zum Vorschlag für ein "Videoüberwachungsverbesserungsgesetz", dessen Regelungen Eingang in den vorgelegten Entwurf gefunden haben und den die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ablehnt. Auch wenn Nummer 1 ein Zitat eines vormals geltenden Gesetzes darstellt, erfüllt diese Formulierung aufgrund ihrer Allgemeinheit jedenfalls nicht die in der Datenschutzgrundverordnung aufgestellten Konkretisierungsanforderungen an mitgliedstaatliche Gesetze und verstößt damit gegen die Datenschutzgrundverordnung.

1.2.2.2 Geplante Zweckänderungsbefugnis zur Durchsetzung rechtlicher Ansprüche streichen

Die Vorschrift des § 23 Absatz 2 Nummer 2 des Entwurfs des BDSG-neu (Bundesdatenschutzgesetz-neu) statuiert die Zulässigkeit zweckändernder Datenverarbeitungen durch Private, wenn "sie zur Geltendmachung, Ausübung oder

Verteidigung rechtlicher Ansprüche erforderlich ist". Für eine solche Regelung lässt die Datenschutzgrundverordnung (DSGVO) keinen mitgliedstaatlichen Regelungsspielraum. Laut Verweis in den eckigen Klammern soll es sich um eine Ausfüllung der Möglichkeiten des Artikels 23 Absatz 2 (gemeint ist wohl: Absatz 1) Buchstabe j DSGVO handeln. Schon der Verweis auf Artikel 23 Absatz 1 j DSGVO ist nicht korrekt. Die Norm der DSGVO ermöglicht unter strengen Voraussetzungen die Abweichung von bestimmten Regelungen der DSGVO, wenn dies "zur Geltendmachung, Ausübung oder Verteidigung **zivil**rechtlicher Ansprüche erforderlich ist". Die Formulierung des Entwurfs zielt darüber hinaus auf alle "rechtlichen" Ansprüche. Aufgrund des abschließenden Charakters der Liste der in Artikel 23 Absatz 1 genannten Rechtsgüter stellt schon dies einen Verstoß gegen die DSGVO dar, der schon allein zur Unzulässigkeit der Nr. 2 führt.

Aufgrund der Uferlosigkeit der Formulierung der Nummer 2, die wieder die Formulierung der an die Mitgliedstaaten gerichteten Gesetzgebungsbefugnis als Formulierung für Datenerhebungsbefugnisse nicht öffentlichen Stellen wiederholt, bestünde die behauptete mitgliedstaatliche Konkretisierungsmöglichkeit aber auch dann nicht, wenn die Nummer 2 auf die Erforderlichkeit für die Geltendmachung, et cetera **zivil**rechtlicher Ansprüche eingeschränkt würde. Artikel 23 Absatz 1 Buchstabe j zielt offensichtlich darauf, den Mitgliedstaaten zu ermöglichen, in Gesetzesmaterien wie dem Zwangsvollstreckungsrecht Regelungen für erlaubte Zweckänderungen aufzunehmen. Die in Artikel 23 Absatz 1 DSGVO genannten einschränkenden Voraussetzungen der Achtung des Wesensgehalts der Grundrechte und Grundfreiheiten und der Erforderlichkeit und Verhältnismäßigkeit der gesetzgeberischen Maßnahme in einer demokratischen Gesellschaft hätten allenfalls Datenverarbeitungen für konkrete Verarbeitungszwecke in bestimmten abgegrenzten Rechtsbereichen wie dem Zwangsvollstreckungsrecht erfüllen können. Die Formulierung in Nummer 2 stellt demgegenüber eine pauschale mitgliedstaatliche Zweckänderungserlaubnis für alle Datenverarbeitungen dar, die für die Geltendmachung, Ausübung oder Verteidigung aller rechtlichen Ansprüche erforderlich ist. Sie verstößt gegen die Anforderungen der DSGVO und muss gestrichen werden.

1.2.2.3 Geplante Zweckänderungsbefugnis zur Wahrung eigener berechtigter Interessen streichen

Die Vorschrift des § 23 Absatz 2 Nummer 3 des Entwurfs sieht eine Befugnis nicht öffentlicher Stellen zur zweckändernden Verarbeitung bereits dann vor, "wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist." Dies unterschreitet das gegenwärtige Datenschutzniveau massiv und verstößt gegen die Datenschutzgrundverordnung (DSGVO).

Im Entwurf des BDSG-neu (Bundesdatenschutzgesetz-neu) wird behauptet, die Formulierung übernehme den gegenwärtigen § 28 Absatz 2 Nummer 1 in Verbindung mit Absatz 1 Nummer 2 Bundesdatenschutzgesetz. Diese Regelung lautet aber: "Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der oder des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt." Der Entwurf des BDSG-neu räumt davon abweichend eine umfassende Verarbeitungsbefugnis anstatt nur einer Nutzungsbefugnis und Übermittlungsbefugnis ein. Zudem unterschlägt er das entscheidende Abwägungskriterium der entgegenstehenden schutzwürdigen Betroffeneninteressen.

Auch inhaltlich ist § 23 Absatz 2 Nummer 3 mit der DSGVO unvereinbar. Dieser Erlaubnistatbestand würde das von der DSGVO als konstitutiv statuierte und nur unter den genannten restriktiven Voraussetzungen relativierbare Prinzip der Zweckbindung von Datenverarbeitungen vollständig auflösen, da jedes berechtigte Interesse ungeachtet der Betroffeneninteressen den Privaten zu zweckändernden Weiterverarbeitungen berechtigte. Der erwähnte Entstehungsprozess der DSGVO belegt eindeutig, dass die DSGVO das alleinige Vorliegen berechtigter Interessen des Verantwortlichen nicht als ausreichende Grundlage für eine zweckändernde Datenverarbeitungsbefugnis ansieht. Obwohl also diesem Ansinnen der Zulassung einer zweckändernden Datenverarbeitung aufgrund berechtigter Interessen des Verantwortlichen im Abstimmungsprozess der EU-Akteure eine eindeutige Absage erteilt wurde, versucht der Entwurf, sie trotz der damit verbundenen Verletzung europäischen Rechts durch das BDSG-neu zu ermöglichen.

Da die gesetzgeberische Auseinandersetzung mit den Risiken des Gesetzes für die Rechte und Freiheiten der betroffenen Personen fehlt, kann nur spekuliert werden, dass es hier zumindest auch um die Einschränkung des in Artikel 22 Absatz 1 gewährleisteten "Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden" geht. Hier scheint also ein Einfallstor für die gewünschte Erleichterung von Big-Data-Anwendungen zu liegen. Diese Hoffnung macht die DSGVO glücklicher Weise selbst zunichte, indem sie gesetzgeberische Versuche wie den vorliegenden nicht als Konkretisierungsregelungen akzeptiert. Auch die Nummer 3 verstößt gegen die DSGVO.

1.2.2.4 Geplante Zweckänderungsbefugnis für allgemein zugängliche Daten streichen

Die Vorschrift des § 23 Absatz 2 Nummer 4 des Entwurfs erlaubt Privaten die zweckändernde Datenverarbeitung, sofern es sich um Daten handelt, die "allgemein zugänglich sind oder die beziehungsweise der Verantwortliche sie veröffentlichen dürfte, es

sei denn, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse der oder des Verantwortlichen offensichtlich überwiegt und kein Grund zu der Annahme besteht, dass die betroffene Person ein schutzwürdiges Interesse an dem Ausschluss der Weiterverarbeitung hat". Diese Zweckänderungsmöglichkeit soll laut Entwurf mit "ex: § 28 Absatz 2 Nummer 1 BDSG-alt in Verbindung mit § 28 Absatz 1 Satz 1 Nummer 3 BDSG-alt" identisch sein. Tatsächlich erweitert die geplante Regelung aber die Möglichkeit zu zweckändernden Datenverarbeitungen Privater. Diese sind nicht wie in der gegenwärtig geltenden Regelung des Bundesdatenschutzgesetzes (BDSG) immer dann ausgeschlossen, wenn das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse der oder des Verantwortlichen offensichtlich überwiegt. Nach der geplanten Regelung ist die Zweckändernde Verarbeitung nur rechtswidrig, wenn zusätzlich kein Grund zu der Annahme besteht, dass die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Weiterverarbeitung haben. Selbst bei offensichtlich entgegenstehendem Interesse der Betroffenen, also in den Fällen, in denen diese in eine zweckändernde Verarbeitung nicht einwilligen würden, dürfen die Daten also zweckändernd verarbeitet werden, es sei denn, es besteht "Grund zur der Annahme", dass die Person ein die Zweckänderung ausschließendes schutzwürdiges Interesse hat. Damit wird auf die subjektive Sicht der Verarbeitenden abgestellt. Sogar in den Fällen, in denen die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Weiterverarbeitung haben, dieses der Verarbeiterin beziehungsweise dem Verarbeiter aber nicht bekannt ist, sie oder er also "keinen Grund" hat, hiervon auszugehen, soll also die zweckändernde Datenverarbeitung erlaubt sein. Damit unterschreitet die geplante Regelung das gegenwärtige Datenschutzniveau erheblich.

Auch aus europarechtlicher Sicht ist die geplante Regelung des § 23 Absatz 2 Nummer 4 nicht zu halten. Laut Begründung ergibt sich die Regelungsbefugnis des Bundesgesetzgeber auch im Hinblick auf die Nummer 4 aus Artikel 6 Absatz 4 in Verbindung mit 23 Absatz 1 Datenschutzgrundverordnung (DSGVO). Warum eine pauschale Befugnis zur zweckändernden Datenverarbeitung allgemein zugänglicher Daten dem Schutz eines der Ziele des Artikels 23 Absatz 1 DSGVO dienen soll, erschließt sich nicht. Inhaltlich könnte am ehesten der Schutz eines "sonstigen wichtigen Zieles des allgemeinen öffentlichen Interesses" Deutschlands in Frage kommen. Die DSGVO macht es den mitgliedstaatlichen Gesetzgebern aber gerade zur Aufgabe, die Schutzziele zu benennen und sich damit auseinanderzusetzen, warum die gesetzliche Regelung eine "in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme" zum Schutz dieses benannten Zieles darstellt. Da entsprechende Erwägungen komplett fehlen und auch schwer zu erbringen wären, ohne verletzend in Grundrechte der Betroffenen einzugreifen, muss auch § 22 Absatz 2 Nummer 4 des Entwurfs gestrichen werden.

1.2.3 Geplante Regelung zur Datenverarbeitung zu Forschungszwecken streichen

Die in § 25 des Entwurfs für das BDSG-neu (Bundesdatenschutzgesetz-neu) geplanten Regelungen zur Datenverarbeitung zu wissenschaftlichen oder historischen Zwecken verstoßen gegen die Anforderungen der Datenschutzgrundverordnung (DSGVO) und müssen daher gestrichen werden, will der Bundesgesetzgeber nicht die Aufhebung durch den Europäischen Gerichtshof riskieren.

Der geplante § 25 Absatz 1 erlaubt die Verarbeitung besonderer Kategorien personenbezogener Daten ohne weitere Voraussetzungen schon dann, wenn dies zur Durchführung wissenschaftlicher oder historischer Forschung erforderlich ist. Nach Artikel 9 Absatz 1 Buchstabe j DSGVO muss eine mitgliedstaatliche Regelung, die entsprechende Verarbeitungen besonderer Kategorien personenbezogener Daten erlaubt, drei Voraussetzungen erfüllen. Sie muss in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen.

Dass die Datenverarbeitung für die Forschung "erforderlich" ist, bedeutet gerade noch nicht, dass sie "in angemessenem Verhältnis zu dem verfolgten Ziel" steht, also verhältnismäßig ist. In der dreistufigen Verhältnismäßigkeitsprüfung sind mit der Erforderlichkeitsprüfung der Datenverarbeitung erst die Eignung und die Erforderlichkeit der Datenverarbeitung für die Zielerreichung, nicht jedoch die Verhältnismäßigkeit im engeren Sinne, also die Angemessenheit der Datenverarbeitung belegt. Genau an dieser Stelle müsste der mitgliedstaatliche Gesetzgeber Verhältnismäßigkeitserwägungen anstellen und nicht pauschal jede geeignete und erforderliche Datenverarbeitung erlauben. Dass dies versäumt wurde, deutet darauf hin, dass hier die zweite Voraussetzung – die der Wahrung des Wesensgehalts des Grundrechts auf Datenschutz – in Zweifel zu ziehen ist. Auch werden keine auf die konkreten Datenverarbeitungssituationen bezogenen spezifischen Maßnahmen vorgesehen. Zwar bedeutet der Verweis auf § 22 Absatz 2 des Entwurfs, dass "angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte vorzusehen" sind. Auch hier gilt jedoch, dass zum einen die bloße Wiederholung des Normtextes des Artikels 9 Absatz 1 Buchstabe j DSGVO gerade noch keine Betätigung des gesetzgeberischen Konkretisierungsauftrags darstellt, derer es aber hier bedurft hätte. Auch werden in § 22 Absatz 2 des Entwurfs keine ausreichenden und effektiven Schutzmaßnahmen geregelt, sondern lediglich beliebig scheinende Vorkehrungen inklusive der Sensibilisierung und Schulung der "an Verarbeitungsvorgängen Beteiligten" in den Raum geworfen. Zudem ist der Verweis auf die Maßgeblichkeit von "Implementierungskosten"

gerade keine angemessene Maßnahme zur Wahrung von Grundrechten! Der geplante § 25 Absatz 1 stellt damit einen eklatanten Verstoß gegen die DSGVO dar.

Der geplante § 25 Absatz 2 bestimmt, dass die Betroffenenrechte auf Auskunft und Erhalt einer Kopie "nicht bestehen", wenn dies "einen unverhältnismäßigen Aufwand" erfordern würde. Dies verstößt gegen die Anforderungen des Artikels 23 DSGVO, wonach Beschränkungen der Betroffenenrechte "den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen und in der gesetzlichen Grundlage spezifische Regelungen nach Artikel 23 Absatz 2 DSGVO getroffen werden müssen". Das elementare Betroffenenrecht auf Auskunft zu beschränken, weil seine Beachtung beim Datenverarbeiter Aufwand verursacht, muss den Wesensgehalt von Grundrechten beeinträchtigen. Das gilt nur unwesentlich eingeschränkt auch für das Recht auf Erhalt von Kopien. Auch diese Regelung muss daher wegen Verstoßes gegen die Anforderungen der DSGVO gestrichen werden.

1.2.4 Keine Einschränkung der Auskunftspflicht zugunsten von Betriebs- und Geschäftsgeheimnissen

In § 31 Absatz 2 Nummer 2 a des Entwurfs soll die Auskunftspflicht der datenverarbeitenden privaten Stellen gegenüber den betroffenen Grundrechtsträgerinnen und Grundrechtsträger in einer Weise eingeschränkt werden, die nicht mit der elementaren Stellung in Einklang gebracht werden kann, die die Datenschutzgrundverordnung den Betroffenenrechten einräumt. Die geplante Regelung beschränkt den Auskunftsanspruch der Betroffenen gegen Private darüber, welche ihrer personenbezogenen Daten in welcher Weise verarbeitet werden, zugunsten des Schutzes von Betriebs- und Geschäftsgeheimnissen. Datenschutzrechtlich verantwortliche Unternehmen sollen grundsätzlich schon dann von der Auskunftspflicht befreit sein, wenn "die Information die Geschäftszwecke" eines Unternehmens "erheblich gefährden würde". Nur im Ausnahmefall, "wenn das Interesse der betroffenen Person an der Information überwiegt", soll sie Auskunft darüber erhalten, welche ihrer Daten vom Unternehmen verarbeitet wurde. Aus datenschutzpolitischer Sicht ist zu vermuten, dass es hier auch um den Schutz der Profilbildungsalgorithmen geht, weil möglicherweise behauptet werden darf, dass schon die Offenlegung der in den Algorithmus einfließenden Datenkategorien, zu der Datenverarbeiter gegenwärtig verpflichtet sind, als Missachtung von Betriebs- und Geschäftsgeheimnissen angesehen werden kann.

1.2.5 "Videoüberwachungsverbesserungsgesetz" zurückziehen!

Auch § 4 Absatz 1 Nummer 2 des Entwurfs für das BDSG-neu (Bundesdatenschutzgesetz-neu) muss gestrichen werden. Diese Regelung wiederholt das vom Bundesministerium des

Innern kürzlich als Entwurf vorgelegte "Videoüberwachungsverbesserungsgesetz". Sie verlagert die Aufgabe der Gewährleistung der öffentlichen Sicherheit auf Private wie die Betreiber von Einkaufszentren und öffentlichem Personennahverkehr und kann nicht begründen, warum die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist (siehe hierzu die Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9. November 2016 "Videoüberwachungsverbesserungsgesetz zurückziehen!" unter der Ziffer 18.8 dieses Berichts).

Bereits die bestehende Bestimmung zur Videoüberwachung durch private Stellen in § 6 b Bundesdatenschutzgesetz (BDSG) lässt es zu, dass bei privat verantworteten Videoanlagen Sicherheitsbelange von Personen, die sich an öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen berücksichtigt werden. Gerade im Bereich von Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs werden bereits heute zahlreiche Kameras betrieben, die sich im Rahmen der gesetzlichen Befugnisse Privater halten. Die privaten Betreiber bleiben aber auch nach der geplanten Regelung frei in der Entscheidung, ob sie rechtlich zulässige Kameras installieren oder ihre legitimen Zwecke beispielsweise auf Durchsetzung des Hausrechts auf andere Weise erfüllen wollen. Ob alle erlaubten Kameras tatsächlich aufgestellt werden, entscheiden die Betreiber also weiterhin selbst. Auch die Tatsache, dass die Betreiber privater Videoüberwachungsanlagen bereits heute in der Regel überfordert sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann, hätte in die Erwägungen Eingang finden sollen.

1.3 Die Datenschutzgrundverordnung als Garantin der informationellen Selbstbestimmung in einem grundrechtsgewogenen Europa

Die Betrachtung der Diskussion auf Bundesebene zeigt, dass die Verabschiedung der Datenschutzgrundverordnung (DSGVO) im Berichtsjahr eine sehr gute Nachricht für die Trägerinnen und Träger des Grundrechts auf informationelle Selbstbestimmung ist und bleibt. Die Datenschutzgrundverordnung ist Garantin der informationellen Selbstbestimmung und bietet den Menschen Schutz vor informationeller Fremdbestimmung durch öffentliche oder private Datenverarbeiter, aber auch durch mitgliedstaatliche Gesetzgeber. Auch sie dürfen den durch die DSGVO gesetzten Standard nicht unterschreiten und müssen – falls sie es dennoch versuchen – damit rechnen, dass die entsprechenden Normen durch den Europäischen Gerichtshof für nichtig erklärt werden. Davon, dass der bremische Gesetzgeber die ihm von der DSGVO eingeräumten Befugnisse nutzen wird, um die

informationelle Selbstbestimmung im Land Bremen in Übereinstimmung mit diesen Grundsätzen auszugestalten, bin ich überzeugt.

Dr. Imke Sommer

2. Neue europäische Datenschutzregelungen – Wird alles anders?

Die Europäische Datenschutzgrundverordnung, die ab Mai 2018 angewendet werden wird, zeigt, dass Europa auch in Bremen ganz nah ist – anders als viele Bürgerinnen und Bürger dies möglicherweise empfinden. Das neue Europäische Datenschutzrecht gilt nämlich für viele deutsche, also auch bremische, Behörden und alle deutschen Unternehmen unmittelbar. So ist es beispielsweise bei den in der Datenschutzgrundverordnung statuierten Rechten der Betroffenen. Die eher allgemein gefassten Regelungen der europäischen Verordnung treten vor allem für private Datenverarbeiter an die Stelle des gegenwärtig geltenden Rechts. Unter anderem in den Bereichen Videoüberwachungen, Telemedien und Auskunfteien wird dies zu neuen Bewertungen der Zulässigkeit von Datenverarbeitungen führen. Ob und wie weit die Datenschutzgrundverordnung den nationalen Gesetzgebern hier Konkretisierungsmöglichkeiten eröffnet, ist Gegenstand der bereits begonnenen datenschutzpolitischen Debatte auf Bundesebene (siehe hierzu Ziffer 1.2 dieses Berichts). Dabei sind die Konkretisierungsanforderungen und Konkretisierungsmöglichkeiten der Datenschutzgrundverordnung Herausforderungen und gleichzeitig auch Chancen für grundrechtsgewogene neue rechtliche Gestaltungen für die Landesgesetzgeber wie die Bremische Bürgerschaft (siehe hierzu Ziffer 1.1 dieses Berichts) und den Bundesgesetzgeber. In Bezug auf die Umsetzung der europäischen Richtlinie "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" ist der gesetzgeberische Spielraum naturgemäß unbestritten. Insofern wird hier die Diskussion über die konkrete Umsetzung im Vordergrund stehen.

Bei allen Änderungen ist aber ein wichtiger Grundsatz der informationellen Selbstbestimmung unverändert geblieben: Dass Verarbeitung personenbezogener Daten nur möglich ist, wenn es hierfür eine Rechtsgrundlage gibt (Verbot mit Erlaubnisvorbehalt), gilt weiterhin.

2.1 Grundsätzliche Stärkung der Rechte der Betroffenen

Was verändert sich für die Menschen in Bremen? Beispielsweise der Auskunftsanspruch der von Datenverarbeitung Betroffenen wird direkt aus Artikel 15 der Datenschutzgrundverordnung hergeleitet und kann elektronisch geltend gemacht werden. Die Betroffenen haben einen Anspruch auf eine kostenlose Kopie ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung sind, durch die datenverarbeitende Stelle. Weitere Kopien sind kostenpflichtig. Wird der Antrag auf Auskunft elektronisch gestellt, so sind die Informationen in einem gängigen elektronischen Format durch die datenverarbeitende Stelle zur Verfügung zu stellen, sofern die Antragstellenden in ihrem elektronischen Antrag auf

Auskunft nichts anderes verlangen. Die Auskunft muss unverzüglich, in jedem Fall innerhalb eines Monats nach Eingang des Antrags, zur Verfügung gestellt werden. Beispielsweise ein Verstoß eines Unternehmens gegen die Pflicht zur rechtzeitigen Auskunftserteilung oder zur vollständigen Auskunftserteilung kann als eine Ordnungswidrigkeit mit einer Geldbuße mit bis zu 20.000.000 Euro oder von bis zu 4 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden, je nachdem, welcher der Beträge höher ist. Diese Sanktionsmöglichkeit zeigt, dass die Datenschutzgrundverordnung der Durchsetzung des Auskunftsanspruchs und damit der Rechte der Betroffenen erhebliche Bedeutung zumisst.

Außerdem wird unmissverständlich klargestellt, dass die Datenschutzgrundverordnung verbindlich für die Verarbeitung der personenbezogenen Daten aller Menschen gilt , die sich in der Europäischen Union aufhalten, wenn die Datenverarbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen in der Union steht oder dazu dient, das Verhalten betroffener Personen in der Union zu beobachten. Dies gilt auch dann, wenn die Daten von einer beziehungsweise einem nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiterin beziehungsweise Auftragsverarbeiter verarbeitet werden. Gerade mit Blick auf den Datenschutz im Internet ist dies von höchster Bedeutung.

2.2 Videoüberwachung

Anders als das bisherige Bundesdatenschutzgesetz (BDSG) enthält die Datenschutzgrundverordnung (DSGVO) keine spezifische Regelung für die Videoüberwachung öffentlich zugänglicher Bereiche. Allerdings bleibt das bisherige Haushaltsprivileg auch nach der DSGVO bestehen. Danach gilt die Verordnung nicht für die Verarbeitung personenbezogener Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird.

Nach Artikel 35 Absatz 3 c DSGVO ist eine Datenschutz-Folgenabschätzung im Fall einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche erforderlich. Dies ist die einzige Regelung der Datenschutzgrundverordnung, die die Videoüberwachung erwähnt. Die Rechtmäßigkeitsvoraussetzungen für eine Videoüberwachung sind nicht unmittelbar aus dieser Norm abzuleiten, da sie die Rechtmäßigkeit der Datenverarbeitung mittels optoelektronischer Vorrichtungen schon voraussetzt. Als mögliche Erlaubnisnormen für Videoüberwachungen kommen neben Einwilligungen zwei Varianten in Betracht. Es sind dies zum einen Artikel 6 Absatz 1 f DSGVO. Danach ist die Verarbeitung zur Wahrung der berechtigen Interessen der beziehungsweise des Verantwortlichen oder einer beziehungsweise eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern

überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Die andere Variante ist die Rechtmäßigkeit der Videoüberwachung nach Artikel 6 Absatz 1 e aufgrund der Erforderlichkeit für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Insoweit sind der Bundesgesetzgeber und Landesgesetzgeber befugt, für öffentliche Stellen eine erste Rechtsgrundlage zu schaffen.

Für eine Einwilligung werden die Voraussetzungen des Artikels 7 DSGVO bei einer Videoüberwachung nur in Einzelfällen in Betracht kommen. Jedenfalls ist auch künftig eine "konkludente" Einwilligung, die aus dem bloßen Betreten von videoüberwachten Bereichen nach Kenntnisnahme der Hinweisbeschilderung hergeleitet wird, nicht ausreichend. Eine Abweichung von der bisherigen Praxis ergibt sich nach unserer Einschätzung für den Bereich der Videoüberwachung aus der Datenschutzgrundverordnung nicht. Die Rechtmäßigkeitsvoraussetzungen nach Artikel 6 Absatz 1 f DSGVO folgen im Wesentlichen den bereits aus dem Bundesdatenschutzgesetz (§ 6 b, § 28 Absatz 1 Satz 1 Nummer 2) bekannten Kriterien der Wahrung berechtigter Interessen, der Erforderlichkeit und der Interessenabwägung. Neu ist der Umstand, dass eine Verarbeitung zukünftig auch zur Wahrung berechtigter Interessen eines Dritten möglich ist. Auch hinsichtlich des "berechtigten Interesses" kann der bisherigen Auslegung auch künftig gefolgt werden, da sich auch aus den Erwägungsgründen der Datenschutzgrundverordnung keine Anhaltspunkte ergeben, die eine neue Bewertung dieses Tatbestandsmerkmals erfordern. Zur Erforderlichkeit ist festzuhalten, dass eine Videoüberwachung zur Verfolgung präventiver Zwecke – wie bisher – mittels Monitoring und interventionsbereitem Personals erfolgen muss.

Bei der Interessenabwägung ergibt sich aus dem entsprechenden Erwägungsgrund der Datenschutzgrundverordnung eine Relativierung des bisher verfolgten strikt objektiven Ansatzes, da nunmehr die "vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen" sind. Ob "vernünftige" Erwartungen bestehen, beurteilt sich laut Erwägungsgrund 47 danach, ob "die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert ist oder eventuell wegen eines Beziehungszusammenhangs sogar verlangt wird" oder eben nicht. Entscheidend wird hier die Vorerwartung einer oder eines durchschnittlichen Betroffenen sein. Es wird jedoch noch zu klären sein, ob die "vernünftigen Erwartungen" auf nationaler oder europäischer Ebene maßgebend sein werden, da diese durchaus gravierend voneinander abweichen können. In die Interessenabwägung muss zudem einfließen, dass die Datenschutzgrundverordnung die "systematische umfangreiche" Videoüberwachung in Artikel 35 Absatz 3 c DSGVO als risikoreich ansieht und deshalb eine Folgenabschätzung für erforderlich hält. Erwähnenswert ist in diesem Zusammenhang, dass durch Artikel 6 Absatz 1 f DSGVO besonders die schutzwürdigen Interessen von Kindern betont werden.

Dieser Aspekt wird bei der Bewertung einer Videoüberwachung besonders zu berücksichtigen sein.

Eine Videoüberwachung im öffentlichen Interesse dürfte insbesondere im öffentlichen Personennahverkehr in Frage kommen, da hier eine Aufgabe der Daseinsvorsorge erfüllt wird. Hierbei ist es unerheblich, ob die Betreiberin beziehungsweise der Betreiber eine öffentliche Stelle oder ein Privatunternehmen ist.

Eine Verarbeitung biometrischer Daten ist grundsätzlich nach Artikel 9 Absatz 1 DSGVO untersagt. Allein der Umstand, dass auf Videobildern Gesichter erhoben werden, ist allerdings noch nicht als biometrisches Datum zu betrachten, es sei denn, dies ist mit einer besonderen technischen Auswertungsmöglichkeit verbunden.

Eine konkret auf Videoüberwachung bezogene Regelung zur Speicherdauer sowie Löschung enthält die DSGVO nicht. Nach der DSGVO sind personenbezogene Daten zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Unter zusätzlicher Berücksichtigung der in der DSGVO getroffenen Regelungen zur Datenminimierung sowie zur Speicherbegrenzung, kann es nach unserer Einschätzung daher bei der bisher nach dem BDSG geübten Praxis bleiben.

Was die Erkennbarkeit von Videoüberwachungsmaßnahmen anbelangt, sind die Transparenzpflichten und die sich daran anschließenden Widerspruchsrechte der Datenschutzgrundverordnung ein starkes Instrument zur Verteidigung der Betroffenenrechte. Da die Einhaltung des Informationskatalogs in Artikel 13 DSGVO auch bei einer Videoüberwachung angemessen und damit adressatengerecht umzusetzen ist, stellt sich die Frage, wie dies realisiert werden kann. Als Mindestanforderungen nach der DSGVO sind die folgenden Angaben zu machen: Piktogramm (Kamerasymbol), Name des Verantwortlichen einschließlich Kontaktdaten, Dauer der Speicherung (für viele Betroffene besonders interessant), in Schlagworten Zweck und Rechtsgrundlage der Videoüberwachung und Hinweis auf Zugang zu den weiteren Pflichtinformationen gemäß Artikel 13 Absatz 2 DSGVO wie Auskunftsrecht, Beschwerderecht, zum Beispiel im Internet, Infoblatt im Laden.

Nach unserem jetzigen Wissenstand bildet Artikel 6 Absatz 1 f DSGVO die maßgebliche Rechtsgrundlage für die Zulässigkeit einer Videoüberwachung. Im Vergleich zu § 6 b BDSG sind hier in Bezug auf die berechtigten Interessen und die Erforderlichkeit keine wesentlichen Unterschiede festzustellen, wohl aber bezüglich der Interessenabwägung.

Unserer Auffassung nach entsprechen die bisher von den datenschutzrechtlichen Aufsichtsbehörden zur Videoüberwachung vertretenen Positionen den Anforderungen der Datenschutzgrundverordnung.

2.3 Telemedien

Die Datenschutzgrundverordnung (DSGVO) trat am 24. Mai 2016 in Kraft und gilt ab dem 25. Mai 2018. Wie in diesem Bericht bereits beschrieben, wird die DSGVO den Datenschutz in Deutschland nachhaltig verändern. So auch das Telemedienrecht.

Das Datenschutzrecht für Telemedien als sektorspezifische Spezialregelung nach § 1 Absatz 3 Bundesdatenschutzgesetz (BDSG) regelt gegenwärtig mit dem Telemediengesetz, bis auf einige Ausnahmen, die elektronischen Informationsdienste und Kommunikationsdienste. Neben den allgemeinen Bestimmungen werden die Zulassungsfreiheit, die Informationspflichten und Bußgeldvorschriften geregelt. Den Kern des Telemediengesetzes bildet allerdings der Abschnitt "Datenschutz", der als Besonderheit eine Abgrenzung und Trennung von Bestandsdaten und Nutzungsdaten vorsieht und sich damit allerdings nicht auf die gegebenenfalls auch gespeicherten Inhaltsdaten bezieht. Die Verarbeitung von Inhaltsdaten richtet sich nach dem Bundesdatenschutzgesetz oder auch anderen speziellen Datenschutznormen. Eine Abgrenzung zwischen den Datenarten und zwischen den einschlägigen Gesetzen gestaltete sich in der Praxis zuletzt teilweise schwierig, wenn es beispielsweise um Datenübermittlungen im Zusammenhang mit Cloud-Verarbeitungsdiensten geht oder ermittelt werden soll, welche Unterschiede zwischen einer klassischen SMS (Short Message Service, Kurznachrichtendienst) und einer Kurznachricht über einen der internationalen Messenger-Dienste bestehen. Momentan fallen die Diensteanbieter der Messenger-Dienste nicht unter die strengeren Regelungen für Telekommunikationsanbieter.

Ab Mitte 2018 gilt die Datenschutzgrundverordnung. Damit werden voraussichtlich alle Regelungen des Telemediengesetzes verdrängt, sofern diese nicht auf der e-Privacy-Richtlinie (Richtlinie 2002/58/EG) oder der Cookie-Richtlinie (Richtlinie 2009/136/EG) beruhen. Die techniknahe Unterscheidung zwischen Bestandsdaten, Nutzungsdaten und Inhaltsdaten fällt damit voraussichtlich weg.

Bei der Betrachtung der neuen Regelungen aus unserer Perspektive als Datenschutzaufsichtsbehörde fällt zunächst auf, welche etablierten Regelungen durch die DSGVO aufgehoben werden. So die eben beschriebene Trennung der Datenarten, aber auch zum Beispiel sehr konkrete Regelungen für die Zwischenspeicherung zur beschleunigten Übermittlung von Informationen. Auf der anderen Seite sind in den fast 100 Artikeln der DSGVO auch Regelungen enthalten, die ihrerseits äußerst positive Auswirkungen auf das Datenschutzrecht für Telemedien haben. So gilt das europäische Datenschutzrecht danach nicht nur für die in der Europäischen Union niedergelassenen Unternehmen, sondern auch für solche Unternehmen, die ein Angebot an einen bestimmten

nationalen Markt in der Europäischen Union richten oder solche Datenverarbeitungen, die dazu dienen, das Verhalten von Personen in der Europäischen Union zu beobachten.

Auch inhaltlich lesen sich die neuen Regelungen mit Perspektive auf das Telemedienrecht zunächst innovativ. Hier ist flankierend für die Telemedien das Recht auf Datenübertragbarkeit zu sehen. Es muss sich zeigen, ob es dadurch auf einfache Weise möglich wird, von einem Online-Shop zu einem Anderen oder von einem sozialen Netzwerk zu einem Anderen zu wechseln und welche Daten portiert werden (können). Im Rückblick auf die dann voraussichtlich abgelöste Unterscheidung zwischen Bestandsdaten, Nutzungsdaten und Inhaltsdaten stellt sich dann aber die Frage, auf welche Datenkategorien sich die Übermittlung bezieht, wie diese Portabilität in der Praxis technisch umgesetzt wird und ob es eventuell eine Wahlmöglichkeit für die Betroffenen bezüglich der Datenkategorien gibt.

Auch das Recht auf "Vergessenwerden", also Löschung, wurde konkretisiert. In der Praxis bezieht sich das durch den Europäischen Gerichtshof in einer Klage gegen Google erstmals angewandte Prinzip bisher lediglich auf Suchmaschinenbetreiber. Fortan wird es auch für alle gewerblichen Internetseitenbetreiber gelten. Bei einer Ausübung des Rechts muss damit nicht nur die Quelle gelöscht werden, sondern es müssen auch in angemessener Weise Dritte über das Löschbegehren informiert werden, denen die Daten zwischenzeitlich übermittelt wurden. Der Versuch, die Hoheit über die eigenen Daten zurück in die Hände der Betroffenen zu geben, muss in Zukunft wahrscheinlich gründlich mit den praktischen Aufwänden für eine solche Maßnahme abgewogen werden.

Diese Aufzählung ließe sich sicher noch weiter fassen, zum Beispiel durch die Besonderheiten bei der Verarbeitung der Daten von Kindern und bei Diensten, die (auch) Kindern im Internet angeboten werden oder durch die neu formulierten Informationspflichten, die bei Telemedien starke Auswirkungen auf das jeweilige Impressum und auf die Datenschutzerklärungen haben dürften. Die Anwendung der DSGVO auf Telemedien und auch die eventuelle Umgestaltung des Telemediengesetzes gehört deshalb wohl zu den spannendsten und in Zukunft sicher heiß diskutierten Feldern des neuen Datenschutzrechts in Europa.

2.4 Auskunfteientätigkeit

Im Bundesdatenschutzgesetz finden sich insbesondere seit einer Gesetzesnovellierung im Jahr 2010 einige Vorschriften, die als solche ausdrücklich die Datenverarbeitungstätigkeit beziehungsweise bestimmte Teilbereiche dieser Tätigkeit sogenannter Wirtschaftsauskunfteien insbesondere zur Kreditwürdigkeitseinschätzung von Personen regeln. So ist beispielsweise festgelegt, unter welchen Voraussetzungen Informationen über

offene Forderungen an Auskunfteien gemeldet werden dürfen. Des Weiteren ist das sogenannte Scoring, also die Erstellung von Wahrscheinlichkeitseinschätzungen zum künftigen Zahlungsverhalten oder einer sonstigen künftigen Verhaltensweise von Personen, normiert und an einige wenige Zulässigkeitsvoraussetzungen geknüpft. Wenngleich diese Regelungen im Bundesdatenschutzgesetz gemessen an dem Ziel eines effektiven Schutzes des Persönlichkeitsrechts zum Teil durchaus erhebliche Mängel aufweisen, sorg(t)en sie doch immerhin für eine gewisse Rechtssicherheit.

Demgegenüber enthält die ab Mai 2018 anwendbare Datenschutzgrundverordnung (DSGVO) keine Sondervorschriften zur Regelung der Datenverarbeitungstätigkeit von Wirtschaftsauskunfteien. Auskunfteibezug hat im Wesentlichen allein eine Bestimmung, die das sogenannte Profiling als Erstellung von Persönlichkeits(aspekt)einschätzungen durch rein automatisierte Datenauswertung definiert und damit das Scoring umfasst. Zum Profiling finden sich sodann in der Datenschutzgrundverordnung an verschiedenen Stellen, insbesondere auch in den allgemeinen Erwägungsgründen zum Rechtstext, weitere Festlegungen.

Um das bisherige Maß an Rechtssicherheit zu erhalten beziehungsweise die angesichts des Fehlens auskunfteispezifischer Bestimmungen in der Datenschutzgrundverordnung ab dem Jahr 2018 für eine Übergangszeit mögliche partielle Rechtsunsicherheit hinsichtlich nunmehr zulässiger Datenverarbeitungstätigkeiten der Auskunfteien zu vermeiden, ist die Bundesregierung bemüht, in dem erforderlichen nationalen Umsetzungsgesetz zur Datenschutzgrundverordnung die bisherigen, eingangs genannten Regelungen des Bundesdatenschutzgesetzes zur Auskunfteientätigkeit aufrechtzuerhalten (siehe hierzu Ziffer 1.2.2, insbesondere Ziffer 1.2.2.3). Wenngleich dieses Ziel durchaus nachvollziehbar ist, ist die Befugnis für eine solche Aufrechterhaltung der bisherigen Vorschriften des Bundesdatenschutzgesetzes europarechtlich äußerst fragwürdig. Hinzu kommt, dass die Bundesregierung um des Ziels der Aufrechterhaltung der bisherigen Rechtssicherheit willen offenkundig auch bereit ist, die selbst in einem von ihr beauftragten Rechtsgutachten konstatierten und zudem auch öffentlich bekannten schwerwiegenden Regelungsdefizite des bisherigen Scoring-Paragrafen im Bundesdatenschutzgesetz zulasten des Persönlichkeitsrechts jeder Bürgerin und jeden Bürgers bestehen zu lassen. Der weitere Verlauf des Gesetzgebungsverfahrens zum nationalen Umsetzungsgesetz zur Datenschutzgrundverordnung bleibt abzuwarten.

2.5 Richtlinie zu europäischem Datenschutzstandard für Justiz und Polizei

Im April 2016 wurde die europäische Richtlinie "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 und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates" (im Folgenden Richtlinie) verabschiedet. Sie verpflichtet die Bundesrepublik Deutschland zur Umsetzung ihrer Bestimmungen in deutsches Recht bis zum Mai 2018. Diese Richtlinie soll erstmalig in den Bereichen Polizei und Justiz eine Datenschutz-Mindestharmonisierung innerhalb der Europäischen Union herbeiführen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat sich mit Empfehlungen und Hinweisen zur Umsetzung dieser Richtlinie geäußert.

Eine Vielzahl von bundesrechtlichen und landesrechtlichen Regelungen ist am Maßstab dieser europäischen Richtlinie zu überprüfen und gegebenenfalls unter Beibehaltung des aktuellen Datenschutzniveaus anzupassen. Hierbei ist zu berücksichtigen, dass es sich bei den Vorgaben der Richtlinie um Mindestanforderungen handelt. Ziel ist danach keinesfalls eine Absenkung des Datenschutzniveaus in Staaten mit einem höheren Datenschutzniveau. Vielmehr soll die Richtlinie ein hohes Schutzniveau mit Mindeststandards in der gesamten Europäischen Union gewährleisten. Die Bundesrepublik Deutschland und damit die Gesetzgeber in Bund und Ländern können zum Schutz der Rechte und Freiheiten der Bürgerinnen und Bürger als betroffene Personen Festlegungen treffen, die strenger sind als die Schutzbestimmungen in dieser Richtlinie. Wo das deutsche Recht bereits ein höheres Schutzniveau gewährleistet, sehen wir alle Beteiligten in der Pflicht sicherzustellen, dass dieses ausnahmslos erhalten bleibt. Umsetzungsspielräume sind nach den Maßgaben des Bundesverfassungsgerichts auszufüllen.

Was ist wichtig für die Bürgerinnen und Bürger in der Freien Hansestadt Bremen? Neben den üblichen Betroffenenrechten wie Anspruch auf Information, Berichtigung oder Löschung ist in Artikel 14 der Richtlinie das Auskunftsrecht für die Bürgerinnen und Bürger verankert. Insbesondere möchten wir darauf hinweisen, dass nur begründete Zweifel an der Identität der Bürgerinnen und Bürger eine Personalausweiskopie erfordern könnten. Die Personalausweiskopie soll also eine Ausnahme bleiben. Begründete Zweifel an der Identität einer natürlichen Person dürfen nicht bei jedem Auskunftsbegehren pauschal angenommen werden, sondern die Verdachtsmomente, die den Zweifel an der Identität der natürlichen Person begründen, sind zu dokumentieren. Das generelle Erfordernis einer beglaubigten Kopie des Bundespersonalausweises an ein jedes Auskunftsersuchen zu stellen, ist eine nicht hinnehmbare Hürde zur Wahrnehmung des Auskunftsrechts im Rahmen dieser Richtlinie und stellt eine Einschränkung des Auskunftsrechts dar. Das Auskunftsrecht der Bürgerinnen und Bürger darf nicht durch einen Generalverdacht auf Identitätstäuschung der Auskunftsersuchenden konterkariert werden. Allein Artikel 15 der Richtlinie schränkt dieses Auskunftsrecht ein, indem er neben dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit (teilweise oder vollständige Einschränkung, "soweit und so lange") die abschließende Aufzählung von einschränkenden Zwecken in Artikel 15 Absatz 1 der

Richtlinie beachtet. Bei einer Einschränkung oder Verweigerung der Auskunft können sich die Bürgerinnen und Bürger als betroffene Personen an die Landesbeauftragte für Datenschutz und Informationsfreiheit wenden, der nach Artikel 17 der Richtlinie die uneingeschränkte Auskunft zu gewähren ist, um die Prüfung darüber zu ermöglichen, ob die Einschränkung oder Verweigerung der Auskunft gegenüber den Betroffenen rechtmäßig sind.

Zum Zwecke einer einheitlichen Umsetzung empfehlen wir, auch für den Bereich, der nicht unter die Datenschutzgrundverordnung (DSGVO) fällt, unter Beachtung der Gesetzgebungskompetenzen von Bund und Ländern allgemeine Bestimmungen wie Anforderungen an die Datensicherheit oder unsere Befugnisse als Aufsichtsbehörde in einem neuen allgemeinen Datenschutzrecht zu regeln, anstatt jeweils bereichsspezifische Umsetzungsvorschriften zu erlassen.

3. Bremische Bürgerschaft – Ergebnisse der Beratungen des 38. Jahresberichts

Bericht und Beschlussempfehlung des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zum 38. Jahresbericht der Landesbeauftragten für Datenschutz vom 10. März 2016 (Drucksache 19/330) und zur Stellungnahme des Senats vom 30. August 2016 (Drucksache 19/718)

I. Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 20. April 2016 den 38. Jahresbericht der Landesbeauftragten für Datenschutz vom 10. März 2016 (Drucksache 19/330) und in ihrer Sitzung am 21. September 2016 die dazu erfolgte Stellungnahme des Senats vom 31. August 2016 (Drucksache 19/718) an den Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Beratung und Berichterstattung.

Der Ausschuss stellte bei den nachfolgend aufgeführten Punkten des 38. Jahresberichts Beratungsbedarf fest:

Ziffer 3.3 Bestellung behördlicher Datenschutzbeauftragter durch die Ortsämter

Ziffer 3.4 Bestellung behördlicher Datenschutzbeauftragter durch die Regionalen Beratungs- und Unterstützungszentren (ReBUz)

Ziffer 4.2 Länderübergreifende Zusammenarbeit im IT-Bereich

Ziffer 4.3 SAP-Verfahren in Bremen

Ziffer 5.2 Einsatz der BodyCam bei der Polizei Bremen

Ziffer 5.4 Prüfung der Falldatei Rauschgift

Ziffer 5.10 Behördlicher Datenschutzbeauftragter und Verfahren im Stadtamt

Ziffer 5.11 Zuverlässigkeitsprüfung der Gewerbebehörde bei Bewachungspersonal

Ziffer 5.12 Namensverwechslung beim Stadtamt

Ziffer 8.1 Datenbank Haaranalysen im Amt für Soziale Dienste

Ziffer 8.3 Fachverfahren OK.JUG des Amtes für Soziale Dienste

Ziffer 10.2 Datenschutzbeschwerden zum Beitragsservice

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

In seiner Sitzung am 30. November 2016 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für Datenschutz und 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.

Die Bestellung behördlicher Datenschutzbeauftragter ist zwischenzeitlich sowohl bei den Ortsämtern als auch bei den Regionalen Beratungs- und Unterstützungszentren (ReBUz) erfolgt (Ziffern 3.3 und 3.4). Für alle Ortsämter wurde ein gemeinsamer Datenschutzbeauftragter bestellt, der bei der Senatskanzlei angesiedelt ist. Für die ReBUz wurde ebenfalls eine zentrale Lösung gewählt, in dem der Datenschutzbeauftragte der Senatorin für Kinder und Bildung diese Aufgabe künftig mit übernimmt. Nach der Umstrukturierung des Stadtamts ist geplant, einen zentralen Datenschutzbeauftragten beim Innenressort zu installieren, der für alle Geschäftsbereiche zuständig sein wird (Ziffer 5.10).

Ferner ist dem Ausschuss berichtet worden, dass bei der Datenbank Haaranalysen im Amt für Soziale Dienste (Ziffer 8.1) der Auftrag für die Erstellung eines Datenschutzkonzepts inzwischen extern vergeben worden ist und nach Fertigstellung des Konzepts eine neue Datenbank in Auftrag gegeben wird. Zum Fachverfahren OK.JUG (Ziffer 8.3) des Amtes für Soziale Dienste hat der Ausschuss zur Kenntnis genommen, dass dieses künftig durch ein neues Fachverfahren abgelöst wird. Bei der Leistungsbeschreibung für das neue Verfahren sind alle datenschutzrechtlichen Hinweise der Landesbeauftragten berücksichtigt worden.

Bezüglich der Datenschutzbeschwerden zum Beitragsservice (Ziffer 10.2) ist dem Ausschuss dargelegt worden, dass sich der geschilderte Fall erledigt hat. Grundsätzlich ist zum häufig kritisierten Meldedatenabgleich festzustellen, dass dieser staatsvertraglich geregelt und rechtlich zulässig ist, was die Gerichte bestätigt haben. Dem Gebot der Datensparsamkeit wird durch die Aussetzung der Möglichkeit des Adressdatenankaufs bei privaten Adresshändlern sowie der Vermieterauskunft bis zum Jahre 2020 grundsätzlich entsprochen.

Zu den datenschutzrechtlich relevanten Themen aus dem Bereich Inneres ist dem Ausschuss berichtet worden, dass es für den Einsatz der BodyCam (Ziffer 5.2) bei der Polizei Bremen inzwischen eine Rechtsgrundlage gibt, die auch mit der Landesbeauftragten abgestimmt worden ist. Der Ausschuss wird sich im Rahmen der Evaluierung des Pilotversuchs erneut mit den datenschutzrechtlichen Aspekten des Einsatzes der BodyCam beschäftigten.

Hinsichtlich der Falldatei Rauschgift (Ziffer 5.4) hat der Ausschuss zur Kenntnis genommen, dass die geschilderten Probleme im Bereich des Datenschutzes bundesweit auftreten. Da die Falldatei Rauschgift jedoch demnächst durch ein neues System abgelöst wird, wird an den bestehenden Problemen derzeit nicht weiter gearbeitet. Der Ausschuss erwartet, dass für das neue System ein datenschutzkonformes Löschkonzept vorgelegt und das Problem der Protokollierung gelöst wird.

Bei der Zuverlässigkeitsprüfung beim Bewachungspersonal (Ziffer 5.11) hat die Gewerbebehörde zugesagt, das beanstandete Einwilligungsmodell nicht fortzuführen. Anhaltspunkte dafür, dass die Behörde unzulässige Erkundigungen über die politische Gesinnung der Bewerber/innen einholt, haben sich nach Aussage der Landesbeauftragten nicht ergeben. Es ist auch nicht davon auszugehen, dass über die gesetzlich geregelten Fälle hinaus Abfragen beim Verfassungsschutz erfolgen.

Im Hinblick auf die länderübergreifende Zusammenarbeit im IT-Bereich (Ziffer 4.2) hat der Ausschuss zur Kenntnis genommen, dass es hier noch einige Themenbereiche gibt, die zwischen der Senatorin für Finanzen und der Landesbeauftragten kontrovers diskutiert werden und für die noch keine für beide Seiten zufriedenstellende Lösung gefunden werden konnte.

Der Ausschuss hat insbesondere die Problematik der sogenannten gemeinsamen Verfahren und der lesenden Zugriffe auf Kalender und Emailinhalte intensiv erörtert und sich die unterschiedlichen Standpunkte erläutern lassen.

Der Ausschuss kritisiert erneut, dass sowohl bei der länderübergreifenden Zusammenarbeit im IT-Bereich als auch bei den SAP-Verfahren (Ziffer 4.3) oftmals die Dokumentenlage nur unvollständig ist und Konzepte nicht (rechtzeitig) vorgelegt werden. Die Kritik hat der Ausschuss bereits in den vergangenen Berichtsjahren mehrfach geäußert und appelliert auch dieses Mal wieder ein die senatorische Dienststelle, Abläufe hier künftig besser zu gestalten.

II. Beschlussempfehlung

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

4. Behördliche Beauftragte für den Datenschutz

4.1 Bestellung behördlicher Datenschutzbeauftragter durch die Gesellschaften

Die Behörden und sonstigen öffentlichen Stellen des Landes, der Gemeinden und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen sind nach dem Bremischen Datenschutzgesetz ungeachtet ihrer Rechtsform zur Bestellung einer beziehungsweise eines behördlichen Datenschutzbeauftragten verpflichtet. Die Pflicht zur Bestellung gilt darüber hinaus auch für Personen oder Stellen, die außerhalb des öffentlichen Bereichs Aufgaben der öffentlichen Verwaltung wahrnehmen und insoweit öffentliche Stellen im Sinne des Bremischen Datenschutzgesetzes sind. Hieraus ergibt sich unter anderem, dass auch Gesellschaften, die mit Aufgaben der öffentlichen Verwaltung betraut sind, ungeachtet ihrer Rechtsform behördliche Datenschutzbeauftragte zu bestellen haben. In Bremen und Bremerhaven gibt es bereits seit längerer Zeit eine Vielzahl von Gesellschaften auch in privater Rechtsform, die mit Aufgaben des Landes oder der Stadtgemeinden betraut sind. Wiederholt mussten wir feststellen, dass bei den Gesellschaften Unkenntnisse oder Unsicherheiten hinsichtlich der Anwendung des Bremischen Datenschutzgesetzes und damit auch der Verpflichtung zur Bestellung einer oder eines behördlichen Datenschutzbeauftragten bestehen.

So meldete uns im Berichtsjahr eine mit öffentlichen Aufgaben des Landes Bremen betraute Gesellschaft mit beschränkter Haftung die Beendigung der Übertragung des Amtes an den bisherigen Funktionsinhaber und die Bestellung eines neuen externen Datenschutzbeauftragten. Während die Meldung nach dem Bremischen Datenschutzgesetz

erfolgte, wurde als Rechtsgrundlage für die Abberufung und die Neubestellung von der Gesellschaft fälschlicherweise jeweils das Bundesdatenschutzgesetz genannt. Auch ging aus dem Bestellschreiben hervor, dass die Gesellschaft davon ausging, dass sich die Aufgaben des neuen Amtsinhabers aus dem Bundesdatenschutzgesetz, nicht aber aus dem Bremischen Datenschutzgesetz ergäben, wie es der Rechtslage entsprochen hätte. Der zwischen der Gesellschaft und dem neuen Datenschutzbeauftragten abgeschlossene Dienstleistungsvertrag orientierte sich ebenfalls an den Bestimmungen des Bundesdatenschutzgesetzes. Auf unsere Hinweise zu der zu beachtenden Rechtslage und unsere diesbezüglichen Änderungsempfehlungen passte die betreffende Gesellschaft das Abberufungsschreiben des bisherigen und das Bestellschreiben des neuen Datenschutzbeauftragen sowie den Vertrag an die Bestimmungen des Bremischen Datenschutzgesetzes an.

In einem ähnlichen Fall, der die Bestellung eines neuen ebenfalls externen Datenschutzbeauftragten durch eine Gesellschaft mit beschränkter Haftung betraf, stellten wir fest, dass die Gesellschaft sowohl Aufgaben als nicht öffentliche wie auch als öffentliche Stelle wahrnimmt. Auch ihr waren öffentliche Aufgaben des Landes Bremen übertragen worden. Die Abberufung und die Neubestellung der beziehungsweise des Datenschutzbeauftragten finden in solchen Fällen ihre Rechtsgrundlage sowohl im Bremischen Datenschutzgesetz als auch im Bundesdatenschutzgesetz. Die Datenverarbeitung zur Wahrnehmung der öffentlichen Aufgaben einschließlich der Bestellung der oder des Datenschutzbeauftragten in Verbindung hiermit richtet sich nach dem Bremischen Datenschutzgesetz, die Erfüllung nicht öffentlicher Aufgaben einschließlich der Bestellung einer beziehungsweise eines Datenschutzbeauftragten für diesen Bereich richtet sich nach dem Bundesdatenschutzgesetz. Im Abberufungsschreiben und im Bestellschreiben sowie im Dienstleistungsvertrag mussten die zu beachtenden Rechtsgrundlagen nebeneinander aufgeführt werden, was letztlich geschah.

Alle Gesellschaften, die öffentliche Aufgaben wahrnehmen, müssen also ungeachtet ihrer Rechtsform prüfen, ob sie neben oder anstelle betrieblicher Datenschutzbeauftragter auch eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen müssen.

Auch nach Artikel 37 der Europäischen Datenschutzgrundverordnung müssen Behörden oder öffentliche Stellen, die personenbezogene Daten verarbeiten, künftig eine Datenschutzbeauftragte oder einen Datenschutzbeauftragen bestellen. Da die Datenschutzgrundverordnung den Begriff der "öffentlichen Stelle" nicht selbst definiert, sollte der bremische Gesetzgeber klarstellend an der jetzigen Formulierung des § 1 Absatz 2 Satz 2 festhalten, die lautet: "Nimmt eine Person oder Stelle außerhalb des öffentlichen

Bereichs Aufgaben der öffentlichen Verwaltung wahr, so ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes."

4.2 Senator für Inneres

Nach dem Bremischen Datenschutzgesetz können mehrere Stellen gemeinsam eine oder einen Beauftragten für den Datenschutz bestellen, wenn dadurch die Aufgabenerfüllung nicht beeinträchtigt wird. Der Senator für Inneres informierte uns über im Rahmen des Ressortprojekts "Zentralisierung von Querschnittsaufgaben" entwickelte Planungen, für die dem Ressort zugeordneten Dienststellen eine zentrale behördliche Datenschutzbeauftragte oder einen zentralen behördlichen Datenschutzbeauftragter zu bestellen. Bislang wurden die Aufgaben der beziehungsweise des Datenschutzbeauftragten in der senatorischen Behörde und den ihr nachgeordneten Dienststellen dezentral wahrgenommen. Die betreffenden Behördenleitungen verständigten sich darauf, die zentrale beziehungsweise den zentralen Datenschutzbeauftragten beim Senator für Inneres anzusiedeln. Im Juli des Berichtsjahres wurde diese Stelle als Vollzeitstelle im Ressort des Senators für Inneres im Rahmen eines Interessenbekundungsverfahrens ausgeschrieben. Die Bestellung der Stelle soll im Januar 2017 erfolgen.

Wir wiesen in diesem Zusammenhang darauf hin, dass die sich aus dem Gesetz für jede einzelne Dienststelle des Ressorts ergebenden Verantwortlichkeiten für personenbezogene Datenverarbeitungen auch bei der Bestellung einer oder eines zentralen behördlichen Datenschutzbeauftragten bestehen bleiben. Die Person, die die zentrale Beauftragtenfunktion wahrnimmt, muss von den einzelnen Dienststellen zur oder zum behördlichen Datenschutzbeauftragten ernannt werden. Dabei muss es jeder Dienststelle frei stehen, eine andere Person zu bestellen. Auch muss sichergestellt sein, dass die beziehungsweise der zentrale behördliche Datenschutzbeauftragte weisungsfrei tätig werden kann. Ihre beziehungsweise seine Aufgaben ergeben sich direkt aus dem Bremischen Datenschutzgesetz. Eine Aufgabenzuweisung durch die Dienststellenleitungen ist deshalb mit der notwendigen Unabhängigkeit der Amtsinhaberin beziehungsweise des Amtsinhabers nicht zu vereinbaren. Die oder der zentrale Beauftragte muss direkt der jeweiligen Behördenleitung unterstehen, die direkte Ansprechpartnerin sein muss. Zur Amtswahrnehmung müssen der oder dem Beauftragten Überprüfungen der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme in den einzelnen Dienststellen unangemeldet möglich sein. Außerdem muss die oder der zentrale Datenschutzbeauftragte bei der Aufgabenerfüllung von allen Dienststellen, die sie oder ihn bestellt haben, unterstützt werden. Sie oder er muss von den Mitarbeiterinnen und Mitarbeitern der einzelnen Dienststellen direkt schriftlich oder mündlich kontaktiert werden können. Ein Umweg, zum Beispiel über die Behördenleitung, darf nicht vorgesehen sein.

Auch hinsichtlich der Beendigung der Funktion der oder des zentralen behördlichen Datenschutzbeauftragten gilt, dass die Bestellung nur in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches widerrufen werden kann. Darüber hinaus ist die Beendigung der Amtsübertragung durch die Dienststellen nur mit dem freiwilligen Einverständnis der Amtsinhaberin oder des Amtsinhabers zulässig.

Die genannten Anforderungen entsprechen weitgehend denjenigen der Europäischen Datenschutzgrundverordnung. Eine Abweichung ergibt sich allerdings beim Abberufungsschutz der Datenschutzbeauftragten: Nach Artikel 38 Absatz 3 Satz 2 Datenschutzgrundverordnung darf die oder der Datenschutzbeauftragte wegen der Erfüllung ihrer beziehungsweise seiner Aufgaben nicht abberufen werden, wohingegen nach § 7 a Absatz 3 Satz 4 Bremisches Datenschutzgesetz die Bestellung behördlicher Datenschutzbeauftragter nur in entsprechender Anwendung des § 626 Bürgerliches Gesetzbuch widerrufen werden kann.

Der Senator für Inneres wird uns über die weitere Entwicklung des Vorhabens auf dem Laufenden halten. Dabei wird auch zu prüfen sein, ob es einer einzigen Person möglich ist, die Funktion der oder des behördlichen Datenschutzbeauftragten dienstellenübergreifend im Ressort des Senators für Inneres mit einer Vielzahl unterschiedlichster Datenverarbeitungsverfahren mit personenbezogenen Verarbeitungen wahrzunehmen.

4.3 Treffen der behördlichen Datenschutzbeauftragten

Die behördlichen Datenschutzbeauftragten aus Bremen und Bremerhaven trafen sich auch im Berichtsjahr, um aktuelle Themen des Datenschutzes zu erörtern und sich über die bei ihrer Tätigkeit gesammelten Erfahrungen auszutauschen.

Schwerpunktmäßig befassten sich die Datenschutzbeauftragten bei ihrem Treffen im Frühjahr, an dem auch zwei Mitarbeiter des IT-Referats der Senatorin für Finanzen teil nahmen, mit dem Thema "IT-Sicherheit in der Verwaltung". Bei der Senatorin für Finanzen wird zurzeit ein aktuelles IT-Sicherheitskonzept für die bremische Verwaltung erarbeitet. Mit der Erstellung des Konzepts sind zahlreiche Datenschutzfragen verbunden, deren Lösung über die bremische Verwaltung hinaus auch in vielen anderen Verwaltungen für den IT-Einsatz von Bedeutung ist. In der Veranstaltung bildete sich eine Arbeitsgruppe der Datenschutzbeauftragten, die sich die Überprüfung der Datenverarbeitung durch die Anstalt öffentlichen Rechts Dataport zur Aufgabe gemacht hat (siehe auch Punkt 4.4 dieses Berichts).

Im Herbsttreffen befassten sich die Datenschutzbeauftragten aus der bremischen Verwaltung schwerpunktmäßig mit der vorgesehenen Prüfung bei Dataport. Im Rahmen dieses Treffens, das ebenfalls mit Beteiligung des IT-Referats der Senatorin für Finanzen

stattfand, stellte der IT-Sicherheitsbeauftragte von Dataport die dort für die Datenverarbeitung getroffenen Sicherheitsmaßnahmen und die Gegebenheiten für eine Überprüfung der Datenverarbeitung von Dataport durch die behördlichen Datenschutzbeauftragten vor.

Darüber hinaus nutzten die teilnehmenden Datenschutzbeauftragten die Treffen, um über ihre Tätigkeit in den zurückliegenden Monaten zu berichten und sich hieraus ergebende Fragen miteinander zu diskutieren. In zunehmendem Maße erörtert wurden auch Fragen, die die Umsetzung der Europäischen Datenschutzgrundverordnung betreffen. Weitere Treffen der behördlichen Datenschutzbeauftragten sind für das Jahr 2017 beabsichtigt.

4.4 Arbeitsgruppe "Prüfung bei Dataport"

Die behördlichen Datenschutzbeauftragten haben nach dem Bremischen Datenschutzgesetz die Aufgabe, auf die Einhaltung der Vorschriften des Gesetzes und anderer Vorschriften über den Datenschutz hinzuwirken. Insbesondere haben sie die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen. Zu den Überwachungsaufgaben gehört auch die Kontrolle der personenbezogenen Datenverarbeitung, die von anderen für die öffentliche Stelle, von der sie bestellt wurden, im Rahmen einer Auftragsdatenverarbeitung durchgeführt werden. Die Anstalt öffentlichen Rechts Dataport verarbeitet als Auftragsdatenverarbeiterin in großem Umfang personenbezogene Daten für die Behörden der Freien Hansestadt Bremen. Aus dieser Konstellation ergeben sich für viele behördliche Datenschutzbeauftragte der bremischen Verwaltung zahlreiche Fragen auch im Hinblick darauf, wie sie bei Dataport prüfend tätig werden können.

Bei einem Treffen der behördlichen Datenschutzbeauftragten im Frühjahr des Berichtsjahres bildete sich aus dem Kreis der Betroffenen eine Arbeitsgruppe, die sich die datenschutzrechtliche Überprüfung der Datenverarbeitung durch Dataport zur Aufgabe gemacht hat (siehe auch Ziffer 4.3 dieses Berichts). An dieser Arbeitsgruppe sind das IT-Referat der Senatorin für Finanzen und die Landesbeauftragte für Datenschutz und Informationsfreiheit unterstützend beteiligt. Auf Einladung der Arbeitsgruppe nahm am Treffen der behördlichen Datenschutzbeauftragten im Herbst der IT-Sicherheitsbeauftragte von Dataport teil, um die Teilnehmerinnen und Teilnehmer der Veranstaltung über das Unternehmen und seine Tätigkeit zu informieren. Der nächste Schritt wird die Überprüfung der mit Dataport abgeschlossenen Datenverarbeitungsaufträge sein.

5. Verwaltungsübergreifende Verfahren

5.1 SAP-Einheitskreditor / Einheitsdebitor

Im Berichtsjahr wurde uns zum Themenkomplex SAP keines der in den letzten drei Berichten (vergleiche zuletzt 38. Jahresbericht, Ziffer 4.3) bemängelten Konzepte vorgelegt. Auch das Projekt zur kontinuierlichen Anpassung und Aktualisierung der Dokumentenlage zu SAP und deren Umsetzung wurde nicht gestartet.

Trotz unzureichender Dokumentenlage soll die Nutzung des Verfahrens SAP einer wesentlichen Änderung unterzogen werden: Im Sinne des Trennungsgebotes wurden bisher für jeden Zweck einzelne Stammdatensätze (Kreditoren und Debitoren) im System angelegt, um den unautorisierten Zugriff auf aufgabenfremde personenbezogene Daten zu verhindern. In Zukunft sollen die Senatorin für Finanzen und die Landeshauptkasse über ein sogenanntes Einheitspersonenkonto auch aufgabenübergreifend auf die Daten zugreifen können. Eine entsprechende Verordnung, die dieses regeln sollte, erreichte uns im Entwurf und entspricht einem Paradigmenwechsel im Verfahren. In einer Stellungnahme stellten wir dar, dass die personenbezogenen Daten aus unserer Sicht nur einzelfallbezogen im erforderlichen Umfang verarbeitet werden dürfen. Weiterhin machten wir deutlich, dass vor der Entscheidung über die wesentliche Änderung des Verfahrens zunächst eine Risikoanalyse durchzuführen ist und die Dokumentationen, vor allem der Berechtigungen, auf den neuesten Stand gebracht werden und anschließend durch die oder den behördlichen Datenschutzbeauftragten geprüft werden müssen. Inwieweit die eingangs beschriebene Dokumentenlage die Einführung einer solchen wesentlichen Änderung behindert oder die geplante Änderung des Verfahrens vielleicht sogar zu einer bewertbaren Dokumentation führen könnte, ist aus unserer Sicht noch offen.

5.2 Länderübergreifende Zusammenarbeit im IT-Bereich

Im Berichtsjahr begann Bremen mit der Nutzung des CCMS (Community Cloud Mail System) als zentralem E-Mail-System, von dem wir im letzten Jahresbericht unter Ziffer 4.2 berichtet hatten. In diesem Artikel hatten wir Zweifel geäußert, dass beim CCMS eine vollständige Trennung der bremischen Daten von denen der anderen Dataport-Trägerländer gegeben ist. Mitte des Jahres erhielten wir von der Senatorin für Finanzen eine umfangreiche und aktualisierte Dokumentation zum CCMS. Zusammen mit den Datenschutzbeauftragten des Landes Schleswig-Holstein und der Freien und Hansestadt Hamburg unterzogen wir diese Dokumente einer eingehenden Analyse. Zentrales Dokument für unsere Analyse war dabei das Papier "CCMS technische und organisatorische Mandantentrennung". Unser Maßstab für die Beurteilung der vollständigen Trennung der Datenbestände der einzelnen Teilnehmerländer war die "Orientierungshilfe Mandantenfähigkeit", die vom Arbeitskreis

Technik der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2012 herausgegeben worden war und die Anforderungen an eine Mandantentrennung in fünf differenziert beschriebenen Prüfschritten festlegt. Zu den Anforderungen aus der Orientierungshilfe gehört nach Prüfschritt 4, dass ein Anwender nur auf die Datensätze seines Mandanten zugreifen können darf. Der direkte Zugriff eines Anwenders auf Daten aus anderen Mandanten muss durch technische Maßnahmen ausgeschlossen sein.

Dem Dokument "CCMS technische und organisatorische Mandantentrennung" war zu entnehmen, dass innerhalb des CCMS die Funktion "Mailtipps" aktiviert ist. Mit dieser Funktion können beim Anschreiben anderer Anwenderinnen und Anwender deren Abwesenheitsnachrichten bereits vor dem Absenden der E-Mail als Hinweis, als sogenannter Mailtipp, angezeigt werden. Innerhalb von CCMS erfolgt dies auch über Mandantengrenzen hinaus für alle Nutzerinnen und Nutzer ohne jegliche Beschränkung. Die Anzeige des Mailtipps bereits während des Verfassens einer E-Mail ist nur möglich, weil währenddessen ein direkter Zugriff auf die Daten der Anwenderinnen und Anwender anderer Mandanten erfolgt. Die Anzeige ist nicht Ergebnis eines E-Mail-Versands und einer daraufhin automatisiert erstellten Antwort-E-Mail mit der Abwesenheitsnachricht, sondern das direkte Auslesen einer potenziellen Abwesenheitsnachricht ohne den Versand einer E-Mail. Dies ist nur möglich, weil ein mandantenübergreifender Zugriff existiert. Hätten die Mandanten getrennte CCMS-Instanzen, wäre diese Funktion nicht nutzbar. Damit wird der Prüfschritt 4 der Orientierungshilfe Mandantentrennung nicht erfüllt.

Alle Teilnehmerinnen und Teilnehmer am CCMS verfügen im System über eine sogenannte Visitenkarte. Auch die Visitenkarte der oder des Adressaten einer E-Mail wird dem Verfasser unmittelbar nach Eingabe der Empfänger-E-Mail-Adresse angezeigt. Dabei wird in der Visitenkarte auch der jeweils aktuelle Kalenderstatus der Empfängerin beziehungsweise des Empfängers aufgeführt. Damit wird offenbart, ob die Empfängerin beziehungsweise der Empfänger anwesend ist, ob sie oder er derzeit verfügbar oder gerade gebucht ist und ab wann sie oder er wieder verfügbar sein wird. Diese Daten basieren direkt auf dem Kalender der Empfängerin beziehungsweise des Empfängers. Eine Aktivierung des Abwesenheitsassistenten ist für die Anzeige "abwesend" in der Visitenkarte nicht erforderlich; der Text der Abwesenheitsnachricht wird nicht dargestellt. Ein weiterer Bestandteil einer Visitenkarte kann ein Foto der zugehörigen Person sein. Dies ist dann der Fall, wenn in dem Mandanten, zu dem die Person zugehörig ist, auf Mandantenebene freigeschaltet ist, dass Anwender Benutzerfotos von sich einstellen können. Das entsprechende Foto wird Verfassern von E-Mails angezeigt, sobald beim Erstellen einer E-Mail das "An"-Feld gefüllt wird und die Adressatin beziehungsweise der Adressat ein Benutzerfoto eingestellt hat. Hat eine Anwenderin beziehungsweise ein Anwender ein Benutzerfoto eingestellt, so berücksichtigt CCMS bei der Anzeige die Mandantentrennung nicht. Das Bild ist nicht nur für Mitarbeiterinnen und Mitarbeitern einer Verwaltung, also

innerhalb des eigenen Mandanten sichtbar, sondern bei mandantenübergreifender Kommunikation auch für die Kolleginnen und Kollegen aus anderen Ländermandanten. Eine solche Anzeige ist ein direkter Zugriff innerhalb der Anwendung CCMS auf die Daten von Anwenderinnen und Anwendern anderer Mandanten und steht im Widerspruch zu einer Mandantentrennung.

Nach unserer Auffassung ist das CCMS dadurch, dass die Mandantentrennung nicht vollständig gegeben ist, ein zentrales Verfahren, in dem personenbezogene Daten länderübergreifend gespeichert und verarbeitet werden. Für ein solches gemeinsames länderübergreifendes Verfahren fehlt eine Rechtsgrundlage. Die gemeinsame Stellungnahme der Landesdatenschutzbeauftragten der Dataport-Trägerländer ist mit gleich lautenden Anschreiben jeweils an die für das CCMS zuständigen Stellen in den Ländern mit der Bitte um Stellungnahme versandt worden. Die bremische Antwort lag uns bis zum Redaktionsschluss nicht vor.

5.3 Verwendung eines Online-Dienstes im BASIS.Bremen Betrieb

Die Cloud-Anwendung Office 365 von Microsoft beinhaltet neben anderen Funktionalitäten wie beispielsweise den Möglichkeiten der virtuellen Zusammenarbeit und Kommunikation via PC die Anwendungen Word, Excel, Outlook und PowerPoint. Die Standardsoftware wird über das Internet bezogen. Die Programme werden damit nicht in der eigenen IT-Infrastruktur der Stellen, die diese Anwendung einsetzen, betrieben und gewartet, sondern es wird im Wesentlichen ein Nutzungszugang zu den Anwendungsprogrammen bereitgestellt.

Zur Prüfung des Einsatzes von Microsoft Online-Diensten in der öffentlichen Verwaltung wurde im Berichtsjahr eine Arbeitsgruppe der Trägerländer der Anstalt öffentlichen Rechts Dataport unter der Leitung Dataports eingerichtet. Parallel dazu konstituierte sich eine Arbeitsgruppe des IT-Ausschusses der bremischen Verwaltung unter Leitung des IT-Referats der Senatorin für Finanzen, an der wir teilnahmen. Sie begutachtete die Möglichkeiten zur Nutzung von Microsoft Online-Diensten durch Verwaltungsarbeitsplätze innerhalb der zentralisierten und standardisierten Betriebsorganisation BASIS.Bremen und kam zu dem Ergebnis, dass eine Anpassung der online zur Verfügung gestellten Software an den BASIS.Bremen-Betrieb zwar möglich, ein Mehrwert der Online-Variante aber gegenwärtig nicht feststellbar sei. Deshalb werden als online Service bereitgestellte Office Versionen vorerst nicht im BASIS.Bremen-Betrieb als Standardbüroprogramm verwendet. Darüber hinaus wurde festgestellt, dass es im Zusammenhang mit Office 365 noch eine Reihe offener Fragen zum Datenschutz und zur IT-Sicherheit gibt.

Die offenen Fragen ergeben sich aus den grundlegenden Eigenschaften von Cloud-Strukturen wie etwa der Exponiertheit im Internet, der öffentlichen Erreichbarkeit und dem Betrieb durch Dritte. Daraus ergeben sich Sicherheitsrisiken, die zu Verletzungen von Vertrautheit, Integrität und Verfügbarkeit der Daten führen können. Risiken können beispielsweise das Einspielen von Schadsoftware, die unzulässige Nutzung leicht zugänglicher externer Schnittstellen oder auch unrechtmäßige Zugriffe interner Mitarbeiterinnen und Mitarbeiter auf die Infrastruktur sein, ebenso komplette Datenverluste durch technische Probleme, eine erhöhte Kompromittierbarkeit dadurch, dass viele Anwenderinnen und Anwender die gleiche Infrastruktur benutzen und, wie bei jeder neuen Technologie, eine Reihe noch unbekannter Gefahren. Den durch eine Analyse genau zu definierenden Risiken muss eine Transparenz der Absicherungsmaßnahmen der Betreiberin beziehungsweise des Betreibers der Cloud gegenüberstehen. Dazu gehören die Umsetzung datenschutzrechtlicher Anforderungen wie beispielsweise eine vollständige Löschungsgarantie für nicht mehr benötigte oder falsche personenbezogene Daten, die Mandantenfähigkeit, also die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen Infrastruktur, eine zuverlässige Datensicherung, das Angebot qualitativ hochwertiger Authentisierungsverfahren, ein sicheres Session Key Management, also die Bereitstellung und Verwaltung von kryptografischen Schlüsseln zum Verschlüsseln von Nachrichten und Dokumenten, und die Möglichkeit der Lokalisierung von Daten durch die verantwortlichen Stellen. Der Schutz der Infrastrukturebene, Plattform und Anwendungsebene muss revisionssicher gewährleistet werden (siehe hierzu die Orientierungshilfe Cloudcomputing, www.datenschutz.bremen.de).

Es ist davon auszugehen, dass im Rahmen von Office 365 Daten mit hohen Vertraulichkeitsanforderungen verarbeitet werden, die hohe Datenschutzstandards und Sicherheitsstandards in Cloud-Diensten voraussetzen. Die Verarbeitung der Daten erfolgt auf den Servern eines Rechenzentrums außerhalb des Zugriffs der verantwortlichen Verwaltungseinheit. Dadurch sind die besonderen Anforderungen für die Verarbeitung personenbezogener Daten im Auftrag zu erfüllen. Die Verpflichtungen im Rahmen der Auftragsdatenverarbeitung erfordern eine intensive Prüfung der Auftragnehmerin oder des Auftragnehmers. Die strukturierte Vorgehensweise nach IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik fordert im Rahmen des Sicherheitsprozesses eine Risikoanalyse und Risikoabwägung. Das bedeutet, dass die Sicherheitsvorkehrungen des Anbieters genau analysiert werden müssen. In die Betrachtung ist auch der Hauptsitz des Cloud-Anbieters einzubeziehen. Die den Online-Dienst Office 365 anbietende Firma Microsoft hat ihren Hauptsitz in den Vereinigten Staaten von Amerika und unterliegt dem Patriot Act, der seit 2002 den Zugriff auf abschließend definierte Datenbestände durch amerikanische Geheimdienste erlaubt. Aufgrund dieser nach bremischem Datenschutzgesetz unzulässigen Zugriffsmöglichkeiten halten wir eine sichere

datenschutzgerechte Nutzung des Microsoft-Online-Dienstes Office 365 nicht für gewährleistet (siehe hierzu die Ziffern 16.1, 16.2 und 16.3 dieses Berichts).

Neue Funktionen, die Administratoren und Nutzern mehr Kontrolle über ihre Informationen in der Cloud-Umgebung Office 365 geben sollen, wie etwa Logs (Protokolldaten) zu Aktionen in Exchange Online und SharePoint Online (Contentmanagmentsystem für Zusammenarbeit) und die Möglichkeit der Verschlüsselung von E-Mails, reichen zur Wahrnehmung der gesetzlich geforderten Auftragskontrolle nicht aus. Obwohl diese neuen Funktionen dem Datenschutz dienlich sein können, bleiben sie Funktionen, die das Unternehmen selbst zur Verfügung stellt, bei denen deshalb die Möglichkeit diese Funktionen unkontrolliert zu verändern, nicht ausgeschlossen werden kann.

Da die grundlegende datenschutzrechtliche Betrachtung des Cloud-Computing von Microsoft hinsichtlich der transatlantischen Datenströme und insbesondere hinsichtlich der Umsetzungsmöglichkeiten der für die Auftragsdatenverarbeitung geforderten Gewährleistungspflichten noch nicht abgeschlossen ist, halten wir die Entscheidung der Senatorin für Finanzen für richtig, das Produkt zum jetzigen Zeitpunkt nicht einzuführen.

Unabhängig von der Möglichkeit, die gesetzlich vorgeschriebene Auftragskontrolle über Bewertungen durch Dritte wie etwa in Form von Zertifikaten vornehmen zu lassen, bleibt der hohe Bedarf nach direkter Kontrolle, je höher der Schutzbedarf der zu verarbeitenden Daten ist. Die Verantwortung für eine datenschutzgerechte Verarbeitung ist nicht übertragbar. Es ist unzulässig, dass die öffentliche Verwaltung die direkte Kontrolle über ihre Datenverarbeitung aufgibt. Damit das nicht passiert, sind eine differenzierte Analyse der Risiken und eine klare Konzeption hinsichtlich der verantwortbaren Cloud-Architektur unverzichtbar. Eine zukünftige Online-Lösung Office 365 darf nicht zum Verlust des Großteils der Kontrolle an die Dienstleisterin beziehungsweise an den Dienstleister führen. Die öffentliche Verwaltung muss weiterhin ihre datenschutzrechtliche Verantwortung wahrnehmen. Sie muss die Beherrschbarkeit ihrer Daten behalten und dafür sorgen, dass die betroffenen Menschen nicht ausspioniert werden können. Sie muss ihre hoheitlichen Interessen und ihre Handlungsspielräume bewahren. Wir erwarten, dass die Gewährleistung des Datenschutzes in einem eventuell beginnenden Folgeprojekt einen hohen Stellenwert einnehmen wird. Die in Zukunft zu klärende Frage wird sein, ob überhaupt und wenn ja ,wie das Angebot von Online-Diensten wie etwa Office 365 unter den rechtlichen Rahmenbedingungen, die die Einhaltung von Informationssicherheitsstandards und Datenschutzstandards fordern, effizient genutzt werden kann.

6. Inneres

6.1 Allgemeines zu den Polizeiverfahren

Aktuell unterliegen das polizeiliche Vorgangsbearbeitungssystem @rtus und der polizeiliche Informations-und Analyseverbund (PIAV) unserer datenschutzrechtlichen Bewertung.

Das polizeiliche Vorgangsbearbeitungssystem @rtus (vergleiche 38. Jahresbericht, Ziffer 5.1) wurde uns im November des Berichtsjahres präsentiert. Gegenstand der datenschutzrechtlichen und datenschutztechnischen Auseinandersetzung im Rahmen von @rtus sind, neben der Verfahrensbeschreibung, die Protokollierung sowie das Berechtigungskonzept und Löschkonzept. Außerdem sind in diesem Zusammenhang die Verfahren @rtus-Recherche und die elektronische Kriminalakte zu berücksichtigen. Wir befinden uns derzeit in der Prüfung.

In der Besprechung zu PIAV im Mai des Berichtsjahres wurde uns ein hervorragendes Konzept zu den datenschutzrechtlichen und datenschutztechnischen Aspekten vorgelegt, dessen Bewertung wir aufgrund des Umfangs der Dokumentation von PIAV und aufgrund der mangelnden Datenschutzkonzeptionen anderer Systeme, die Schnittstellen zu PIAV haben, noch nicht abschließen konnten. Es handelt sich dabei um das genannte polizeiliche Vorgangsbearbeitungssystem @rtus, das eine Schnittstelle zum polizeilichen Informationssystem Ermittlung und Recherche (PIER) hat und das System PIER selbst, das über eine direkte Schnittstelle zu PIAV verfügt. In der Besprechung forderten wir, dass nur bereinigte Daten migriert werden, und betonten erneut, dass PIER temporär für Großverfahren genutzt wird und keine dauerhafte Nutzung erforderlich ist. Dieser Umstand wirkt sich auf die Datenlieferung nach PIAV aus und muss berücksichtigt werden. Das Protokollierungskonzept von PIAV prüfen wir derzeit unter Vorbehalt der Bedenken gegenüber der unvollständigen Protokollierung von @rtus. Wir betonten, dass wir eine automatisierte Löschung der personenbezogenen Daten bei Erreichen der Aussonderungsprüffrist in @rtus, PIER und PIAV befürworten, und dass eine fehlende Dokumentation zu einer unzulässigen Speicherung führen kann (vergleiche hierzu 38. Jahresbericht, Ziffer 5.4).

Die Fertigstellung des Datenschutzkonzepts für die Telekommunikationsüberwachung zusammen mit dem Landeskriminalamt Niedersachsen (vergleiche hierzu 37. Jahresbericht, Ziffer 5.2) stagniert. Im August des Berichtsjahres trafen wir uns mit der Landesbeauftragten für Datenschutz Niedersachsen und besprachen alle offenen Punkte wie 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.

Die offenen Themen mit den Polizeien der Freien Hansestadt Bremen sind neben dem oben genannten Polizeiverfahren @rtus und der Telekommunikationsüberwachung mit dem Landeskriminalamt Niedersachsen auch noch das jeweilige Rahmendatenschutzkonzept der Polizei Bremen und der Ortspolizeibehörde Bremerhaven, PIER sowie das Rechen- und Dienstleistungszentrum für die Telekommunikationsüberwachung, das fehlende Datenschutzkonzept für das Verfahren INPOL-Land, das fehlende Löschkonzept der Polizei Bremen für die Falldatei Rauschgift als INPOL-Anwendung (vergleiche hierzu 38. Jahresbericht, Ziffer 5.4) und die noch ausstehende Mitteilung des behördlichen Datenschutzbeauftragten über die Ergebnisse der Vorabkontrollen betreffend Intrapol (vergleiche hierzu 37. Jahresbericht, Ziffer 5.3).

6.2 BodyCam bei der Polizei Bremen

Die Diskussion über die Zulässigkeit des Einsatzes von BodyCams bei der Polizei Bremen begleiten wir seit mehr als einem Jahr. Unsere grundsätzlichen Kritikpunkte (vergleiche hierzu 38. Jahresbericht, Ziffer 5.2) haben wir im Laufe des Gesetzgebungsprozesses gegenüber dem Gesetzgeber und der Verwaltung geäußert, die sie nur in wenigen Punkten aufgegriffen haben.

Mit Wirkung zum 24. Juni 2016 wurde § 29 Absatz 5 Bremisches Polizeigesetz dahingehend geändert, dass nunmehr "der Polizeivollzugsdienst (…) personenbezogene Daten bei Anhaltesituationen und Kontrollsituationen im öffentlichen Verkehrsraum (…) mittels Aufzeichnungen kurzzeitig verdeckt technisch erfassen und, soweit dies nach den Umständen zum Schutz von Polizeivollzugsbeamten, von Betroffenen oder von Dritten erforderlich ist, offen erheben und aufzeichnen" darf. Damit kann der Einsatz einer Kamera, die am Körper der Polizistin beziehungsweise des Polizisten angebracht ist, eine sogenannte BodyCam, erlaubt sein. Nach der gesetzlichen Regelung müssen solche Aufzeichnungen "auch auf Verlangen einer oder eines Betroffenen" angefertigt werden, "sofern die technischen Mittel in der Anhaltesituation und Kontrollsituation verfügbar sind". Auch in diesen Fällen ist die Aufzeichnung nur erlaubt, sofern die Voraussetzungen des § 29 Absatz 5 Satz 1 Bremisches Polizeigesetz vorliegen. Die Aufzeichnungen dürfen für mindestens zwei Monate gespeichert werden. Danach müssen sie gelöscht oder vernichtet werden, "soweit nicht die Aufbewahrung im Einzelfall zur Verfolgung von Straftaten weiterhin erforderlich ist". Der vom Gesetzgeber gewählte Begriff "Aufzeichnung" umfasst sowohl Videoaufzeichnungen als auch Tonaufnahmen.

Aus dem verfassungsrechtlichen grundsätzlichen Verbot der heimlichen Überwachung folgt, dass die BodyCams für die Bürgerinnen und Bürger gut sichtbar sein müssen, sodass diese darüber informiert sind, was gerade aufgenommen wird.

Mit der Formulierung "darf (…) mittels Aufzeichnungen kurzzeitig verdeckt technisch erfassen" wollte der Gesetzgeber auch das sogenannte Pre-Recording erlauben. Unter "Pre-Recording" wird eine Videoaufzeichnung von 30 Sekunden Länge im Stand-by-Modus "vor dem eigentlichen Auslösen einer Videoaufzeichnung" verstanden. Die Aufnahme läuft also schon unmittelbar nach dem Einschalten der Videokamera, wenn diese sich noch im Stand-by-Modus befindet. Nach dem Einschalten der Kamera leuchtet konstant eine kleine rote Lampe und kennzeichnet den Stand-By-Modus. Während des "Pre-Recording" leuchtet diese rote Lampe weiterhin konstant. Insofern entsteht der fälschliche Eindruck, dass die Körperkamera nicht aufzeichnet, obwohl dies in einer 30 Sekunden währenden Zeitschleife geschieht. Das "Pre-Recording" stellt damit eine nicht erkennbare, also verdeckte Videoaufzeichnung dar. Die Aufnahmezeit von 30 Sekunden für das "Pre-Recording" wird von der Polizei Bremen als kurzzeitig im Sinne des Gesetzes angesehen und ist fest eingestellt. Die "Pre-Recording"-Daten werden erst dann dauerhaft gespeichert, wenn die Polizeibeamtin oder der Polizeibeamte die Videoaufzeichnung durch Druck auf einen Knopf auslöst und das Gerät von dem Stand-By-Modus in den Aufnahmebetrieb wechselt. Dies ist erkennbar durch ein rotes Licht am Gerät: Nach dem Auslösen der Aufnahme, also während der Videoaufzeichnung, blinkt das rote Licht.

Seit Anfang November 2016 werden die ersten sieben BodyCams von der Polizei Bremen genutzt. Sie verfügen über die Funktionen Aufnehmen, Vorspulen oder Zurückspulen durch Drücken der entsprechenden Tasten sowie Ansehen durch Drücken der Wiedergabe-Taste. Die Polizei benutzt bei den Identitätsfeststellungen Überziehwesten, die über ein Klettverschlusssystem den Hinweis auf eine Videoaufzeichnung gewährleisten. Der Senator für Inneres hat angekündigt, einmal im Vierteljahr eine Evaluierung vorzunehmen. Insbesondere die Erforderlichkeit von Aufnahmen im Rahmen des "Pre-Recording" sollte aus unserer Sicht dabei evaluiert werden, da die verfassungsrechtlich gebotene Verhältnismäßigkeit einer verdeckt stattfindenden, polizeilichen Videoaufzeichnung nur in absoluten Ausnahmefällen gegeben sein kann.

6.3 Online-Wache

Die Polizeien der Freien Hansestadt Bremen möchten den Bürgerinnen und Bürgern als zeitgemäßen Bürgerservice die Möglichkeit geben, Strafanzeigen jeweils über ein Internetangebot der Polizei Bremen und der Ortspolizeibehörde Bremerhaven zu erstatten, also die sogenannte Online-Wache eröffnen. Hinsichtlich der Ausgestaltung dieser Online-Wachen soll das Angebot nach Auswertung der Erfahrungen aus anderen

Bundesländern bewusst auf die Anzeigenerstattung von Delikten geringerer persönlicher Eingriffsintensität wie zum Beispiel Fahrraddiebstahl oder Kraftfahrzeugsachbeschädigung begrenzt werden.

Für die Polizei Bremen und die Ortspolizeibehörde Bremerhaven sollen Internetwachen eingerichtet werden, die die datenschutzrechtlichen Belange sorgfältig berücksichtigen. Aus unserer Sicht muss insbesondere der sichere Datentransfer vom Rechner der anzeigenden Person in das Polizeinetz gewährleistet sein. Dies kann unter anderem mit dem Einsatz (Ende-zu-Ende) verschlüsselter E-Mails gewährleistet werden, wirft aber, sofern auch Dateianhänge zugelassen sind, weitere Fragen zur Sicherstellung der informationstechnischen Sicherheit des Polizeinetzes auf. Wir wurden frühzeitig beteiligt und werden das Verfahren weiter begleiten.

6.4 Bundesverfassungsgerichtsurteil zum Bundeskriminalamtgesetz

Mit seinem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz (BKAG) führte das Bundesverfassungsgericht (BVerfG) seine ständige Rechtsprechung zu den Voraussetzungen für die Durchführung von heimlichen Überwachungsmaßnahmen und zur weiteren Nutzung und Übermittlung der Daten zu anderen Zwecken an dritte Behörden systematisch zusammen. Das Bundesverfassungsgericht erklärte einige Regelungen des Bundeskriminalamtgesetzes für verfassungswidrig. Soweit das Urteil Aussagen zur Zulässigkeit verdeckt durchgeführter Überwachungsmaßnahmen zum Zweck der Gefahrenabwehr oder Strafverfolgung enthält, hat es Auswirkungen auf die Beurteilung der Verfassungsmäßigkeit des Bremischen Polizeigesetzes (BremPolG). Das Bremische Polizeigesetz wurde deshalb im Lichte der Entscheidung des Bundesverfassungsgerichts vom Senator für Inneres geprüft, der gesetzgeberischen Handlungsbedarf sieht. Daher wird das Bremische Polizeigesetz zeitnah geändert werden.

Aus unserer Sicht sind die sich aus dem Urteil ergebenden Vorgaben des Bundesverfassungsgerichts für die verfassungsgemäße Ausgestaltung von polizeilichen Eingriffsbefugnissen und Datenübermittlungen sowie für zweckändernde Datennutzungen besonders bedeutsam für die Änderungen des Bremischen Polizeigesetzes. Sie sind insbesondere bei der gesetzgeberischen Gestaltung der § 33 Absatz 2, Absatz 4 und Absatz 5, § 34, § 36, § 36 b Absatz 6, § 36 d und § 36 f BremPolG zu berücksichtigen. Sie sind im Folgenden zusammengefasst.

Sofern verdeckt durchgeführte Ermittlungsbefugnisse besonders tief in die Privatsphäre der Betroffenen eingreifen, ist es nach dem Bundesverfassungsgericht Aufgabe des Gesetzgebers, einen angemessenen Ausgleich zwischen der Schwere des Grundrechtseingriffs einerseits und der Pflicht des Staates zum Schutz der Bevölkerung

(Gefahrenabwehr und Strafverfolgung) andererseits zu schaffen. Der Verfassungsgrundsatz der Verhältnismäßigkeit verlange, dass derartige Ermittlungsbefugnisse auf den Schutz gewichtiger Rechtsgüter begrenzt blieben. Im Gefahrenabwehrrecht seien sie nur dann verfassungsgemäß, wenn im Einzelfall eine Gefährdung der geschützten Rechtsgüter hinreichend konkret absehbar sei. Neben der Zielperson dürfe sich die Maßnahme nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte erstrecken.

Im Urteil heißt es wörtlich: "Eigene verfassungsrechtliche Grenzen ergeben sich hinsichtlich des Zusammenwirkens der verschiedenen Überwachungsmaßnahmen. Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können. Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssen die Sicherheitsbehörden mit Rücksicht auf das dem "additiven" Grundrechtseingriff innewohnende Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt."

Weiter verweist das BVerfG darauf, dass der Einsatz von besonderen Mitteln zur Überwachung außerhalb von Wohnungen grundsätzlich einen Richtervorbehalt erfordere, sofern eine Datenerhebung durch langfristige Observation stattfinde oder nicht öffentliche Gespräche erfasst würden. Eine Wohnraumüberwachung bei Kontaktpersonen und Begleitpersonen sei unangemessen, weil eine derartige Maßnahme besonders tief in die Privatsphäre eindringe. Bei der Wohnraumüberwachung oder beim Zugriff auf informationstechnische Systeme seien zudem besonders strenge Regelungen zum Schutz des Kernbereichs privater Lebensführung erforderlich. So seien nach Durchführung derartiger Maßnahmen zunächst alle erhobenen Daten von einer unabhängigen Stelle daraufhin zu sichten, ob diese höchstpersönliche Informationen enthalten, es sei denn, es sei Gefahr im Verzug.

Verdeckt durchgeführte Überwachungsmaßnahmen, die typischerweise dazu führen könnten, in den geschützten Kernbereich privater Lebensgestaltung einzudringen, bedürften besonderer Schutzregelungen. Erst diese flankierenden Regelungen machten die Maßnahme verhältnismäßig. Die verfassungsrechtlichen Anforderungen an Transparenz, individuellen Rechtsschutz sowie unabhängiger Kontrollen müssten erfüllt sein. Hierzu gehörten die Pflicht zur Benachrichtigung betroffener Personen, richterliche Kontrollbefugnisse, regelmäßige Kontrollen durch eine unabhängige Aufsicht, umfassende Protokollierungspflichten, Berichtspflichten gegenüber dem Parlament und der Öffentlichkeit sowie wirksame Sanktionsmöglichkeiten und Löschungspflichten.

Nach dem Grundsatz der Zweckbindung dürften Daten über das ursprüngliche Ermittlungsverfahren hinaus im Rahmen der festgelegten Zweckbestimmung weiter genutzt werden, solange die erhebungsberechtigte Behörde die Daten in demselben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutze. Damit verbunden sei eine Nutzung der Daten als bloßer Spurenansatz. Eine zweckändernde Nutzung der Daten habe sich dabei an dem sogenannten Grundsatz der hypothetischen Datenneuerhebung zu orientieren. Die neue Datennutzung müsse dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, das ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könne. Das Kriterium der Datenneuerhebung gelte allerdings nicht schematisch abschließend und schließe die Berücksichtigung weiterer Gesichtspunkte nicht aus. Als neu zu rechtfertigender Eingriff bedürfe es eines eigenen, hinreichend spezifischen Anlasses. Dabei reiche aus, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergebe.

Bei Daten, die aus einer Wohnraumüberwachung oder einem Zugriff auf informationstechnische Systeme stammten, gelte für eine weitere oder zweckändernde Nutzung strengere Maßstäbe. Hier müssten zusätzlich die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sein. Dies sei nur dann der Fall, wenn eine dringende oder im Einzelfall hinreichend konkretisierte Gefahrenlage vorliege.

Die generelle Übermittlung von Daten, die zum Zweck der Gefahrenabwehr erhoben worden seien, an Strafverfolgungsbehörden sei verfassungswidrig. Die sehr weit formulierten Maßstäbe eines Auskunftsverlangens der Strafverfolgungsbehörden nach § 161 Absatz 1 und Absatz 2 der Strafprozessordnung seien als verfassungsrechtlich gebotene Begrenzung einer zweckändernden Datennutzung nicht ausreichend. Daten dürften nur zur Verfolgung solcher Straftaten genutzt werden, für die sie mit entsprechenden Mitteln erhoben werden dürften. Darüber hinaus müsse ein gleichgewichtiger Rechtsgüterschutz vorliegen. Diese Grundsätze gälten auch bei der Übermittlung von Daten an Nachrichtendienste.

Eine Übermittlung von Daten, die aus einer optischen Wohnraumüberwachung zum Zweck der Gefahrenabwehr stammten, an Strafverfolgungsbehörden sei verfassungswidrig.

6.5 Stadtamt Bremen – Organisatorisches

Eine Vielzahl von Eingaben erreichte uns von Kundinnen und Kunden des Stadtamtes Bremen. So sorgte sich ein Petent um die Einhaltung des Datenschutzes im BürgerServiceCenter-Mitte, weil die zu den Wartezonen auf den Etagen nahe gelegenen Schreibtische teilweise nur unzureichend mit Stellwänden abgetrennt worden waren, sodass Wartende die Angelegenheiten der anderen Kunden mitbekamen. Das daraufhin von uns

angeschriebene Stadtamt sagte zu, es würden weitere Stellwände aufgestellt und die fraglichen Schreibtische zukünftig nur in Ausnahmefällen genutzt. Vollständig ließe sich die beklagte Situation aufgrund der baulichen Ausgestaltung der Etagen allerdings nicht vermeiden.

Ein anderer Petent hielt den Einsatz von Beschäftigten eines Sicherheitsdienstes am Empfang im BürgerServiceCenter-Stresemannstraße für datenschutzrechtlich fragwürdig. Das Stadtamt verwies darauf, dass von den Sicherheitskräften keine hoheitlichen Aufgaben übernommen würden, sondern diese zur Steuerung der Besucherinnen und Besucher eingesetzt würden und eine Verarbeitung personenbezogener Daten hierfür erforderlich sei. Die Sicherheitsfirma ließe sich dafür insbesondere bei vorhandenen Sprachschwierigkeiten Dokumente oder Anschreiben zeigen. Die externen Mitarbeiterinnen und Mitarbeiter würden bezüglich des Datenschutzes unterwiesen und zur Einhaltung des Datenschutzes schriftlich verpflichtet. Unter diesen Voraussetzungen halten wir den Einsatz des privaten Sicherheitsdienstes für möglich.

Vom Stadtamt selbst erreichte uns eine Anfrage bezüglich der Löschung von personenbezogenen Daten, die sich auf Fundsachen wie Notebooks und Mobiltelefonen befinden. Durch Personaleinsparungen und Organisationsveränderungen sah das Stadtamt keine Möglichkeit, selbst die Datenlöschung bei Fundsachen durchzuführen um diese gegebenenfalls an die Finderinnen und Finder rechtmäßig auszuhändigen. Das Stadtamt fragte daher an, ob eine Löschung der Daten im Auftrag durch ein externes Unternehmen geschehen dürfe. Wir halten eine schriftlich fixierte Auftragsdatenverarbeitung grundsätzlich für möglich, verwiesen aber darauf, dass das Stadtamt die Auftragnehmerin oder den Auftragnehmer sorgfältig auswählen und sich bei diesem von der Einhaltung der technischen und organisatorischen Maßnahmen überzeugen muss. Insbesondere bei Verwendung von Flash-Speichern, die in modernen Notebooks und in Smartphones eingesetzt werden, stellt es eine technische Herausforderung dar, die Daten ohne Möglichkeit der Wiederherstellung zu löschen. Das Stadtamt muss sich davon überzeugen, dass die Auftragnehmerin beziehungsweise der Auftragnehmer dies gewährleisten kann. Davon, dem zu beauftragenden Unternehmen zu erlauben, die Geräte zu versteigern, falls kein Interesse der Finderinnen und Finder an der Fundsache besteht, rieten wir zur klaren Abgrenzung des Auftragsdatenverarbeitungsverhältnisses gegenüber einer deutlich komplizierter zu vereinbarenden Funktionsübertragung ab.

6.6 Polizei Bremen – Personenbezogene Daten auf facebook-"Fanseite"

Entgegen unserer Empfehlung gingen die facebook-"Fanseiten" der Polizeien Bremen und Bremerhaven am 1. Juni 2015 online. Wie im 38. Jahresbericht unter Ziffer 5.5 begründet, ist ein datenschutzkonformer Betrieb von facebook-"Fanseiten" nicht möglich. Bis zum

Redaktionsschluss hat der Arbeitskreis I der Konferenz der Innenminister des Bundes und der Länder, den wir bei seinen Gesprächen mit facebook unterstützt hatten, kein abschließendes Votum dazu abgelegt, welche Rechtmäßigkeitsanforderungen die Anwendung "Fanseite" erfüllen muss.

Rund ein halbes Jahr nach der Online-Stellung der bremischen facebook-"Fanseite" beschrieb uns eine aufgebrachte Petentin, dass auf dieser Seite über einen Polizeieinsatz über die Auflösung einer privaten Feier unter Einsatz mehrerer Polizeiwagen und Polizeihunde berichtet worden sei und dabei der Nachname eines mit dem Einsatz in Beziehung stehenden Bürgers von der Polizei genannt worden sei. Als Nachsatz in der Nachricht auf facebook wurde ein Ausspruch des bekannten italienischen Künstlers Antonello da Messina[2] zitiert und der Name des Künstlers genannt. Der Einsatz fand laut Petentin bei einem Herrn Messina statt. Auf ihren Hinweis, dass durch diese Anspielung eventuell Datenschutzrechte des Betroffenen verletzt worden seien, antwortete die Polizei nach Aussage der Petentin unter Nutzung der öffentlichen Kommentarfunktion, dass es sich um ein "Inside-Joke" handele. Die zitierte Antwort wurde nach kurzer Zeit wieder gelöscht und ersetzt durch "Eine Anspielung worauf?". Die Petentin hatte zur Beweissicherung Bildschirmfotos angefertigt, die sie uns übermittelte. Kurz darauf wurden die Gegendarstellung des Betroffenen und die Kommentare unserer Petentin gelöscht. Sie erhielt von der Polizei zudem eine Verwarnung, dass ihr bei weiteren Verstößen gegen die Netiquette der Polizei eine Sperrung drohe.

Auf Nachfrage bestätigte uns die Polizei, dass der von der Petentin genannte Betroffene tatsächlich eine Beziehung zu dem beschriebenen Einsatz hatte.

Im vorliegenden Fall schloss damit mit der Petentin mindestens eine dritte Person von dem Zitat auf den Beteiligten, was der Polizei über die Kommentarfunktion mit Hinweis auf die Datenschutzgesetze mitgeteilt worden war. Schon zu diesem Zeitpunkt wäre eine Löschung des Zitats wegen des eindeutigen Hinweises angebracht gewesen, da mit dem Zitat eine Personenbestimmbarkeit auf der Hand lag. Jedenfalls, nachdem wir uns in dieser Angelegenheit an die Polizei gewandt hatten, löschte diese die gesamte Nachricht einschließlich sämtlicher Kommentare.

Die Namen sowohl des Zitatgebers als auch des Betroffenen wurden zum Schutz des Betroffenen geändert.

[2] Die Namen sowohl des Zitatgebers als auch des Betroffenen wurden zum Schutz des Betroffenen geändert.

6.7 Zuverlässigkeitsüberprüfung bei Bewachungspersonal

Bereits in unserem 38. Jahresbericht hatten wir unter Ziffer 5.11 darüber berichtet, dass die stadtbremische Gewerbebehörde auf unsere Kritik hin ihre Verfahrensweise bei Zuverlässigkeitsprüfungen von Bewerberinnen und Bewerbern für Bewachungstätigkeiten durch Verzicht auf die bis dato unzulässiger Weise eingeholten datenschutzrechtlichen Einwilligungen geändert hatte. Zugleich hatte uns die Gewerbebehörde versichert, dass politische Grundeinstellungen der mit Bewachungsaufgaben zu betrauenden Personen bei der Überprüfung der Zuverlässigkeit grundsätzlich nicht berücksichtigt würden. Insoweit war es selbstverständlich nicht um politische Anschauungen gegangen, die sich im strafbaren Bereich etwa der Volksverhetzung bewegen, oder die sich in Form einer Mitgliedschaft einer Bewerberin beziehungsweise eines Bewerbers in einer verbotenen Vereinigung zeigen oder gezeigt haben. Denn solche Anschauungen müssen nach den einschlägigen bewachungsrechtlichen Vorschriften zulasten der Bewerberin beziehungsweise des Bewerbers berücksichtigt werden und führen regelmäßig zur Beurteilung als unzuverlässig.

Offengeblieben und klärungsbedürftig war für uns, in welchem Ausmaß die Gewerbebehörde im Rahmen der Zuverlässigkeitsprüfung strafrechtliche Verurteilungen berücksichtigt, Strafakten beizieht und deren Inhalte (zum Beispiel auch aus eingestellten Strafverfahren) eigenständig verwertet sowie Stellungnahmen der Polizei unter Verwertung deren präventiv-polizeilicher Informationen, also Gefahrenabwehrinformationen, einholt. Bedauerlicherweise konnten wir auch in diesem Berichtszeitraum diese Fragen nicht abschließend mit der Gewerbebehörde klären.

Für eine weitgehende Klärung dieser offenen Fragen, jedenfalls für die Zukunft, sorgte im Berichtszeitraum dann aber der Gesetzgeber selbst. Als Reaktion auf bekanntgewordene Misshandlungsfälle in Flüchtlingsunterkünften trat am 1. Dezember 2016 das Gesetz zur Änderung bewachungsrechtlicher Vorschriften in Kraft. Neu eingeführt wurde unter anderem eine Vorschrift, die festlegt, bei welchen Straftaten Gewerbebehörden von der Unzuverlässigkeit einer Bewerberin beziehungsweise eines Bewerbers für eine Wachpersonaltätigkeit auszugehen haben. Damit ist nunmehr ein eindeutiger rechtlicher Rahmen gezogen, welche Straftaten im Rahmen der Zuverlässigkeitsprüfung berücksichtigt werden dürfen und welche Straftaten mangels anzunehmender Auswirkung auf die Befähigung als Wachperson irrelevant sind. Neu eingeführt wurde des Weiteren eine Pflicht der zuverlässigkeitsprüfenden Gewerbebehörde, eine Stellungnahme einer Wohnortpolizeibehörde darüber einzuholen, ob und gegebenenfalls welche tatsächlichen Anhaltspunkte ihr bekannt sind, die Bedenken gegen die erforderliche Zuverlässigkeit einer Wachdienstbewerberin beziehungsweise eines Wachdienstbewerbers begründen könnten. Aufgrund der Aufnahme einer solchen ausdrücklichen Rechtspflicht in das Bewachungsgewerberecht, die zugleich als spezielle Datenerhebungsbefugnis der

Gewerbebehörde bei der Polizei zu verstehen ist, und unter Berücksichtigung der Gesetzesmaterialien, die von einer "neu vorgesehenen" Einbindung von Polizeidienststellen sprechen, ist klar, dass die im bisherigen Bewachungsgewerberecht geregelte Datenerhebungsbefugnis der Gewerbebehörde nach Ansicht des Gesetzgebers die Einholung polizeilicher Stellungnahmen nicht umfasste. Sofern also die stadtbremische Gewerbebehörde bereits bisher solche polizeilichen Stellungnahmen über zu überprüfende Wachpersonalbewerber eingeholt haben sollte, was sowohl das ehemals verwendete Einwilligungsformular der Gewerbebehörde als auch die stadtparlamentarische Drucksache 18/611 S nahelegen, wäre ihr Vorgehen ohne datenschutzrechtliche Handlungsbefugnis gewesen.

Hinzuweisen ist noch auf eine weitere datenschutzrechtlich relevante Neuerung im Bewachungsgewerberecht. Bis zum Ablauf des Jahres 2018 soll ein sogenanntes Bewacherregister eingerichtet werden. In diesem sollen bundesweit Daten zu Bewachungsgewerbetreibenden und ihrem Bewachungspersonal gespeichert werden. Näheres soll eine Rechtsverordnung der Bundesregierung regeln.

7. Justiz

7.1 Aufbewahrungsfristen in der Justiz

Wir wurden in diesem Berichtsjahr über eine geplante Änderung der Regelungen über Aufbewahrungsfristen für Schriftgut in der Justiz informiert. Diese Regelungen sind Gegenstand der Verordnung über die Aufbewahrung von Schriftgut in der Justiz und Justizverwaltung vom 26. September 2016, die am 27. Oktober 2016 in Kraft trat. Wir wiesen dabei zum einen darauf hin, dass es erforderlich ist sicherzustellen, dass durch die Beiziehung von abgeschlossenen Verfahrensakten bei den Gerichten die Aufbewahrungsfristen als gesetzlich gestaltete Höchstfristen nicht unterlaufen werden. Die Höchstfristen werden zum Beispiel überschritten, wenn keine Weglegung der Akte verfügt wurde beziehungsweise werden kann, solange die Akte beigezogen wurde und somit eine Aufbewahrungsfrist gar nicht in Gang gesetzt wurde beziehungsweise wird. Auch halten wir es für datenschutzrechtlich bedenklich, dass bei Fristablauf der beigezogenen Akte diese nicht unverzüglich vernichtet wird, sondern deren Aufbewahrung verlängert wird.

Weiterhin gibt es zwischen dem Senator für Justiz und Verfassung und uns Dissens in Bezug auf eine Regelung in der Verordnung über die Aufbewahrung von Schriftgut in der Justiz und Justizverwaltung, wonach im Einzelfall längere als die in der Anlage vorgesehenen Aufbewahrungsfristen verfügt werden können, soweit dies aus besonderen Gründen erforderlich sein sollte, eine kürzere Aufbewahrungsfrist jedoch nicht vorgesehen ist. Dies kann aus unserer Sicht im Einzelfall unverhältnismäßig sein. Die

Aufbewahrungsfristen sind typisierte Festlegungen der Erforderlichkeit aus Gründen der Praktikabilität in Regelfällen. Nach dem Bremischen Gesetz zur Ausführung des Gerichtsverfassungsgesetzes darf nach Beendigung des Verfahrens Schriftgut nur so lange aufbewahrt werden, wie schutzwürdige Interessen der Verfahrensbeteiligten oder sonstiger Personen oder öffentliche Interessen dies erfordern. Ausnahmen in besonderen Einzelfällen müssen zur Wahrung dieses Verhältnismäßigkeitsgrundsatzes möglich sein. Daher sind Abweichungen betreffend die Dauer der Speicherung dahingehend zu ermöglichen, dass eine Frist verkürzt werden kann.

Eine Verkürzung der Höchstfrist im Einzelfall im Rahmen der Verhältnismäßigkeit als verfassungsrechtlichem Grundsatz nicht zu ermöglichen, steht auch im Gegensatz zur Begründung des genannten Gesetzes, in der es in Bezug auf die Verordnungsermächtigung heißt: "In der Rechtsverordnung werden für alle Aktentypen Fristen benannt werden, nach deren Ablauf das Schriftgut zu vernichten ist. Es handelt sich hierbei nicht um Mindestfristen sondern um Höchstfristen. Die einheitliche Aufbewahrung aller Akten eines definierten Verfahrenstyps dient der Rechtssicherheit und der Gewährleistung eines bundeseinheitlichen Standards. Durch § 29 Absatz 1 Satz 1 wird sichergestellt, dass Akten nicht länger als in der Rechtsverordnung vorgesehen aufbewahrt werden. Neben der Definition konkreter Aufbewahrungsfristen ermöglicht es die Regelung in § 29 a Absatz 1, wie von den Datenschutzbeauftragten des Bundes und der Länder inhaltlich gefordert, Einzelfallprüfungen oder Prüffristen für einzelne Akten oder Aktenbestandteile vorzusehen, soweit dies aus Gründen der Verhältnismäßigkeit geboten ist."

Eine Fristverkürzung im Einzelfall nicht zuzulassen, unterläuft damit die gesetzliche Legitimation von Höchstfristen und deren mögliche Ausgestaltung im Einzelfall.

7.2 Keine Verschlüsselung von E-Mails mit sensiblen Daten

Anlässlich einer Bürgerbeschwerde erfuhren wir, dass E-Mails mit besonders sensiblen personenbezogenen Daten durch den Senator für Justiz und Verfassung sowohl behördenintern als auch an andere Behörden unverschlüsselt versandt wurden. Es verstößt gegen das Bremische Datenschutzgesetz die besonders sensiblen personenbezogenen Daten mit unverschlüsselter E-Mail zu versenden. In der maßgeblichen Richtlinie für die Nutzung der Elektronischen Post heißt es: "Die Übermittlung sensibler Daten mittels E-Mail ist nur unter Einsatz geeigneter Verschlüsselungsverfahren zulässig." Wir machten den Senator für Justiz und Verfassung darauf aufmerksam, künftig personenbezogene Daten mit verschlüsselter E-Mail zu versenden. Eine Stellungnahme dazu liegt uns bisher nicht vor.

7.3 Gesetz über die psychosoziale Prozessbegleitung

Durch das Opferrechtsreformgesetz aus dem Jahr 2015 wurde § 406 g Strafprozessordnung mit dem Titel "Psychosoziale Prozessbegleitung" neu in die Strafprozessordnung aufgenommen. Danach können Verletzte einen Beistand einer psychosozialen Prozessbegleitung im Strafverfahren erhalten. Die psychosozialen Prozessbegleiterinnen und Prozessbegleiter dürfen im Strafprozess während der Hauptverhandlung gemeinsam mit dem Opfer anwesend sein, insbesondere bei Vernehmungen des Opfers. Die Grundsätze der psychosozialen Prozessbegleitung sowie die Anforderungen an die Qualifikation und die Vergütung dieser Prozessbegleitung richten sich nach dem Bundesgesetz über die psychosoziale Prozessbegleitung im Strafverfahren. Das Bremische Ausführungsgesetz über die psychosoziale Prozessbegleitung im Strafverfahren (BremAGPsychPbG) regelt konkret die Voraussetzungen für die Anerkennung als psychosoziale Prozessbegleitperson und für die Anerkennung von Ausbildungslehrgängen oder Weiterbildungslehrgängen zur psychosozialen Prozessbegleitung sowie das jeweilige Anerkennungsverfahren in der Freien Hansestadt Bremen.

Dabei sind zwei Aspekte von datenschutzrechtlicher Relevanz: Erstens ist die prozessbegleitende Person wegen der besonderen Schutzbedürftigkeit des Opfers verpflichtet, ein erweitertes Führungszeugnis vorzulegen, und zweitens wird ein Verzeichnis über die anerkannten prozessbegleitenden Personen in der Freien Hansestadt Bremen erstellt, welches der Staatsanwaltschaft, den für die Auswahl einer psychosozialen Prozessbegleitperson nach § 406 g Absatz 3 Strafprozessordnung zuständigen Strafgerichten und der Polizei zum Zwecke der Weitergabe an das Opfer zur Verfügung gestellt werden soll. Wir haben zum Führen des Verzeichnisses eine Stellungnahme abgegeben, die vom Senator für Justiz und Verfassung berücksichtigt worden ist. Insbesondere hat in den Fällen des Widerrufs oder der Rücknahme der Anerkennung als psychosoziale Prozessbegleitperson eine unverzügliche Löschung der prozessbegleitenden Person im Verzeichnis zu erfolgen. Außerdem haben wir empfohlen, den konkreten Zweck sowie die Inhalte des Verzeichnisses (Kontaktdaten wie beispielsweise postalische Adresse, Telefonnummer, Faxnummer und E-Mail-Adresse) konkret zu benennen und klarzustellen, welchen öffentlichen Stellen das Verzeichnis zur Verfügung gestellt wird. Unsere Empfehlungen wurden in der Gesetzesbegründung zu § 8 BremAGPsychPbG aufgegriffen.

8. Gesundheit

8.1 Schweigepflicht gilt auch unter Ärztinnen und Ärzten

Im 38. Jahresbericht hatten wir über eine Patientin berichtet, die Zweifel an der Rechtmäßigkeit eines ihr vorgelegten Einwilligungsformulars bei ihrem behandelnden

Kardiologen gehabt hatte, mit dem sie den Zugriff aller Mitarbeiterinnen und Mitarbeiter der vier Standorte der kardiologischen Partnerschaftsgesellschaft auf ihre Patientendaten erlauben sollte. Bei Überprüfung des Einwilligungsformulars hatte sich herausgestellt, dass das Formular nicht den Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligungserklärung entsprach und gegen die Pflicht zur Wahrung der ärztlichen Schweigepflicht verstieß. Erst nach Androhung eines Zwangsgeldes waren uns die Verfahrensbeschreibungen und Zugriffsbeschreibungen zur Verfügung gestellt worden.

Dieser Fall wird uns auch im nächsten Jahr noch beschäftigen, da das Einwilligungsformular für die Erklärung zur Datenerhebung von Befunden bei behandelnden Ärztinnen und Ärzten trotz mehrmaliger Aufforderung auch im Berichtsjahr noch nicht vollständig unseren Anforderungen entsprechend geändert wurde. Es fehlen noch immer die namentliche Nennung der einzelnen Ärztinnen und Ärzte, der Hinweis auf die Freiwilligkeit der Einwilligung, auf die Folgen der Verweigerung einer Einwilligung und die Möglichkeit zum Widerruf mit Wirkung für die Zukunft. Zudem wird die Einwilligung weiterhin nicht konkret im Bedarfsfall abgefragt, sondern pauschal vor Beginn der Behandlung eingeholt.

8.2 Datenpanne in einer Hausarztpraxis

Ein Petent berichtete uns, dass in seiner Patientenakte, die er von seiner ehemaligen Hausärztin erhalten hatte, ein Blutbild einer anderen Patientin und ein ausführlicher Arztbericht mit Diagnosen eines weiteren Patienten abgelegt worden waren. Offensichtlich handelte es sich um Unterlagen, die dem Patienten irrtümlich zugesandt worden waren. Darin lag ein Verstoß gegen die ärztliche Schweigepflicht.

Wir baten die Hausärztin um Stellungnahme zur Verletzung der ärztlichen Schweigepflicht durch die unbefugte Offenbarung von Gesundheitsdaten und forderten sie auf, Maßnahmen zur künftigen Vermeidung eines solchen Vorfalls zu ergreifen und die betroffene Patientin und den betroffenen Patienten über diese Datenpanne persönlich aufzuklären. Eine solche Aufklärung muss nach dem Bundesdatenschutzgesetz eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten.

Die Hausärztin konnte die falsche Zuordnung in ihrer Patientenakte rekonstruieren und informierte die betroffene Patientin und den betroffenen Patienten unverzüglich in persönlichen Gesprächen über die Datenpanne und erläuterte ihnen mögliche nachteilige Folgen. Zur zukünftigen Gewährleistung der ärztlichen Schweigepflicht legte sie uns schriftlich dar, dass eine tägliche Überprüfung der elektronisch abgelegten medizinischen Daten der Patientinnen und Patienten eingeführt worden sei, um die korrekte Zuordnung sicherzustellen. Als weitere Maßnahme würden zukünftig medizinische Unterlagen an eine

Patientin beziehungsweise einen Patienten erst nach Durchsicht einer Mitarbeiterin oder eines Mitarbeiters herausgegeben werden.

9. Soziales

9.1 Anonymität von Auszubildenden in der Ausgleichsverordnung

Die bremische Verordnung über die Erhebung von Ausgleichsbeträgen zur Finanzierung der Ausbildungsvergütung in der Altenpflegeausbildung wurde im April 2015 nach Abstimmung mit uns in Kraft gesetzt. Die ursprüngliche Verordnung hatte an verschiedenen Stellen Regelungen zur Anonymisierung von Daten vorgesehen. Die geplante Novellierung dieser Verordnung in unserem Berichtsjahr sah vor, dass die bisher anonymisierten Daten der Auszubildenden nun unter vollständiger Namensnennung und Angabe des Geburtsdatums von der Arbeitgeberin beziehungsweise vom Arbeitgeber geliefert werden sollten.

Wir baten die Senatorin für Soziales, Jugend, Frauen, Integration und Sport um Darlegung der Notwendigkeit der Nennung des vollständigen Namens und des Geburtsdatums der Auszubildenden. Dabei stellte sich heraus, dass es bisher in der Praxis keine Anhaltspunkte für Betrugsfälle bei der Mittelvergabe gegeben hatte. Probleme aufgrund der Anonymisierung hatten sich nur deshalb ergeben, weil Auszubildende gemeldet worden waren, die in bremischen Pflegeeinrichtungen beschäftigt waren, aber eine niedersächsische Altenpflegeschule besuchten.

Diese Fälle können auch erkannt werden, wenn die Arbeitgeber in der Neuregelung der Verordnung verpflichtet werden, zu jedem Ausbildungsverhältnis die kooperierende Altenpflegeschule anzugeben. Um das gewünschte Ziel herbeizuführen bedarf es also weiterhin nicht der Angabe der Namen und Geburtsdaten. Auch sofern Auszubildende ihre Arbeitgeber wechseln, weil sie sich beispielsweise im ersten Ausbildungsbetrieb nicht wohl gefühlt haben, sind sie möglicherweise nicht damit einverstanden, dass dies bei ihren alten oder neuen Ausbildungsstätten bekannt wird. Solche Wechsel der Ausbildungsstelle können in der novellierten Verordnung ohne Preisgabe der Identität der Auszubildenden abgebildet werden, indem die Informationen über die vorhandenen Ausbildungsverhältnisse getrennt nach erstem, zweitem und drittem Ausbildungsjahr geliefert werden. Im Ergebnis konnte die Neufassung der Verordnung daher in Zusammenarbeit mit der Senatorin für Soziales, Jugend, Frauen, Integration und Sport wieder konsequent anonymisiert werden. Die Verordnung ist am 1. Juli 2016 in Kraft getreten.

9.2 Keine vollständige Vorlagepflicht für private Kontoauszüge

Ein Petent wandte sich an uns und teilte mit, dass das Sozialamt ihn im Zusammenhang mit einem Antrag auf Grundsicherung wegen Erwerbsminderung aufgefordert habe, seine

Kontoauszüge der letzten drei Monate vollständig vorzulegen. Dabei sei ihm kein Hinweis auf die Möglichkeit der Schwärzung von personenbezogenen Daten gegeben worden.

Die Erhebung von geschützten Sozialdaten, zu denen auch Kontodaten gehören können, ist nur zulässig, wenn ihre Kenntnis zur Erfüllung einer im Sozialgesetzbuch genannten Aufgabe der erhebenden Stelle erforderlich ist. Das Bundessozialgericht hat dazu entschieden, dass den Sozialbehörden im Rahmen der Mitwirkungspflichten auf Verlangen aktuelle Kontoauszüge vorzulegen sind, aber bestimmte Zahlungsausgänge, die besonders schützenswerte personenbezogene Daten betreffen, nicht preisgeben werden müssen. Dies gilt beispielsweise für Gewerkschaftsbeiträge und Beiträge an politische Parteien oder Religionsgemeinschaften.

Wir forderten das Sozialamt auf, in Zukunft die Anspruchssteller auf die Möglichkeit des Schwärzens einzelner Buchungen bereits bei der Anforderung der Kontoauszüge hinzuweisen, da die Betroffenen den Behörden nur die Daten zur Verfügung stellen müssen, die diese zur Erfüllung ihrer Aufgabe benötigen. Das Sozialamt teilte uns daraufhin mit, dass Kontoauszüge grundsätzlich nicht archiviert würden. Die Sachbearbeiterinnen und Sachbearbeiter seien angewiesen, die Kontoauszüge durchzusehen und lediglich das Ergebnis in einem Aktenvermerk festzuhalten. Nur in Ausnahmefällen dürften Kontoauszüge eingescannt werden. Dies gelte nur, wenn alle nicht relevanten Daten geschwärzt seien. Dieses Schwärzen der Daten erfolge im Beisein der Leistungsberechtigten. Auf das Recht der beziehungsweise des Leistungsberechtigten, die Daten selbst zu schwärzen, sofern sie nicht zur Erfüllung einer Aufgabe nach dem Sozialgesetzbuch erforderlich sind, würden die Mitarbeiterinnen und Mitarbeiter nochmals explizit hingewiesen.

9.3 Offener Aktenschrank während der Sprechzeit

Ein Petent berichtete uns, dass er während der Sprechzeit des Amtes für Soziale Dienste in der Abteilung für Vaterschaftsanerkennungsangelegenheiten im offenen Aktenschrank vollständige Namen anderer Personen lesen konnte. Auf unseren Hinweis, hierin liege eine Verletzung des informationellen Selbstbestimmungsrechtes der Betroffenen, erklärte das Amt für Soziale Dienste, dass es sich bei dem geschilderten Vorgang um einen bedauerlichen Einzelfall handele und alle Aktenschränke abschließbar seien. Der Vorfall sei zum Anlass genommen worden, alle Mitarbeiterinnen und Mitarbeiter in der folgenden Dienstbesprechung darauf hinzuweisen, dass zukünftig Namen und sonstige personenbezogene Daten während der Sprechzeiten weder in den Aktenschränken noch auf den Schreibtischen einsehbar sein dürften.

10. Kinder und Bildung

10.1 Weitergabe von Gesundheitsdaten über die Schuleingangsuntersuchung

Wir wurden darüber unterrichtet, dass der Schulärztliche Dienst in der Schuleingangsuntersuchung erhobene Gesundheitsdaten regelmäßig ohne wirksame Einwilligung der Eltern an die Grundschule übermittelte. Nach dem Bremischen Schuldatenschutzgesetz darf eine solche Übermittlung grundsätzlich nur mit Einwilligung der Betroffenen erfolgen. Nach dem Bremischen Datenschutzgesetz bedarf dies zusätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Bei der Einwilligung in die Weitergabe von Gesundheitsdaten liegen jedoch keine besonderen Umstände vor, die eine andere Form als die Schriftform rechtfertigen.

Auf unsere Anfrage mit Hinweis auf die Rechtslage legte das Gesundheitsamt Bremen ein Formular vor, das Angaben über das Ergebnis der Schuleingangsuntersuchung zur Mitteilung an die Schule enthält; schriftliche Einwilligungserklärungen würden gegenwärtig jedoch nicht eingeholt. Für die Zukunft werde eine entsprechende Einwilligungserklärung erstellt und mit uns abgestimmt. Dies ist inzwischen erfolgt.

10.2 Kopplung Masterarbeiten und schulinterne Evaluation

Eine Vereinbarung zwischen der Senatorin für Kinder und Bildung und der Universität Bremen sah vor, dass studentische Forschungsaufgaben, bei denen Schülerinnen und Schüler befragt oder Informationen über sie verarbeitet werden, als schulinterne Evaluation durchgeführt werden durften. Forschungsarbeiten im Kontext von Schule und Bildung – insbesondere Masterarbeiten – eigneten sich als schulinterne Evaluation. Dies verstieß unseres Erachtens gegen den verfassungsrechtlichen Grundsatz der Zweckbindung. Nach dem Bremischen Schuldatenschutzgesetz (BremSchulDSG) sind schulinterne Evaluationen Untersuchungen der Schule zur Überprüfung der Durchführung und des Erfolges ihrer pädagogischen Arbeit. Eine Masterabschlussarbeit dagegen ist nach dem Bremischen Lehrerausbildungsgesetz ein wesentlicher Bestandteil eines Zeugnisses über die bestandene Prüfung. Insoweit handelt es sich hier um in unterschiedlichen Gesetzen konkret geregelte und demzufolge klar abgrenzbare Zwecke. Zudem können Einwilligungen der Erziehungsberechtigten in die Datenverarbeitung zu einer schulinternen Evaluation nicht als Einwilligungen zur Datenverarbeitung für einen anderen Zweck genutzt werden.

Die Bildungsbehörde erklärte uns, das Genehmigungsverfahren bei Forschungsvorhaben durch Hochschulen und andere Forschungsinstitute sei hinsichtlich der studentischen Forschungsarbeiten aufwändig und wegen seiner Verfahrensdauer und Aufgabenstellung für

Masterarbeiten weder angemessen noch geeignet. Deshalb sei die gesetzliche Regelung für schulinterne Evaluationen analog angewendet worden. Als Lösungsansatz für diese Problematik bereitete das Bildungsressort eine neue gesetzliche Regelung für Masterarbeiten im BremSchulDSG vor, gegen die wir keine Bedenken haben. Darüber hinaus vereinbarten wir mit der Senatorin für Kinder und Bildung, dass ab sofort übergangsweise bis zur Schaffung dieser neuen Vorschrift bereits danach verfahren wird. Anfang November 2016 brachte der Senat den Gesetzesentwurf in die Bremische Bürgerschaft (Landtag) ein.

10.3 Übergabegespräche zwischen abgebenden und aufnehmenden Schulen

Wir erhielten Kenntnis darüber, dass zumindest an einer Schule in Bremerhaven im Rahmen von Übergabegesprächen zwischen abgebenden und aufnehmenden Schulen regelmäßig Protokolle angefertigt wurden, die teilweise sehr sensible Angaben enthielten. Dies waren beispielsweise Informationen über die besondere familiäre Situation, Auffälligkeiten im emotionalen Bereich wie Gewaltproblematiken und Suchtproblematiken, Empfehlungen, mit welchen Kindern die betreffenden Schülerinnen und Schüler gemeinsam eine Schulklasse besuchen sollten, und mit welchen Kindern dies nicht empfohlen werde und sonstige Informationen über Medikamente, Bettnässen, Förderbedarf, besondere Stärken und die Namen von Ansprechpartnerinnen und Ansprechpartnern im Regionalen Beratungs- und Unterstützungszentrum. Diese Daten gehören nicht zu den Lernentwicklungsdaten wie Halbjahreszeugnis und Leistungsdaten, die nach dem Bremischen Schuldatenschutzgesetz beim Schulwechsel an die aufnehmende Schuler übermittelt werden dürfen.

Das Schulamt Bremerhaven erklärte auf unsere Anfrage, dass nach seiner Kenntnis lediglich das Halbjahreszeugnis und Leistungsdaten weitergegeben würden. Daraufhin übermittelten wir der Schulbehörde das Musterprotokoll einer Schule mit dem Hinweis, dass es sich nach unseren Informationen nicht nur um die Vorgehensweise der dort aufgeführten Schule handele. Vielmehr würden die anderen Schulen in Bremerhaven ebenso verfahren. Daraufhin erklärte das Schulamt, die Schulleitungen würden noch einmal explizit von der Schulaufsicht auf die geltende Rechtslage hingewiesen, wonach für die Weitergabe weiterer Daten die Einwilligung der Erziehungsberechtigten zwingend vorliegen muss, ansonsten ausschließlich Leistungsdaten weitergegeben werden dürfen.

10.4 Rechnungsversand via E-Mail

Bei der Online-Anmeldung zu einem Kurs der Bremer Volkshochschule hatte ein Kursinteressent das Lastschriftverfahren als Zahlungsart ausgewählt. Er gab seine Bankverbindungsangaben in das entsprechende Web-Formular der gesicherten Online-

Verbindung ein. Daraufhin erhielt er eine unverschlüsselte E-Mail der Bremer Volkshochschule, in deren Anhang sich eine Anmeldebestätigung nebst Rechnung sowie ein zu unterschreibender Vordruck eines SEPA-Basis-Lastschriftmandats befanden. Der Lastschriftvordruck war bereits mit den zuvor online angegebenen Bankverbindungsdaten, Kontoinhaber, Kreditinstitut, BIC, IBAN des Kursteilnehmers (vor-) ausgefüllt. Auch in der angehängten Anmeldebestätigung nebst Rechnung befand sich die Information, dass die Volkshochschule den Betrag "in Höhe von … am … von dem Konto … bei der Bank …, Kontoinhaber …" abbuchen werde. Der Betroffene war über den Versand seiner Bankverbindungsdaten per einfacher, unverschlüsselter E-Mail wenig erfreut und bat uns um datenschutzrechtliche Überprüfung.

Mit den Vorgaben des Bremischen Datenschutzgesetzes (BremDSG) war dieses Verfahren der Versendung der Anmeldebestätigung nebst Rechnung und des Lastschriftermächtigungsformulars eindeutig unvereinbar. Das BremDSG schreibt für den Umgang mit personenbezogenen Daten generell das Ergreifen geeigneter technischer und organisatorischer Maßnahmen vor. Insbesondere fordert das Gesetz verantwortliche Stellen auf, sicherzustellen, dass im Fall einer elektronischen Übertragung von Daten kein unbefugtes Lesen, Kopieren, Verändern und Entfernen erfolgen kann. Auch die verwaltungsinterne Richtlinie zur Nutzung elektronischer Post schließt eine solche Handhabung eindeutig aus. In Abschnitt 4 Ziffer 4 Absatz 3 der Richtlinie heißt es: "Die Übermittlung sensibler Daten mittels E-Mail ist nur unter Einsatz geeigneter Verschlüsselungsverfahren zulässig." Niemand käme auf die Idee, eine Postkarte mit Bankverbindungsdaten einem beliebigen Unbekannten zur Auslieferung bei einem Dritten auszuhändigen. Genau dem entspricht aber der unverschlüsselte E-Mail-Versand von Unterlagen mit Bankverbindungsdaten. Die unverschlüsselte E-Mail ist weder gegen eine Kenntnisnahme durch Unbefugte noch gegen eine inhaltliche Veränderung geschützt. Ihr Versandweg im Netz ist unbekannt, ihr Ankommen nicht sichergestellt. Dem unbefugten Zugriff auf Bankverbindungsdaten und ihrem Missbrauch durch Dritte öffnete die Bremer Volkshochschule also Tür und Tor. Betroffen waren alle Kursteilnehmerinnen und Kursteilnehmer mit Online-Anmeldung und Auswahl der Lastschriftzahlung.

Wir wandten uns an die Bremer Volkshochschule und erläuterten unmissverständlich, dass diese Übersendung von Bankverbindungsdaten der Kursteilnehmer im Rahmen der Buchungsbestätigung via E-Mail ohne Einsatz geeigneter Verschlüsselung mit dem geltenden Recht unvereinbar und geeignet sei, Vermögensinteressen der Kursteilnehmer massiv zu gefährden. Bis zu einer Softwareanpassung, falls diese nötig sei, müsse eine datenschutzgerechte Zwischenlösung gefunden werden. In der Folge fanden weitere Abstimmungen dazu statt, wie schlussendlich eine datenschutzgerechte Lösung aussehen könne.

Fast ein halbes Jahr später teilte uns der Kursteilnehmer, der uns auf den Datenschutzverstoß aufmerksam gemacht hatte, mit, die Volkshochschule verfahre unverändert wie gehabt, sende weiterhin Buchungsbestätigungen nebst vorausgefülltem SEPA-Lastschriftmandat via unverschlüsselter E-Mail. Wir wandten uns neuerlich an die Bremer Volkshochschule und monierten das bewusste Hinwegsetzen über klare Rechtsvorgaben und die wissentliche Inkaufnahme der irreversiblen Gefährdung der Vermögensinteressen der Kursteilnehmer. Eine förmliche Beanstandung stellten wir in Aussicht. Kurz darauf erreichte uns die Nachricht der Bremer Volkshochschule, man habe nunmehr eine Softwareänderung vorgenommen und damit die Problematik behoben.

11. Telemedien

11.1 Synchronisierung von Kontaktdaten in beruflichen Netzwerken

Netzwerke, die dazu dienen sich beruflich untereinander zu vernetzen, bieten Funktionen, das eigene Adressbuch mit dem Anbieter zu "synchronisieren". Damit ist gemeint, dass dem Anbieter die betreffenden Daten übermittelt werden. Solche Übermittlungen fallen in den Anwendungsbereich des Bundesdatenschutzgesetzes, weil insbesondere bei beruflichen Netzwerken in der Regel davon ausgegangen werden kann, dass damit in Zusammenhang stehende Datenübermittlungen nicht ausschließlich dem persönlichen oder familiären Bereich zuzuordnen sind.

Im Berichtszeitraum erreichten uns mehrere Anfragen bezüglich der Zulässigkeit einer solchen Übermittlung von personenbezogenen Daten an berufliche Netzwerke, die ihren Hauptsitz in den Vereinigten Staaten von Amerika haben. Nach unserer Beratung löschten die Betreffenden ihre Accounts (Konten) in dem jeweiligen Netzwerk ausnahmslos. In vielen Fällen war ihnen nicht bewusst gewesen, dass sie Daten in das Ausland übermittelten und in einigen Fällen sogar einen E-Mail-Versand auslösten, der suggerierte, dass die Empfängerin beziehungsweise der Empfänger von der Übermittlerin oder dem Übermittler persönlich zu dem beruflichen Netzwerk eingeladen werden sollte.

11.2 Personenbezogene Daten auf privaten Internetseiten

Zur Veröffentlichung von personenbezogenen Daten auf privaten Internetseiten, also zum Beispiel von Namen, persönlichen Daten und auch ganzen Dokumenten, bedarf es entweder der Einwilligung der Personen, auf die sich die Daten beziehen, oder einer Rechtsvorschrift, die eine Veröffentlichung im Internet erlaubt oder anordnet. Solche Rechtsvorschriften finden sich in den Datenschutzgesetzen, sind aber immer an Bedingungen geknüpft, die zur Veröffentlichung erfüllt sein müssen. Häufig ist als Bedingung eine positive Abwägung zwischen den Rechten und Interessen der beziehungsweise des Verantwortlichen und der

oder des Betroffenen erforderlich. In einigen uns vorgetragenen Fällen, in denen personenbezogene Daten auf privaten Internetseiten veröffentlicht wurden, konnten wir kein überwiegendes Interesse der Verantwortlichen feststellen. Auch lagen keine Einwilligungen zur Veröffentlichung vor.

Die Verantwortlichen verwiesen auf Nachfrage und teils aufgrund der Aufforderung zur Löschung der Daten zum Teil darauf, dass die Veröffentlichungen durch das Medienprivileg und durch die Meinungsäußerungsfreiheit erlaubt würden. Diesen Hinweis hielten wir in den betreffenden Fällen für unzutreffend

Nach einem Urteil des Bundesgerichtshofs vom 23. Juni 2009 kann das Medienprivileg zwar auch auf die Veröffentlichung von Internetseiten Anwendung finden, da es nicht nur für Druckerzeugnisse gelte, sondern für die "Presse" im verfassungsrechtlichen Sinn, also auch für die "elektronische Presse". Dies gelte allerdings lediglich, wenn die Veröffentlichung unter den Pressebegriff des Grundgesetzes falle. Internetseiten, zum Beispiel Weblogs und Microblogging-Angebote, könnten hierunter fallen, wenn es sich um professionelle journalistisch-redaktionell gestaltete Angebote handelt, wenn also das jeweilige Angebot den Eindruck vermittelt, dass Tatsachen umfassend recherchiert und dabei verschiedene Informationsquellen genutzt werden, das Angebot einen gewissen Grad an organisatorischer Verfestigung aufweist, die Kontinuität gewährleistet und Informationen ausgewählt, gewichtet und für den Nutzer aufgearbeitet werden. Diese Angebote seien dabei in ein besonderes Regelwerk von Rechten und Pflichten, den Pressekodex, eingebunden. Die von uns aufgrund der Eingaben untersuchten Internetseiten genügten diesen Anforderungen nicht. Daher konnten sich die Verantwortlichen nicht auf die Pressefreiheit berufen.

Auch die Meinungsäußerungsfreiheit rechtfertigt die Veröffentlichung personenbezogener Daten nur im Ausnahmefall. Das Grundrecht auf Meinungsäußerung ist nicht schrankenlos gewährt. Nach dem genannten Urteil des Bundesgerichtshofs muss eine Person gegenüber denjenigen, die unter Berufung auf die Meinungsäußerungsfreiheit ihre personenbezogenen Daten veröffentlichen, zwar grundsätzlich Einschränkungen ihres Rechts auf informationelle Selbstbestimmung hinnehmen. Dies gelte aber nur, wenn und soweit solche Beschränkungen von hinreichenden Gründen des Gemeinwohls oder überwiegenden Rechtsinteressen Dritter getragen würden und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe die Grenze des Zumutbaren noch gewahrt sei.

In den von uns bearbeiteten Fällen überwogen das Rechtsinteresse und die rechtfertigenden Gründe Dritter nicht. Eine Veröffentlichung im Internet bedeutet nämlich, dass die Daten einer weltweiten Öffentlichkeit für den Betroffenen unkontrollierbar zur Verfügung gestellt werden und auch durch Suchmaschinen zugänglich sind. Es handelte sich deshalb um

intensive Eingriffe in das Persönlichkeitsrecht. Zur Schilderung des jeweiligen Sachverhalts auf den Internetseiten hätte jeweils auch eine anonymisierte Darstellung genügt.

In den von uns bearbeiteten derartigen Fällen wurden die personenbezogenen Daten auf den privaten Internetseiten gelöscht oder die Veröffentlichungen derartig durch technische Maßnahmen eingeschränkt, dass die Daten nur noch von Mitgliedern des persönlichen oder familiären Bereichs abgerufen werden können.

12. Beschäftigtendatenschutz

12.1 Aufbewahrung von Rettungsdienstprotokollen

Die Protokolle des Rettungsdienstes enthalten im Wesentlichen ärztliche Angaben über Befunde von Notfallpatientinnen und Notfallpatienten einschließlich entsprechender Gesundheitswerte sowie Daten über die Beschäftigten des Rettungsdienstes. Diese Dokumente wurden 30 Jahre lang aufbewahrt. Begründet wurde dies mit der im Bürgerlichen Gesetzbuch enthaltenen Verjährungsfrist sowie einem Urteil des Bundesgerichtshofs. Hieraus wurde geschlossen, die Daten müssten für den Fall, dass innerhalb von 30 Jahren ein Schadensersatzanspruch geltend gemacht werden würde, aufbewahrt werden. Diese Speicherung war ein typischer Fall einer unzulässigen Vorratsdatenspeicherung. Auch das genannte Urteil rechtfertigt eine 30-jährige Speicherfrist nicht, befasst es sich doch ausschließlich damit, dass Behandlungsfehler der Notärztin beziehungsweise des Notarztes im Rettungsdienst als hoheitliche Tätigkeit nach Amtshaftungsgrundsätzen zu beurteilen sind.

Die Speicherdauer beziehungsweise Löschfrist bestimmt sich nach dem Bremischen Hilfeleistungsgesetz und dem Bremischen Datenschutzgesetz. Danach sind Daten, die für die Aufgabenerfüllung nicht mehr benötigt werden, aber aus Dokumentationsgründen aufzubewahren sind, zu sperren. Gesperrte Daten dürfen nicht mehr verarbeitet werden, es sei denn, die Verarbeitung ist zur Behebung einer bestehenden Beweisnot oder aus sonstigen überwiegenden Interessen der verantwortlichen Stelle oder im rechtlichen Interesse eines Dritten liegenden Gründen unerlässlich oder die oder der Betroffene haben in die Verarbeitung eingewilligt. Als Dokumentationsgründe kommen ausschließlich diejenigen der Ärztinnen und Ärzte nach ihrer Berufsordnung in Frage, wonach die Dokumente zehn Jahre lang aufzubewahren sind. Nach Feststellungen von Performa Nord aus dem Jahr 2009 gab es seit 1990 lediglich einen Fall im Zusammenhang mit einem Behandlungsfehler im Rettungswagen, der innerhalb eines Zeitraums von zwei Jahren nach dem Rettungseinsatz bearbeitet wurde.

Wir forderten daher, die Protokolle des Rettungsdienstes nach zehn Jahren zu vernichten. Der Senator für Inneres änderte seine Entscheidung und wies die Feuerwehr Bremen an, die 10-jährige Aufbewahrungsfrist zu beachten.

12.2 Telefonische Weiterleitung von der Beihilfestelle zum Bürgertelefon

Soweit Beschäftigte der Beihilfestelle aufgrund von Abwesenheitszeiten nicht erreichbar sind, erfolgt eine telefonische Weiterleitung zum Bürgertelefon. Unmittelbar vor der Weiterleitung ertönt eine Ansage der Beihilfestelle, die nicht auf die Weiterleitung an das Bürgertelefon verweist, sondern den Eindruck vermittelt, innerhalb der Beihilfestelle weitergeleitet worden zu sein. Dadurch kamen Beihilfeberechtigte in die unangenehme Situation, private Details zu ihren Erkrankungen den Beschäftigten am Bürgertelefon mitzuteilen. Für die Betroffenen war nicht erkennbar, dass sie nicht mit Beschäftigten der Beihilfestelle, sondern mit Beschäftigten des Bürgertelefons sprachen.

Wir baten den Eigenbetrieb Performa Nord, bei der die Beihilfestelle angesiedelt ist, mitzuteilen, in welcher Weise sichergestellt wird, dass Beihilfeberechtigte in solchen Fällen zweifelsfrei feststellen können, dass es sich nicht um die Beihilfestelle, sondern um das Bürgertelefon handelt. Daraufhin erklärte Performa Nord, um den schutzwürdigen Belangen der Betroffenen zu wahren, werde eine unmissverständliche Begrüßungsansage "Herzlich willkommen bei der Auskunft von Performa Nord" eingesetzt; dann erfolge die Namensnennung der oder des Beschäftigten.

12.3 Veröffentlichung des Wählerverzeichnisses für Betriebsratswahlen im Intranet

Für die Betriebsratswahlen veröffentlichte der Wahlvorstand der Gesundheit Nord Klinikverbund gGmbH das Wählerverzeichnis mit den Daten der insgesamt über 600 Beschäftigten im Intranet des Konzerns. Das Wählerverzeichnis enthielt die Angaben Vorname, Name, Funktion und Geschäftsbereich. Neben den Beschäftigten der vier Standorte des Klinikverbunds konnten auch Beschäftigte anderer Betriebe und Unternehmen, die das Intranet ebenfalls nutzen, Zugang zu den Beschäftigtendaten erhalten. Auch konnten die Wählerlisten beliebig geladen und verschickt beziehungsweise an Dritte übermittelt werden.

Der Wahlvorstand erklärte, er habe das Wählerverzeichnis im Intranet veröffentlicht, weil viele Beschäftigte, die an der Betriebsratswahl teilnehmen könnten, an verschiedenen Standorten arbeiten. Dadurch könnten die Wahlberechtigten, ohne zu den teilweise weit entfernten Auslagestellen kommen zu müssen, prüfen, ob sie in das Wählerverzeichnis eingetragen sind. Wir teilten dem Wahlvorstand daraufhin mit, die Betriebsratswahl erstrecke

sich nur auf die Beschäftigten der Gesundheit Nord Klinikverbund gGmbH, nicht jedoch auf die Beschäftigten der übrigen Gesellschaften, die das Intranet ebenfalls nutzen. Insoweit handelte es sich um eine unzulässige Datenübermittlung an Dritte.

Nach der Wahl verwies der neu gewählte Betriebsrat darauf, dass die Gesundheit Nord Klinikverbund gGmbH nur ein Intranet für alle Beschäftigten des Konzerns betreibt. Eine Zugangsbeschränkung für einzelne Betriebe oder Geschäftsbereiche sehe die bestehende Konfiguration des Intranets nicht vor. Der Betriebsrat sagte aber zu, künftige Gremien über die im Vorfeld der Wahl entstandene Problematik zu informieren. Das Wählerverzeichnis sei nach der Wahl aus dem Intranet entfernt worden.

12.4 Diebstahl einer Festplatte mit Beschäftigtendaten

Performa Nord meldete uns den Diebstahl einer Festplatte, auf der sich Namen, Adressen, Gehaltsdaten und Kontoverbindungsdaten von Beamtinnen und Beamten sowie Richterinnen und Richtern befinden. Die Festplatte sei in einem Serverraum aufbewahrt worden, der ständig verschlossen sei und zu dem nur wenige Personen Zutritt hätten. Aufgrund von Bauarbeiten und einer Fensterreinigung sei der Serverraum kurzzeitig geöffnet gewesen. Diesen Sachverhalt teilte Performa Nord auch den Betroffenen mit. Der Eigenbetrieb hält einen gezielten Datendiebstahl und eine missbräuchliche Verwendung oder Veröffentlichung der Daten für unwahrscheinlich, kann dies aber nicht mit absoluter Sicherheit ausschließen.

Wir halten es für möglich, dass in diesem Fall wie in der Vergangenheit in ähnlich gelagerten Fällen die Festplatte verkauft und die darauf gespeicherten personenbezogenen Daten an wirtschaftliche Akteure, die mit Daten handeln, gelangen könnten oder Kontodaten für unzulässige strafbare Abrufe von Geldern verwendet werden. Insoweit bestehen durch den Diebstahl der Festplatte erhebliche Gefahren für die Rechte der Betroffenen. Wir erfragten bei Performa Nord die technischen und organisatorischen Maßnahmen nach dem Bremischen Datenschutzgesetz (BremDSG), die getroffen worden waren, um insbesondere die Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle bezüglich der auf der gestohlenen Festplatte gespeicherten Daten zu gewährleisten. Außerdem wollten wir wissen, welche Maßnahmen aufgrund dieser Datenpanne nunmehr getroffen wurden beziehungsweise werden.

Nach Angaben der Behörde wurde die unverschlüsselte externe Festplatte seit 2011 nicht an einem Arbeitsplatz in dem für die Bearbeitung zuständigen Bereich, sondern im Serverraum platziert und mittels eines USB an den Server angeschlossen. Der Zugang zum Serverraum hatte eine selbstschließende Tür und war nicht mit einem unabhängig von der Hauptschließanlage konzipierten Schließzylinder versehen. Als Sofortmaßnamen seien neben der Verschlüsselung von Datenträgern und Datensicherungen unter anderem der

Schließzylinder gegen einen von der Hauptschließanlage unabhängigen Schließzylinder und die Türklinke gegen einen Türknauf ausgetauscht worden. Dadurch könne die Tür von außen nur noch mit einem Schlüssel geöffnet werden. Des Weiteren plane Performa Nord weitere Maßnahmen zur Gewährleistung der Zutrittskontrolle und Zugangskontrolle. Die uns genannten Maßnahmen halten wir für angemessen.

Inzwischen erreichten uns mehrere Eingaben Betroffener. Hierbei ging es auch um den Ersatzanspruch des durch die Panne eventuell entstandenen Schadens, der beispielsweise durch die Änderung von Bankverbindungen eintreten könnte. Hierzu verwiesen wir auf die Regelung zum Schadensersatz im BremDSG. Danach entscheiden die ordentlichen Gerichte über die Ansprüche.

Zur Meldung dieser Datenpanne und der Information an die Betroffenen war Performa Nord gesetzlich nicht verpflichtet. Seit 2009 enthält das Bundesdatenschutzgesetz die Pflicht zur Meldung von Datenpannen durch Bundesbehörden und nicht öffentliche Stellen. In Bremen war seinerzeit geplant, diese Regelung zu übernehmen. Jedoch wurde darauf verzichtet, weil die EU-Kommission den Entwurf einer Datenschutzgrundverordnung (DSGVO) vorlegte, die diese Pflicht für alle verantwortlichen Stellen vorsieht. Die DSGVO ist inzwischen in Kraft getreten und wird Ende Mai 2018 auch in der bremischen Verwaltung unmittelbar anwendbar sein.

12.5 Versuchte Erhebung von Gesundheitsdaten bei einem Arzt durch den Arbeitgeber

Ein Arbeitgeber bekundete seine Verwunderung über eine vorab ausgestellte Arbeitsunfähigkeitsbescheinigung bei der Arztpraxis seines Beschäftigten per Anruf bei dessen behandelnden Arzt. Zudem soll er nach dem Gesundheitszustand des Betroffenen gefragt haben. Die Arztpraxis verwies auf die Schweigepflicht und empfahl dem Arbeitgeber, etwaige Fragen mit dem Beschäftigten direkt zu klären. Auf unsere Nachfrage erklärte der Arbeitgeber, die in der Bescheinigung eingetragenen Daten seien unklar und könnten von der Lohnbuchhaltung ohne Rückfrage beim Arzt nicht erfasst werden. Nachdem die Arztpraxis ausschließlich die Richtigkeit der Angaben auf der Bescheinigung betonte, sei das Gespräch beendet worden. Er habe im Telefongespräch ausdrücklich erklärt, dass er keine Informationen zur Erkrankung seines Beschäftigten erheben wollte.

Wir wiesen den Arbeitgeber auf das Bundesdatenschutzgesetz hin, wonach personenbezogene Daten beim Betroffenen zu erheben sind. Nur unter sehr engen Voraussetzungen dürfen sie bei Dritten erhoben werden. In diesem Fall hätte es ausgereicht, Zweifel an der Richtigkeit der Angaben auf der Arbeitsunfähigkeitsbescheinigung direkt gegenüber dem Beschäftigten darzulegen und sich von diesem die Richtigkeit der Angaben

bestätigen zu lassen. Daher baten wir den Arbeitgeber, dem Beschäftigten zuzusichern, zukünftig in ähnlich gelagerten Fällen keine Daten bei Ärztinnen und Ärzten anzufragen beziehungsweise sich an die gesetzlichen Vorgaben zu halten. Dies hat uns der Arbeitgeber inzwischen bestätigt.

12.6 Kopieren von Personalausweisen durch eine Leiharbeitsfirma

Eine Leiharbeitsfirma kopierte regelmäßig anlässlich der Unterzeichnung von Arbeitsverträgen die Personalausweise von einzustellenden Personen. Das Unternehmen erklärte, die Kopien würden zusammen mit den Arbeitsverträgen dafür verwendet, die Daten in das Personalverwaltungssystem einzugeben. Die Beschäftigten hätten in die Speicherung der Daten eingewilligt.

Wir wiesen die Firma auf ein Urteil des Verwaltungsgerichts Hannover aus dem Jahr 2013 hin, wonach das Kopieren von Personalausweisen gegen das Personalausweisgesetz verstößt. Darüber hinaus ist nach dem Bundesdatenschutzgesetz eine Einwilligung im Beschäftigungsverhältnis regelmäßig nicht wirksam, weil sie in den meisten Fällen nicht auf der freien Entscheidung der oder des Betroffenen beruht. Dies war auch hier der Fall, weil die Betroffenen aufgrund des Ungleichgewichts gegenüber dem Arbeitgeber mit erheblichen Nachteilen bis zum Nichtzustandekommen des Arbeitsvertrags rechnen müssen, wollten sie eine Einwilligung in das Kopieren der Personalausweise verweigern. Wir baten das Unternehmen, zukünftig auf die Anfertigung von Kopien der Personalausweise zu verzichten und sämtliche in der Vergangenheit angefertigten Kopien dieser Dokumente zu vernichten und uns dies zu bestätigen. Dies ist inzwischen erfolgt und wurde uns bestätigt.

12.7 Speicherung aller Internetaktivitäten der Beschäftigten eines Kreditinstituts

In einem Kreditinstitut wurden alle personenbezogenen Internetaktivitäten der Beschäftigten für einen Zeitraum von fünf Monaten gespeichert. Dies entsprach einer Betriebsvereinbarung und wurde mit der Sicherstellung der Verfügbarkeitskontrolle und der Wahrung der berechtigten Interessen des Kreditinstituts begründet. Im Fall einer arbeitsrechtlich verbotenen Internetnutzung überwögen diese Interessen die schutzwürdigen Interessen der Beschäftigten. Die Protokollierung diene des Weiteren der Einhaltung der Mindestanforderungen an das Risikomanagement. Der Betriebsvereinbarung zufolge durften die Protokolldaten darüber hinaus zur Überprüfung des Verdachts von Missbrauch gespeichert und genutzt werden.

Wir wiesen das Kreditinstitut darauf hin, dass für die vorgenannten Zwecke eine personenbezogene Protokollierung aller Internetaktivitäten nicht erforderlich ist. Es reicht

aus, lediglich die IP-Adressen verkürzt um die letzten vier Ziffern zu speichern. Nur die stichprobenweise Sichtung aufgerufener Internetseiten ohne Personenbezug ist angemessen. Wenn sich hierbei herausstellen sollte, dass unzulässige Seiten aufgerufen worden sind, besteht regelmäßig die Möglichkeit, unter Einschaltung der oder des betrieblichen Datenschutzbeauftragten und der Beschäftigtenvertretung für einen begrenzen Zeitraum eine Protokollierung unter Nutzung der vollständigen ungekürzten IP-Adressen des bestimmten Arbeitsbereichs vorzunehmen, in dem die unzulässige Internetnutzung stattfand. Nach allgemeiner Erfahrung werden unzulässige Seiten wiederholt aufgerufen, sodass eine derartige zweistufige Überprüfung regelmäßig zur Identifizierung der Nutzerin beziehungsweise des Nutzers führt, die oder der die unzulässigen Seiten aufruft. Nach Durchführung der Maßnahme müssen die betroffenen Beschäftigten über die zeitlich begrenzte personenbezogene Protokollierung und Auswertung unverzüglich benachrichtigt werden.

Wir verwiesen darüber hinaus darauf, dass die schutzwürdigen Interessen der Beschäftigten überwiegen, wenn ihre sämtlichen Internetaktivitäten sozusagen "auf Vorrat" für fünf Monate gespeichert werden. Dies war besonders gravierend, weil nach Angaben des Unternehmens seit der Einführung des Internetzugangs im Jahr 2003 nur in einem Fall tatsächlich auf der Basis der Protokolldaten eine Überprüfung durchgeführt worden sei. Das Unternehmen erklärte, unsere Anforderungen sowohl in technischer als auch in organisatorischer Hinsicht umzusetzen.

13. Videoüberwachung

13.1 Beschäftigte in einem Restaurant

In einem Restaurant wurden Beschäftigte und Gäste videoüberwacht und tonüberwacht. Der bei uns eingegangenen Eingabe zufolge könne der Geschäftsführer Videodaten und Tondaten über das Internet auf seinem Handy jederzeit abrufen. Deshalb seien die Betroffenen einer mehr oder weniger lückenlosen Überwachung während ihres Aufenthalts in dem Restaurant ausgesetzt. Der Geschäftsführer erklärte dazu, es seien zwei Kameras angebracht, die dazu dienten, in der Nacht Einbruchsalarm auf seinem Handy per SMS auszulösen. Er habe immer mehr mit Taschendieben, Falschgeld und Diebstahl aus der Garderobe zu tun. Eine Videoaufzeichnung und Tonaufzeichnung finde nicht statt. Weder führte er eine Vorabkontrolle durch noch hatte er eine betriebliche Datenschutzbeauftragte beziehungsweise einen betrieblichen Datenschutzbeauftragten bestellt.

Als Ergebnis unserer Prüfung tauschte der Geschäftsführer des Restaurants die Videokameras durch Bewegungsmelder aus.

13.2 Auszubildende in einem Großraumbüro

In einem Großraumbüro waren zwei Kameras auf die Arbeitsplätze mehrerer Auszubildenden und auf den Schreibtisch des Geschäftsführers gerichtet. Die Videoüberwachung wurde nicht aufgezeichnet, war jedoch über das Tablet des Geschäftsführers jederzeit einsehbar. Die Auszubildenden waren damit einer unzumutbaren lückenlosen Überwachung ausgesetzt, insbesondere weil sie nicht wissen konnten, ob und wann der Geschäftsführer die Bilder einsah. Der Geschäftsführer erklärte uns, der Zweck der Videoüberwachung sei zu prüfen, wer und wann jemand bei seiner Abwesenheit nach Geschäftsschluss etwas an seinem Schreibtisch suche. Häufig hielten sich Vertreterinnen und Vertreter außerhalb der Geschäftszeiten in dem Großraumbüro auf. Die Kameras seien nur außerhalb dieser Zeiten aktiviert. Wir hielten es als alternativ für zumutbar, nach Verlassen des Großraumbüros Unterlagen, die sich auf dem Schreibtisch befinden, einzuschließen und insoweit vor unbefugtem Zugriff zu sichern.

Nachdem der Geschäftsführer unsere Aufforderung abgelehnt hatte, die Videokameras abzumontieren, führten wir eine Prüfung vor Ort durch. Hierbei stellten wir insbesondere fest, dass die Kameras zeitlich unbegrenzt aktiviert waren. Auch im Hinblick darauf, dass weder eine Vorabkontrolle durchgeführt noch eine betriebliche Datenschutzbeauftragte oder ein betrieblicher Datenschutzbeauftragter bestellt wurde, montierte der Geschäftsführer die Videokameras letztendlich ab.

13.3 Toiletten in einem Großhandel

Uns erreichte eine Beschwerde, wonach in den Geschäftsräumen eines Großhändlers neben anderen Bereichen auch die Toiletten videoüberwacht werden. Zudem habe der Geschäftsführer jederzeit vor Ort Zugriff auf die Videobilder. Der Geschäftsführer bestritt die Überwachung der Toiletten vehement. Aufgrund einer Prüfung vor Ort stellten wir jedoch an einem Monitor im Verkaufsbüro fest, dass tatsächlich eine Kamera die Toilettentüren erfasste und die Bilder live auf dem Monitor zu sehen waren. Dadurch konnten der Geschäftsführer und die Beschäftigten im Verkaufsbüro zumindest während der Bürozeiten feststellen, wer sich wie oft und wie lange in welchem Toilettenraum aufhielt. Zudem hatte der Geschäftsführer einen Zugriff auf die Videodaten über seinen Arbeitsplatzrechner. Auch wurden die Bilddaten bis zu drei Monaten gespeichert. Hierdurch wurden die Persönlichkeitsrechte der Beschäftigten und sonstiger Personen wie Handwerkerinnen und Handwerker sowie Besucherinnen und Besucher erheblich verletzt, weil sie nicht unbeobachtet die Toilettenräume betreten und verlassen konnten und der Geschäftsführer die Möglichkeit hatte, unbemerkt das Betreten und Verlassen der Toiletten zu kontrollieren. Die Zugriffe durch den Geschäftsführer wurden nicht protokolliert. Diese gravierenden Mängel waren nicht verwunderlich, da die gesetzlich vorgeschriebene Vorabkontrolle nicht

durchgeführt worden war. Erst wenige Tage vor dem Prüftermin wurde eine betriebliche Datenschutzbeauftragte bestellt.

Wir gaben der Firma auf, die Kameras so auszurichten, dass die Toilettentüren nicht mehr erfasst werden können und entsprechende technische Maßnahmen zu treffen. Ebenso verlangten wir neben anderen Anforderungen eine Verkürzung der Speicherfrist für die übrige Videoüberwachung der Geschäftsräume auf das notwendige Maß. Das Unternehmen bestätigte die Umsetzung dieser Anforderungen.

13.4 Tonüberwachung und Videoüberwachung am Arbeitsplatz

Wir erhielten eine Beschwerde, wonach am Empfangstresen im Eingang des Büros eines Unternehmens eine Videokamera mit Mikrofonfunktion und Lautsprecherfunktion installiert sei und dabei auch Arbeitsplätze überwache. Die Kamera sei schwenkbar, sodass die dort arbeitende Beschäftigte permanent überwacht werden könnte. Ebenso könnten ihre Telefongespräche mitgehört beziehungsweise aufgezeichnet werden.

Die Firma erklärte, die Kamera diene zur Prävention und Aufklärung eines möglichen Diebstahls. Die Kamera sei nur zwischen 19:00 und 06:00 Uhr und am Wochenende in Betrieb. Die Tonfunktion sei nicht aktiviert. Zur näheren Erläuterung war der Antwort eine Stellungnahme des betrieblichen Datenschutzbeauftragten beigefügt, nach der es Zweck der Kamera sei, die Eingangstür der Büroetage während der Geschäftszeiten zu erfassen, um den Beschäftigten im Büro zu ermöglichen, die klingelnde Person zu sehen ohne zum Eingang laufen zu müssen.

Wir erklärten dem Unternehmen, dass zur Zugangskontrolle der Einsatz einer Videokamera im Eingangsbereich am Empfangstresen nur zulässig ist, wenn es dazu keine zumutbare Alternative gibt und schutzwürdige Interessen der Betroffenen nicht überwiegen. Zumutbar wäre es gewesen, die Kamera als Live-Video anstelle am Empfangstresen im Eingangsbereich neben oder an der Eingangstür zum Büro zu installieren und ausschließlich auf die Eingangstür auszurichten. In diesem Fall würden die schutzwürdigen Interessen der sich am Eingangstresen aufhaltenden Beschäftigten gewahrt, weil sie nicht mehr von der Kamera erfasst würden. Außerdem müssten die Videodaten nach maximal 72 Stunden automatisch gelöscht werden. Die Tonfunktion wäre irreversibel zu deaktivieren, weil die einfache Deaktivierung ohne besonderen Aufwand jederzeit aktiviert und insoweit unbefugt das gesprochene Wort von Personen aufgezeichnet werden kann, was strafbewehrt ist.

Nach Erhalt unserer Stellungnahme erklärte die Firma, die Kamera sei vor dem Hintergrund der Irritationen in der Belegschaft ersatzlos abgebaut worden.

13.5 Kameras an öffentliche Bereiche angrenzenden Betriebsgebäuden

Im Berichtsjahr wurden an uns mehrere Beschwerden über Videokameras herangetragen, die an Fassaden von Betriebsgebäuden befestigt waren, die wiederum direkt an öffentlichen Fußwegen, Straßen und Parkplätzen angrenzten. Hierbei handelte es sich vorwiegend um Fälle, in denen die Betreiber der Kameras ihr Eigentum vor Einbruch und Vandalismus schützen wollten, wobei jedoch durch die Ausrichtung der Kameras auch immer öffentliche Bereiche mit erfasst wurden.

Nach dem Bundesdatenschutzgesetz ist die Videoüberwachung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. In vielen Fällen der Überwachung von Hausfassaden stützen sich die Betreiber der Anlagen auf die Wahrnehmung des Hausrechts. Dieses rechtfertigt es jedoch nicht, öffentliche Straßen, Wege und Parkplätze mit zu erfassen. Eine Überwachung der Hausfassaden ist grundsätzlich nur zulässig, wenn dabei nicht auch öffentlich zugängliche Bereiche erfasst werden. Sollte dies jedoch nicht vermieden werden können, weil etwa die Hausfassade direkt an einen Fußweg angrenzt, darf die Überwachung nur auf das zwingend notwendige Ausmaß beschränkt werden und einen maximal einen Meter breiten Streifen entlang der Fassade erfassen. Voraussetzung ist allerdings, dass es sich nachweislich um einen besonders einbruchsgefährdeten oder beschädigungsgefährdeten Bereich handelt.

In allen Fällen erreichten wir, dass die Kameras entweder entsprechend neu ausgerichtet wurden und nur noch der unmittelbare Fassadenbereich erfasst wird oder mit irreversiblen Schwärzungen bei der Bildspeicherung gearbeitet wird, sodass öffentliche Bereiche nicht mehr erfasst werden. Außerdem wurden an den Fassaden deutlich sichtbare Hinweisschilder angebracht, die auf eine Videoüberwachung hinweisen.

13.6 Fitnessstudio

Im März führten wir in einem Fitnessstudio eine datenschutzrechtliche Prüfung der installierten Videoüberwachungsanlage durch. Hierbei sahen wir die jeweils installierten Kameras im Eingangsbereich und an den Feuerwehrnottüren als datenschutzrechtlich zulässig an. Im eigentlichen Trainingsbereich sowie im Saunabereich waren keine Kameras installiert. Problematisch war jedoch eine im Herrenumkleidebereich angebrachte Domekamera, die über der Durchgangstür zum Fitnessbereich angebracht war. Diese Kamera war installiert worden, weil es zuvor in diesem Bereich zu einem gewaltsamen Aufbruch mehrerer Spinde gekommen war. Durch die dunkle Abdeckung der Kuppel wurde bei den Besucherinnen und Besuchern der Eindruck erweckt, dass auch der Kabinengang,

Teilbereiche der Spinde sowie die sich davor befindlichen Umkleidebereiche mit erfasst werden. Bei den von der Kamera erfassten Bereichen handelt es sich um einen öffentlich zugänglichen Raum im Sinne des Bundesdatenschutzgesetzes, weil er von allen betreten werden kann, die den Eintrittspreis entrichtet haben. Eine Videobeobachtung öffentlich zugänglicher Räume durch nicht öffentliche Stellen ist nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Insoweit bedurfte es einer angemessenen Abwägung beider Rechtsgüter. Aufgrund der von der Geschäftsführung dargelegten Gründe zur Installation der Kamera bestanden keine Zweifel am berechtigten Interesse, das Eigentum des Fitnessstudios vor Vandalismus zu schützen. Allerdings ist eine Videobeobachtung unzulässig, wenn Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Beim Umkleidebereich handelt es sich um einen Bereich, in dem auch die letzten Hüllen fallen, und somit der letzte höchstpersönliche Lebensbereich der Besucherinnen und Besucher, nämlich deren Intimsphäre, betroffen ist. Diese ist unter allen Umständen zu respektieren und zu schützen. Außerdem überwiegen schutzwürdige Interessen der Betroffenen, wenn eine gezielte Überwachung einzelner Personen möglich ist, durch die die Betroffenen zu einem Objekt der Beobachtung werden, der sie sich nicht entziehen können. Hinsichtlich der Überwachung des Umkleidekabinengangs, der Spindbereiche mit den davor befindlichen Umkleidebereichen sowie der Zugangstür war es den Betroffenen nicht möglich, dieser Beobachtung auszuweichen. Sie waren damit erheblich in ihrem Persönlichkeitsrecht verletzt. Wir kamen daher zu dem Ergebnis, dass die schutzwürdigen Interessen der Betroffenen überwiegen und aus diesem Grund die Kamera abzumontieren ist. Auf unsere Beanstandung hin reagierte die Geschäftsführung umgehend und entfernte die Kamera. Des Weiteren forderten wir die Geschäftsführung auf, die Einsichtnahme und Entnahme von gespeicherten Bilddaten zu protokollieren. Aus den Protokollen muss ersichtlich sein, welche Person, zu welchen Zwecken und unter welchen Voraussetzungen Einsicht in die Bilddaten genommen hat.

13.7 Einkaufszentren

Wie schon in den Vorjahren war auch in diesem Berichtszeitraum die Videoüberwachung in Einkaufszentren ein aktuelles Thema. Vor allem ging es dabei darum, wie die zu privaten Zwecken installierten Videokameras in Einkaufszentren von der Landespolizei genutzt werden können.

Die gegenwärtige Rechtslage stellt sich folgendermaßen dar: Die Betreiber von Einkaufszentren dürfen Kameras installieren, um gesetzlich akzeptierte Ziele wie Diebstahlschutz zu verfolgen. Voraussetzung ist, dass sie sich hierbei im Rahmen der gesetzlichen Vorgaben nach § 6 b Bundesdatenschutzgesetz (BDSG) halten. Allerdings gibt

es keine gesetzliche Verpflichtung, alle gesetzlich erlaubten Kameras tatsächlich zu installieren. Dies erklärt, warum beispielsweise die Einkaufszentren im Land Bremen eine unterschiedliche Videoüberwachungsdichte aufweisen. Auch zeigt die Prüfpraxis, dass teilweise eine reine Beobachtung (Monitoring) stattfindet, um gezielt Wachpersonal einsetzen zu können, und deshalb nicht immer alle Videodaten aufgezeichnet werden.

Sofern die Betreiber von Einkaufzentren sich dafür entschieden haben, Kameras zu installieren, dürfen die entstehenden Bilder nach § 6 b Absatz 3 Satz 2 BDSG von der Polizei genutzt werden, "soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist". Darüber hinaus hat die bremische Polizei nach dem Bremischen Polizeigesetz (BremPolG) im Zusammenhang mit der Videoüberwachung Befugnisse zur Videoüberwachung mit eigenen Kameras. So kann sie nach § 29 Absatz 3 BremPolG öffentlich zugängliche Orte, an denen vermehrt Straftaten begangen werden oder bei denen aufgrund der örtlichen Verhältnisse die Begehung von Straftaten besonders zu erwarten ist, mittels Bildübertragung und Bildaufzeichnung offen und erkennbar beobachten, wenn dies zur Abwehr von Gefahren für die öffentliche Sicherheit inklusive der Verhütung von Straftaten erforderlich ist.

Ein Genehmigungsverfahren für von Privaten betriebene Videokameras in Einkaufszentren ist gesetzlich nicht vorgesehen. Vor dem Einsatz von Videokameras muss die private Betreiberin beziehungsweise der private Betreiber jedoch eine datenschutzrechtliche Vorabkontrolle durchführen, an der auch die oder der betriebliche Datenschutzbeauftragte beteiligt werden muss. Eine Videoüberwachung in Einkaufszentren ist weder grundsätzlich unzulässig noch grundsätzlich zulässig. Zu klären ist im Einzelfall, in welchen Bereichen eine Videoüberwachung tatsächlich erforderlich und geeignet ist, um die mit der Videoüberwachung beabsichtigten gesetzmäßigen Ziele der Betreiberin und der Betreiber wie Diebstahlsschutz zu erreichen, und ob keine überwiegenden schutzwürdigen Interessen von Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeitern entgegenstehen. Darüber hinaus können die Erfassungsbereiche der Kameras durch irreversible Schwärzungen auf das zur Zweckerreichung unbedingt Erforderliche begrenzt werden. Da die Einkaufszentrenketten überregional verteilt sind, arbeiten die datenschutzrechtlichen Aufsichtsbehörden in Deutschland eng zusammen. Die Aufsichtsbehörden sehen Kameras an Geldautomaten, in Gastronomiebereichen inklusive Verweilzonen, in Fahrstühlen, an Fahrtreppen, an Laufwegen inklusive Verweilzonen, in Toiletten und Toilettenzugängen sowie in Umkleidebereichen als grundsätzlich unzulässig an. In diesen Bereichen ist den privaten Betreiberinnen und Betreibern der Einsatz von Kameras allenfalls dann möglich, wenn die Erforderlichkeit sowie deren Zweckmäßigkeit nachgewiesen werden können und es sich bei den erfassten Bereichen um solche handelt, die von den Besucherinnen und Besuchern des Einkaufszentrums nur durchschritten werden, um zu den Geschäften im Zentrum zu gelangen oder dieses wieder zu verlassen, nicht um dort zu verweilen.

Der Bundesminister des Inneren legte am 2. November 2016 den Entwurf für ein "Videoüberwachungsverbesserungsgesetz" vor. Danach soll § 6 b Absatz 1 BDSG folgender Satz 2 angefügt werden:

> "Bei öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Einrichtungen und Fahrzeugen des öffentlichen Personenverkehrs ist der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als wichtiges öffentliches Interesse bei der Abwägungsentscheidung nach Satz 1 Nummer 3 in besonderem Maße zu berücksichtigen."

Darüber hinaus soll nach § 6 b Absatz 3 Satz 1 BDSG folgender Satz eingefügt werden:

> "Absatz 1 Satz 2 gilt entsprechend."

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) forderte den Bundesinnenminister in ihrer Entschließung vom 9. November 2016 (siehe hierzu Ziffer 18.8 dieses Berichts) auf, den Gesetzesentwurf zurückzuziehen. Dort heißt es wörtlich: "Der Gesetzesentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzesentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungener Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen. Gleichwohl lässt es die einschlägige Bestimmung des § 6 b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Absatz 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des Bundesministeriums des Innern suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des

Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben. Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen. Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen. Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landesgesetzliche und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen."

Der Entwurf des Bundesministeriums des Inneren für das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) übernahm in nur wenig veränderter Form die Formulierung des Videoüberwachungsverbesserungsgesetzes. Die genannte Kritik gilt damit auch hierfür.

14. Auskunfteien, Inkasso, Kreditwirtschaft

14.1 Betrügerische Inkassoschreiben

Bereits im Jahr 2013 hatte sich eine Betroffene an uns gewandt und uns um Hilfe bei der Durchsetzung ihres Rechts gebeten. Sie hatte von einem als "Inter Media Finanz Management" firmierenden angeblichen Inkassodienstleister aus Bremen eine Mahnung und schriftliche Zahlungsaufforderung erhalten. Da sich die Betroffene nicht erklären konnte, worauf diese Forderung beruhen sollte und wie der angebliche Inkassodienstleister an ihre Kontaktdaten gekommen war, schrieb sie diesen an und machte ihren datenschutzrechtlichen Auskunftsanspruch geltend. Auf ihr, an die im Briefkopf des Inkassoschreibens angegebene Adresse gerichtetes Auskunftsersuchen erhielt sie jedoch keine Antwort, ein Einschreiben konnte nicht zugestellt werden.

Bei unseren Nachprüfungen ergab sich, dass ein Unternehmen "Inter Media Finanz Management" nicht im Handelsregister eingetragen war. Es handelte sich also nur um eine rechtlich nicht existente Scheinfirma. Auch im Rechtsdienstleistungsregister, geführt beim Landgericht Bremen als zuständiger Registrierungsstelle, war unter dieser Firma keine Person respektive Stelle als Inkassodienstleister registriert. Die im Briefkopf des Inkassoschreibens angegebene Geschäftsadresse war ebenso unzutreffend wie die angegebene Telefonnummer und Homepage-Angabe. Lediglich die zum Ausgleich der Forderung angegebene IBAN (International Bank Account Number, Internationale Bankkontonummer) wies auf ein Konto bei einem Kreditinstitut oder Finanzdienstleister im Ausland hin. Da wir also mit den uns zur Verfügung stehenden Mitteln keine datenverarbeitende Person oder Stelle ermitteln konnten, konnten wir der Betroffenen bei der Durchsetzung ihres Auskunftsanspruchs nicht helfen, mussten das Verfahren einstellen. Da allerdings offenkundig war, dass die Betroffene und möglicherweise auch andere Personen durch Vortäuschen einer Forderung betrogen werden sollten, gaben wir die Angelegenheit an die Staatsanwaltschaft zur Prüfung der Einleitung strafrechtlicher Ermittlungen gegen Unbekannt ab. Im aktuellen Berichtszeitraum erreichte uns dann die erfreuliche Nachricht der Staatsanwaltschaft, dass einige für die Abzockmasche der "Inter Media Finanz Management" verantwortliche Personen ermittelt und gegen sie Strafverfahren eingeleitet worden seien.

14.2 Einhaltung datenschutzrechtlicher Unterrichtungspflichten bei Inkassounternehmen

Im Zuge einer Gesetzesnovellierung wurde im Jahr 2010 eine Vorschrift neu in das Bundesdatenschutzgesetz aufgenommen, die ausdrücklich festlegt, unter welchen Voraussetzungen Informationen über Forderungsschulden einer Person an sogenannte Wirtschaftsauskunfteien, die Bonitätsdaten sammeln, weitergegeben werden dürfen. Zugelassen hat der Gesetzgeber in der einschlägigen Vorschrift eine Meldung über Schulden einer Person an eine Auskunftei unter anderem auch dann, wenn

a) der Betroffene, also der tatsächliche oder vermeintliche Schuldner, nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

c) die verantwortliche Stelle den Betroffenen beziehungsweise Schuldner rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

d) der Betroffene beziehungsweise Schuldner die Forderung nicht bestritten hat.

Welche Informationen im Detail die gesetzlich vorgeschriebene Unterrichtung nach Buchstabe c) vor Ausführung der Datenübermittlung enthalten muss, ist zwar umstritten. Nach zwei höchstrichterlichen Entscheidungen des Bundesgerichtshofs ist jedoch die entscheidende Frage geklärt, nämlich dass in der Unterrichtung ausdrücklich und für jedermann verständlich darauf hingewiesen werden muss, dass ein Bestreiten der Forderung eine Informationsübermittlung an Auskunfteien ausschließt. Gesetzgeberischer Zweck der Unterrichtung ist es nämlich, den tatsächlichen oder vermeintlichen Schuldnerinnen beziehungsweise Schuldnern von Forderungen vor Augen zu führen, was passiert, wenn sie weiterhin nicht auf die geltend gemachte Forderung reagieren und ihnen zugleich deutlich zu machen, dass sie im Fall des Nichtbestehens der Forderung auch die Möglichkeit haben, die Übermittlung einer fehlerhaften Forderungsinformation an Auskunfteien auszuschließen, eben indem sie die Forderung bestreiten. Dies könnte zum Beispiel unter Hinweis darauf erfolgen, dass kein Vertrag geschlossen wurde, der Vertrag wirksam gekündigt wurde oder dass bereits bezahlt wurde.

Da diese Befugnis zur Forderungsmitteilung an Auskunfteien insbesondere für Inkassounternehmen von besonderer Bedeutung ist, weil sie mit dem Hinweis auf eine Mitteilung an Auskunfteien zusätzlichen Zahlungsdruck bei Betroffenen erzeugen können, kontrollierten wir im Berichtszeitraum registrierte Inkassounternehmen in Bremen daraufhin, ob sie Schuldnerinnen und Schuldner ordnungsgemäß unterrichten. Lediglich bei einem der überprüften Unternehmen mussten wir feststellen, dass der Unterrichtungspflicht nicht ordnungsgemäß nachgekommen wurde. Erst als wir androhten, mit einer Anordnung eine Änderung des bisherigen Unterrichtungstextes zu erzwingen, reagierte das Unternehmen und änderte seinen Unterrichtungstext ab.

14.3 Fehlerhafte Datenspeicherung einer Wirtschaftsauskunftei

Die Hauptgeschäftstätigkeit von Wirtschaftsauskunfteien liegt in der Sammlung und Beauskunftung von Wirtschaftsinformationen, also im massenhaften Umgang mit personenbezogenen Daten. Konflikte und Beschwerden Betroffener sind vorprogrammiert, insbesondere da Negativeintragungen beziehungsweise Negativauskünfte von Auskunfteien die persönliche Lebensgestaltung empfindlich beeinflussen können. Aus dem Berichtszeitraum sei ein Fall geschildert, der nach Auswirkung wie Umfang des Rechtsverstoßes nicht gravierend, aber eben typisch ist:

Ein Betroffener legte uns in Kopie eine Aufstellung der zu seiner Person gespeicherten Daten einer Auskunftei vor. Er hatte diese in Ausübung seines Betroffenenauskunftsanspruchs erhalten. Unter den Zahlungsinformationen fand sich ein Hinweis auf ein abgeschlossenes außergerichtliches Inkassoverfahren über eine Forderung eines Geräte-Reparaturservices. Wie uns der Betroffene nachweisen konnte, hatte er diese

Forderung aber bereits gegenüber dem Reparaturservice als unberechtigt zurückgewiesen. Aus seiner Sicht hatte es überhaupt keinen Vertragsabschluss gegeben, der zu einer solchen Forderung hätte berechtigen können. Ein zivilgerichtliches Klageverfahren zur Klärung dieses Forderungsstreits war seitens des Reparaturservices nicht angestrengt worden. Die Existenz der Forderung war also umstritten. Der Reparaturservice hatte allerdings die umstrittene Forderung an ein Inkassobüro zwecks Durchsetzung abgegeben, dabei aber nicht auf das Bestrittensein der Forderung durch den vermeintlichen Schuldner hingewiesen. Der Betroffene selbst sah sich nicht veranlasst, außerhalb eines Gerichtsverfahrens auf die aus seiner Sicht unbegründeten Forderungsschreiben des Inkassobüros zu reagieren. Das Inkassobüro stellte schließlich seine Bemühungen um einen Forderungseinzug ergebnislos ein, übermittelte aber zuvor noch die Forderung an eine Wirtschaftsauskunftei. Forderungen gegenüber natürlichen Personen, die nicht gerichtlich verifiziert sind oder deren Existenz nicht eindeutig und ausdrücklich durch die Schuldnerin beziehungsweise durch den Schuldner anerkannt ist, dürfen nur unter bestimmten Voraussetzungen an Auskunfteien übermittelt werden. Ausgeschlossen ist eine Übermittlung insbesondere auch dann, wenn die Forderung bestritten ist, wie es vorliegend der Fall war.

Wir veranlassten daher die Löschung des fehlerhaften Inkassoverfahrenseintrags zum Betroffenen bei der Auskunftei. Für eine Sanktionierung der fehlerhaften Datenspeicherung blieb kein Raum, da die Auskunftei keine Kenntnis davon hatte und auch nicht haben konnte, dass es sich um eine seitens des vermeintlichen Schuldners bestrittene Forderung handelte.

14.4 Die ungelöste Scoring-Problematik

Bereits im letzten Jahresbericht hatten wir in Bezug auf Scoringverfahren der Wirtschaftsauskunfteien über den dringenden gesetzlichen Reformbedarf berichtet, den nicht zuletzt eine seitens der Bundesregierung in Auftrag gegebene Studie aufgezeigt hatte (siehe hierzu 38. Jahresbericht, Ziffer 13.6). Obwohl der Parlamentarische Staatssekretär des Bundesministeriums der Justiz und für Verbraucherschutz bei der Vorstellung der Studie Ende des Jahres 2015 geäußert hatte: "Die Studie hat einmal mehr bestätigt, wie wichtig ein klarer Rechtsrahmen für das Scoring ist. Wir nehmen die Ergebnisse der Studie ernst, denn das Scoring ist für Verbraucherinnen und Verbraucher von fundamentaler Bedeutung. Es darf nicht sein, dass jemand zu Unrecht ein Darlehen nicht erhält, eine Wohnung nicht anmieten kann oder im Versandhandel nicht auf Rechnung bestellen kann.", unterbreitete die Bundesregierung dem Bundestag keine gesetzlichen Reformvorschläge.

In dieses Bild passt auch die parlamentarische Behandlung eines Gesetzesentwurfs zur Verbesserung der Scoringbedingungen, den die Fraktion Bündnis 90 / Die Grünen im Mai 2015 in den Bundestag eingebracht hatte (Drucksache 18/4864). Dieser wurde in der ersten Beratung im Bundestag an mehrere Fachausschüsse zur weiteren Erörterung

überwiesen. Im Juni 2015 wurde noch ein weiterer Fachausschuss mit der Erörterung betraut. Seitdem finden sich keine Spuren des Gesetzesentwurfs mehr im parlamentarischen Betrieb.

Die defizitäre Rechtslage beim Scoring soll nun also offenbar im Interesse der scoringbetreibenden Wirtschaftsauskunfteien bis zur Anwendbarkeit der Europäischen Datenschutzgrundverordnung im Mai 2018 beibehalten werden (siehe hierzu Ziffer 2.5 dieses Berichts).

14.5 Unterrichtungspflicht bei Datenerhebungen nach dem Geldwäschegesetz

Mit einem Erfolg konnten wir im aktuellen Berichtszeitraum ein Klageverfahren vor dem Oberverwaltungsgericht in der Berufungsinstanz beenden, dem folgender Sachverhalt zugrunde lag: Bereits im Jahr 2010 hatten wir eine datenschutzrechtliche Prüfbitte hinsichtlich Datenerhebungen eines Kreditinstituts im Zusammenhang mit der Eröffnung eines sogenannten Mietkautionstreuhandkontos erhalten. Mietkautionstreuhandkonten dienen der vermietenden Partei dazu, ausgehändigte Mietkautionen der Mietpartei gesondert vom sonstigen Vermögen anzulegen. Inhaberin beziehungsweise Inhaber des Mietkautionstreuhandkontos ist die Vermieterin beziehungsweise der Vermieter, wirtschaftlich Berechtigte oder Berechtigter des hinterlegten Geldbetrags hingegen die Mieterin beziehungsweise der Mieter. Bei der Eröffnung eines solchen Kontos hatte sich die kontoeröffnungswillige Person gewundert, warum sie in dem ihr zum Ausfüllen vorgelegten Kontoeröffnungsformular Vorname(n), Nachname, Anschrift und Geburtsdatum sowie Geburtsort des Mieters angeben sollte. Das Konto werde doch schließlich von ihr allein geführt. Auch auf gezielte Nachfrage konnte ihr die Bankmitarbeiterin den Grund dieser Datenabfrage im Formular nicht erläutern.

Wird ein Konto eröffnet, muss ein Kreditinstitut nach den Vorgaben des Geldwäschegesetzes bestimmte Identifizierungen vornehmen. Handelt es sich um ein Treuhandkonto, muss das Kreditinstitut nicht nur die kontoeröffnende Kundin beziehungsweise den kontoeröffnenden Kunden, als Vertragspartnerin beziehungsweise Vertragspartner identifizieren, sondern auch die Treugeberin oder den Treugeber beziehungsweise die wirtschaftlich Berechtigten des angelegten Geldbetrags, vorliegend also den Mieter. Da der vorstehend genannte Umfang der Datenerhebung des Kreditinstituts zur Identifizierung des Mieters aus unserer Sicht über die Vorgaben des Geldwäschegesetzes hinausging und das Unterlassen einer Information gegenüber der kontoeröffnenden Person über Grund und Zweck dieser Datenerhebungen zu seiner Mietpartei gegen das Bundesdatenschutzgesetz verstieß, verpflichteten wir nach erfolgloser Anmahnung rechtmäßigen Verhaltens im Frühjahr 2012 das Kreditinstitut mit einer

Anordnung zur Beseitigung dieser Rechtsverstöße. Das Kreditinstitut erhob daraufhin Klage gegen unsere Anordnung.

Im Laufe des erstinstanzlichen Prozesses erledigte sich ein Klageteil durch eine überraschende Änderung des Geldwäschegesetzes. Mit der Gesetzesänderung wurde der Datenerhebungsumfang zum Treugeber ausgeweitet, indem nunmehr auch Geburtsdatum, Geburtsort und Anschrift als generell zu erhebende Daten festgelegt wurden. Hierüber berichteten wir bereits in unserem 36. Jahresbericht unter Ziffer 17.1 ausführlich. Im Rechtsstreit weiter zu klären war aber die Frage der Rechtmäßigkeit des zweiten Teils unserer Anordnung. Darin hatten wir dem Kreditinstitut eine Unterrichtung der Kontoeröffnenden über Zwecke, Empfängerkategorien und Rechtsgrundlage einer solchen Datenerhebung und Datenspeicherung über die Mieterinnen und Mieter aufgegeben. Rechtliche Grundlage für diese Vorgabe an das Kreditinstitut war das Bundesdatenschutzgesetz, welches vorschreibt, dass datenverarbeitende Stellen grundsätzlich immer dann, wenn sie personenbezogene Daten unmittelbar bei einer oder einem Betroffenen erfragen, über die Identität, die Zweckbestimmungen der Datenerhebung und Datenverwendung und die Empfängerkategorien informieren müssen. Beruht die Datenerhebung auf einer gesetzlichen Verpflichtung, muss zusätzlich auch über das entsprechende Fachgesetz, das diese Verpflichtung enthält, informiert werden. Betroffene sollen durch diese Information in die Lage versetzt werden, durch Gesetzeslektüre die Zulässigkeit der Datenerhebung zu kontrollieren. Das Kreditinstitut hatte bestritten, dass es zu einer solchen Information der Kontoeröffnenden verpflichtet sei. Die Unterrichtungspflicht des Bundesdatenschutzgesetzes greife nicht ein, denn Vermieterinnen und Vermieter seien bezüglich der anzugebenden Daten ihrer Mieterinnen und Mieter nicht betroffen. Wir hingegen gingen davon aus, dass Angaben dazu, wen eine Vermieterin beziehungsweise ein Vermieter als ihre beziehungsweise seine Mietpartei und Vertragspartei ausgesucht hat und wo seine Mieter wohnen, also zur Anschrift des vermieteten Objekts, zugleich auch Angaben über sachliche Verhältnisse der Vermieterin oder des Vermieters, und damit auch ihre oder seine personenbezogenen Daten sind. Dies löst unserer Auffassung nach die Informationspflicht nach dem Bundesdatenschutzgesetz, insbesondere über Zweckbestimmungen der Datenerhebung und Datenverwendung und die Empfängerkategorien und die Rechtsgrundlage der Datenerhebung gegenüber der Vermieterin beziehungsweise dem Vermieter, aus.

In erster Instanz hatte das Verwaltungsgericht die Rechtsansicht des Kreditinstituts geteilt. Da dieses Urteil aus unserer Sicht die datenschutzrechtliche Rechtslage verkannt hatte, legten wir Rechtsmittel gegen das Urteil ein. In der mündlichen Berufungsverhandlung signalisierte das Oberverwaltungsgericht dem Kreditinstitut, dass eindeutig die von uns angemahnte Informationspflicht gegenüber Vermietern bestehe und daher ein Urteil zu unseren Gunsten erginge, sollte es nicht zu einer vergleichsweisen Einigung mit uns

kommen. Das Kreditinstitut erklärte sich daraufhin zu einer Information wie von uns gefordert bereit. Wir stimmten mit dem Kreditinstitut einen Informationstext ab und schlossen einen Prozessvergleich mit diesem Inhalt vor dem Oberverwaltungsgericht. Der abgestimmte Informationstext wurde seitens des Kreditinstituts in das Kontoeröffnungsformular für das Mietkautionstreuhandkonto aufgenommen. Kundinnen und Kunden werden nunmehr darüber unterrichtet, dass die Datenerhebung über Mieterinnen und Mieter aufgrund einer Rechtspflicht des Kreditinstituts aus dem Geldwäschegesetz erfolgen und unter bestimmten Umständen die erhobenen Daten an bestimmte Behörden zwecks Geldwäschebekämpfung weitergegeben werden müssen.

Exemplarisch zeigt dieses Verfahren, welcher enorme Aufwand notwendig ist und wie lange es dauern kann, Anforderungen des Datenschutzrechts durchzusetzen, selbst wenn sie für Unternehmen ohne nennenswerten Aufwand umzusetzen sind.

14.6 Fehlerhafte Kontenübersicht beim Online-Banking

Auch das Online-Banking sorgt hin und wieder für Überraschungen. Ein Kunde eines Kreditinstituts wandte sich an uns und bat um unsere Hilfe. Er war als Kassenwart bei Verein X und Verein Y tätig und verfügte jeweils über einen Online-Banking-Zugang zu den Vereinskonten bei diesem Kreditinstitut. Kürzlich hatte er auch bei einem weiteren Verein Z das Amt des Kassenwarts übernommen. Er wurde daher auch seitens des Vereins Z mit einer Kontovollmacht versehen und es wurde ein Online-Banking-Zugang zu dem Vereinskonto beantragt. Das Konto des Vereins Z wurde ebenfalls durch dasselbe Kreditinstitut geführt.

Einige Tage nach Beantragung des Online-Zugangs zum Konto des Vereins Z, wollte der Kassenwart den Kontenstand bei Verein X kontrollieren. Nachdem er sich beim Konto des Vereins X online eingeloggt hatte, überraschte ihn der unerwartet hohe Kontostand. Bei näherem Hinsehen entdeckte er in der Online-Kontenübersicht, dass dort nicht nur das Konto des Vereins X aufgelistet war, sondern er zugleich auch das Konto des Vereins Z einsehen konnte, zu dem er sich nicht eingeloggt hatte. Und die Kontenstände der Vereine X und Z waren in der Online-Gesamtübersicht kurzerhand saldiert worden, woraus der angezeigte hohe Kontenstand bei Verein X resultierte.

Datenschutzrechtlich muss eine datenverarbeitende Stelle durch technisch-organisatorische Maßnahmen sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden können und dass auf Datenbestände ausschließlich durch Zugriffsberechtigte entsprechend dem Umfang ihrer Berechtigung zugegriffen werden kann. Auch wenn es sich vorliegend an und für sich nicht um Daten einer natürlichen Person im Sinne des Bundesdatenschutzgesetzes, sondern von Vereinen handelte, wandten wir uns an

das Kreditinstitut. Dieses behob auf unser Ersuchen unmittelbar diese technisch-organisatorische Panne.

15. Dienstleistungen, Handel, Gewerbe, Mieterdatenschutz

15.1 Zahlungsmahnung mittels offener E-Mail an alle Schuldnerinnen und Schuldner

Ein Bremer Unternehmen hatte offenbar Schwierigkeiten mit der Zahlungsmoral etlicher seiner Kundinnen und Kunden. Um die offenen Beträge bei den Säumigen anzumahnen, versandte ein Mitarbeiter des Unternehmens unter dem Betreff "Offene Rechnung" kurzerhand eine E-Mail. In dieser wies er auf die Zahlungssäumnis und den alsbaldigen Zugang einer postalischen Mahnung hin. Zum Versand dieser E-Mail nutzte er das "offene", also für jeden Empfänger einsehbare E-Mail-Adressfeld "An" statt des "verdeckten" Adressfeldes "BCC" (zur Problematik siehe hierzu 37. Jahresbericht, Ziffer 14.1). Die genutzten E-Mail-Adressen der säumigen Kundinnen und Kunden im Adressfeld waren dabei überwiegend personalisiert, bestanden also aus Name und Vorname (beziehungsweise Anfangsbuchstabe des Vornamens) sowie gegebenenfalls Zugehörigkeitsangabe zu einem Arbeitgeber, Verein et cetera, waren also bestimmten oder jedenfalls bestimmbaren Personen eindeutig zuzuordnen. Infolgedessen erhielten alle über 100 säumigen Kundinnen und Kunden im Wege dieser E-Mail nicht nur den eigentlichen Nachrichteninhalt, sondern darüber hinaus auch die personalisierten E-Mail-Adressen aller Mit-Empfängerinnen und Mit-Empfänger der E-Mail nebst Informationen über deren Kundeneigenschaft und über die Nichtzahlung einer gekauften Ware. Datenschutzrechtlich betrachtet handelte es sich um eine Übermittlung von Informationen zu persönlichen und sachlichen Verhältnissen bestimmter beziehungsweise jedenfalls bestimmbarer natürlicher Personen, also personenbezogener Daten im Sinne des Bundesdatenschutzgesetzes. Eine Befugnis zu dieser Übermittlung hatte das Unternehmen beziehungsweise dessen Mitarbeiter freilich nicht. Denn weder existierte eine Einwilligung jeder einzelnen Inhaberin beziehungsweise jedes einzelnen Inhabers der E-Mail-Adressen in die Weitergabe dieser personenbezogenen Informationen an sämtliche E-Mail-Mitempfängerinnen und E-Mail-Mitempfänger noch rechtfertigte eine gesetzliche Erlaubnisvorschrift diese Datenübermittlung.

Nachdem wir auf den Sachverhalt aufmerksam geworden waren und das Unternehmen hiermit konfrontiert hatten, zeigte sich der verantwortliche Mitarbeiter des Unternehmens sogleich einsichtig und bedauerte den vorschnellen und unüberlegten Mahnungsversand. Aus unserer Sicht war es gleichwohl geboten, diesen Datenschutzverstoß im Wege eines Bußgeldbescheids zu ahnden. Das verhängte Bußgeld wurde umgehend gezahlt.

15.2 Offenlegung des Abstimmungsverhaltens eines Gesellschafters

Wir erhielten folgenden Sachverhalt zur Prüfung: Der Beschwerdeführer war mit vielen anderen Anlegern zusammen mit einer Geldeinlage an einer Kommanditgesellschaft beteiligt. In einer Versammlung der der Gesellschafterinnen und Gesellschafter der Kommanditgesellschaft seien zu verschiedenen Tagesordnungspunkten Abstimmungen notwendig gewesen. Die Abstimmung sei schriftlich erfolgt, die Abstimmungsunterlagen seien in einer Wahlurne gesammelt worden. Dies führte den Beschwerdeführer zu der Auffassung, die Abstimmung sei auch geheim gewesen. Die Auswertung der Abstimmungsunterlagen und deren spätere Aufbewahrung habe ein gewählter Abstimmungsleiter übernommen. Nun sei er kürzlich von verschiedenen Mitgesellschafterinnen und Mitgesellschafter im Rahmen innergesellschaftlicher Auseinandersetzungen auf sein Abstimmungsverhalten in dieser Gesellschafterversammlung angesprochen worden. Die Mitgesellschafterinnen und Mitgesellschafter hätten dabei genaue Kenntnis seines Abstimmungsverhaltens gehabt. Diese Offenlegung seines Abstimmungsverhaltens vermutlich durch den Abstimmungsleiter verletzte seiner Ansicht nach sein Persönlichkeitsrecht. Wir wandten uns an den Abstimmungsleiter zwecks weiterer Sachverhaltsklärung. Dieser räumte ein, dass er Informationen über das Abstimmungsverhalten auch des Beschwerdeführers zu bestimmten Tagesordnungspunkten auf Anfrage an die Mitgesellschafterinnen und Mitgesellschafter des Betroffenen zur Wahrung deren gesellschaftsrechtlicher Rechte herausgegeben habe.

Entgegen erster Vermutung kamen wir bei näherer rechtlicher Begutachtung zu dem Ergebnis, dass kein Verstoß gegen Bestimmungen des Bundesdatenschutzgesetzes vorlag. Zwar handelte es sich bei der Offenbarung von Informationen zum Abstimmungsverhalten des Betroffenen in der Gesellschafterversammlung eindeutig um eine Übermittlung von Daten zur Person des Betroffenen. Allerdings war der Abstimmungsleiter auf der Grundlage des Bundesdatenschutzgesetz befugt, auch ohne Einwilligung des Betroffenen die fraglichen Informationen an die Mitgesellschafterinnen und Mitgesellschafter herauszugeben. Nach dem Bundesdatenschutzgesetz ist nämlich eine Übermittlung personenbezogener Daten für einen anderen als den Zweck, der der Datenerhebung zugrunde lag, zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

Die Feststellung, Bewertung und Abwägung der berechtigten Drittinteressen einerseits mit den schutzwürdigen Betroffeneninteressen andererseits musste vorliegend maßgeblich die einschlägigen handelsrechtlichen und gesellschaftsrechtlichen Vorschriften und Wertungen berücksichtigen. Weder enthalten das Handelsgesetzbuch noch die auf Gesellschafterversammlungen in Kommanditgesellschaften analog anwendbaren

Bestimmungen des Gesetzes betreffend die Gesellschaften mit beschränkter Haftung (GmbH-Gesetz) ausdrückliche Regelungen zur Form von Abstimmungen in Gesellschafterversammlungen. Auch im Gesellschaftsvertrag der Kommanditgesellschaft selbst war zur Abstimmungsform keine Regelung getroffen. Schließlich hatten auch die Gesellschafterinnen und Gesellschafter selbst in der Versammlung keine besondere Abstimmungsform festgelegt. Die Wahl der Abstimmungsform lag damit letztlich beim Vorsitzenden der Gesellschafterversammlung beziehungsweise dem gewählten Abstimmungsleiter. Der Abstimmungsleiter hatte aber lediglich ein schriftliches Abstimmungsverfahren für alle abzustimmenden Tagesordnungspunkte bestimmt. In der Festlegung einer schriftlichen Abstimmung lag aber entgegen der unausgesprochenen Erwartung des Beschwerdeführers nicht zugleich die Festlegung einer geheimen Abstimmung. Eine geheime Abstimmung ist gesellschaftsrechtlich ein Ausnahmefall des Abstimmungsverfahrens und findet nur dann statt, wenn dies ausdrücklich durch die Gesellschafterversammlung beschlossen oder eben im Gesellschaftsvertrag festgelegt worden ist. Fehlt es wie vorliegend an einem solchen Beschluss beziehungsweise einer solchen Festlegung, so erfolgt die Abstimmung entsprechend dem Normalfall der Abstimmung unter dem Gesichtspunkt gesellschafterlicher Treuepflicht stets in offener Form. Im Übrigen besteht nach ganz überwiegender Ansicht im Fachschrifttum grundsätzlich auch kein Anspruch einer einzelnen Gesellschafterin beziehungsweise eines einzelnen Gesellschafters auf eine geheime Abstimmung.

Aus diesen Gründen war hier also ein berechtigtes Interesse der Mitgesellschafterinnen und Mitgesellschafter anzuerkennen, das Abstimmungsverhaltens ihrer Mitgesellschafterinnen und Mitgesellschafter zu kennen und diese Information für gesellschaftseigene Zwecke in Wahrnehmung ihrer gesellschafterlichen Rechte zu nutzen. Dieses berechtigte Interesse überwog das schutzwürdige Interesse des Betroffenen als (Mit-)Gesellschafter an der Geheimhaltung seines Abstimmungsverhaltens.

15.3 Missachtung des Betroffenenauskunftsrechts

Das gesetzliche Auskunftsrecht der von einer Datenverarbeitung betroffenen Personen gegenüber datenverarbeitenden Stellen wird unserer Einschätzung nach erfreulicherweise mehr und mehr seitens der Betroffenen in Anspruch genommen. Die weitaus meisten Unternehmen scheinen sich zwischenzeitlich auch auf solche Auskunftsbitten eingestellt zu haben. Beschwerden wegen Missachtung des Auskunftsrechts betreffen in unserer Aufsichtspraxis zumeist Unternehmen, deren Geschäftstätigkeit von vornherein gewisse Zweifel aufkommen lässt.

Beispielhaft hierfür sei folgender Fall geschildert: Das seitens eines Betroffenen um Auskunft ersuchte Kleinstunternehmen ist den eigenen Angaben nach geistiger Rechteinhaber

bezüglich Filmmaterials. Tatsächlicher Geschäftsgegenstand scheint allerdings die Abmahnung von Personen wegen behauptet illegaler Downloads des Filmmaterials im Internet zu sein. Ein Betroffener, der wegen eines angeblichen Downloads eine Abmahnung erhalten hatte, machte gegenüber dem Unternehmen seinen datenschutzrechtlichen Auskunftsanspruch geltend. Das Unternehmen reagierte jedoch nicht auf das erste schriftliche Auskunftsgesuch. Das nachfolgend mittels Einschreiben versandte Auskunftsgesuch des Betroffenen konnte wegen Adresswechsels nicht zugestellt werden. Geschäftsadresswechsel sind bei diesem Unternehmen an der Tagesordnung, die geführten Geschäftsadressen aber stets reine Briefkastenanschriften. Der Geschäftsführer des Unternehmens hat seinen Wohnsitz offiziell in Übersee, ist also praktisch kaum zu erreichen und zu belangen. Bei Unternehmen wie diesem stoßen wir bei der Verfolgung des Rechtsverstoßes und der Durchsetzung geltenden Datenschutzrechts leider an praktische Grenzen.

15.4 Weitergabe von Mieterdaten an potenzielle Vermieter

Eine Hausverwaltung übermittelte an alle Wohnungseigentümerinnen und Wohnungseigentümer einer Wohnanlage ein Schreiben mit vermeintlich zutreffenden Informationen über eine ehemalige Mieterin. Es handelte sich um die Mitteilungen, die Mieterin habe massive Probleme mit der Hausverwaltung gehabt, es habe unangenehme Streitigkeiten und Vorkommnisse zwischen der Betroffenen und anderen Bewohnerinnen und Bewohnern des Hauses sowie mit dem Verwaltungsbeirat und der Hausverwaltung gegeben und es sei eine Räumungsklage anhängig. Diese Aussagen sind unbewiesen geblieben. Die Betroffene sah sich in ihren Persönlichkeitsrechten verletzt, weil sie häufiger von teilweise unbekannten Personen auf diese Datenübermittlung angesprochen worden war.

Erst nach Vorlage der Kopie eines anonymisierten Schreibens der Hausverwaltung bestätigte der Verwalter der Wohnanlage uns gegenüber die Datenübermittlung. Wir erklärten ihm, er müsse sich in seinem Verhalten zwar an dem aus dem Wohnungseigentumsgesetz ableitbaren ordnungsgemäßen berechtigten Interesse der Gesamtheit der Wohnungseigentümerinnen und Wohnungseigentümer orientieren. Insoweit sei er befugt, diese über konkrete Risiken zu unterrichten. Dazu gehöre es jedoch nicht, die hier in Rede stehenden Angaben über die ehemalige Mieterin an alle Wohnungseigentümerinnen und Wohnungseigentümer zu übermitteln. Die nicht belegte Aussage, die ehemalige Mieterin habe geäußert, sich in der Wohnanlage erneut um eine Wohnung bewerben zu wollen, stellt kein konkretes Risiko für die anderen Wohnungseigentümerinnen und Wohnungseigentümer dar, da nicht absehbar war, ob, wann und an wen sich die Betroffene als Mietinteressentin wenden würde. Berechtigte Interessen zur Verringerung von Risiken bei Mietvertragsabschlüssen, bestehen grundsätzlich erst bei

einer konkreten Mietvertragsanbahnung. Eine solche lag hier offensichtlich nicht vor, sodass diese Datenübermittlung nicht erforderlich war.

Dagegen überwogen die schutzwürdigen Interessen der Betroffenen an dem Ausschluss der Übermittlung, weil dadurch alle 36 Wohnungseigentümerinnen und Wohnungseigentümer unzulässig unbewiesene nachteilige Informationen über die ehemalige Mieterin erhielten. Nach dem Bundesdatenschutzgesetz sind unzulässig übermittelte Daten bei den Empfängerinnen und Empfängern zu löschen, weil es sich um eine unzulässige Speicherung handelt. Wir verlangten daher von dem Hausverwalter, alle Datenempfängerinnen und Datenempfänger aufzufordern, das besagte Schreiben zu vernichten und sich dies bestätigen zu lassen. Dies sagte die Hausverwaltung zu.

16. Internationales und Europa

16.1 Safe Harbor – Auskunftsersuchen

Die Safe-Harbor-Entscheidung des Europäischen Gerichtshofs vom 6. Oktober 2015 (siehe hierzu 38. Jahresbericht, Ziffer 15.2) hat weitreichende Folgen, was den Datentransfer aus der Europäischen Union (EU) in die Vereinigten Staaten von Amerika (USA) betrifft. Die Unzulässigkeit dieser Rechtsgrundlage führte europaweit zu Unsicherheiten auf Seiten der Unternehmen.

Um einen Überblick über die verschiedenen Grundlagen für Datentransfers in sogenannte Drittländer, insbesondere in die USA, zu bekommen, baten wir im Mai des Berichtsjahres 29 zufällig ausgewählte bremische Unternehmen um Auskunft und erfragten, ob die Unternehmen personenbezogene Daten in die USA übermittelten, auf welcher Rechtsgrundlage die Übermittlung stattfand, wie die entsprechenden technischen und organisatorischen Maßnahmen umgesetzt wurden und ob die Unternehmen über eine betriebliche Datenschutzbeauftragte oder einen betrieblichen Datenschutzbeauftragten verfügten. Ziel des Auskunftsersuchens war dabei auch, die Unternehmen in Bezug auf den internationalen Datentransfer zu sensibilisieren.

Die Auswertung des Auskunftsersuchens ergab ein positives Bild: 16 der 29 angeschriebenen Unternehmen gaben an, dass keine personenbezogenen Daten in die USA übermittelt wurden. Die Auswertung der übrigen Unternehmen lässt den Schluss zu, dass diese – zumindest in Bezug auf das Safe-Harbor-Urteil (Aktenzeichen C-362/14, unter http://curia.europa.eu/juris/documents.jsf?num=C-362/14 abrufbar) – gut informiert und vorbereitet waren. Aus datenschutzrechtlicher Sicht ist besonders hervorzuheben, dass keines der angeschriebenen Unternehmen Safe Harbor als Grundlage für den Datentransfer in die USA nutzte. Einige Bremer Unternehmen waren sogar von sich aus aktiv geworden

und hatten sich unmittelbar nach Bekanntwerden des Urteils bei uns nach alternativen Instrumenten und Möglichkeiten erkundigt. Die Unternehmen setzen gegenwärtig als rechtliche Grundlage neben den EU-Standardvertragsklauseln und den sogenannten verbindlichen Unternehmensregelungen (Binding Corporate Rules, BCR) auch Auftragsdatenverarbeitungsverträge und Einwilligungen ein. Dass auch diese Instrumente mit Vorsicht zu genießen sind, wird unter Ziffer 16.3 dieses Berichts (Auswirkungen des Urteils des Europäischen Gerichtshofs auf andere Rechtsgrundlagen) näher beschrieben. Inzwischen existiert mit dem – zum Zeitpunkt des Auskunftsersuchens noch nicht in Kraft getretenen – sogenannten Datenschutzschild (EU-US Privacy Shield) eine weitere Übermittlungsgrundlage (siehe hierzu Ziffer 16.2 dieses Berichts).

Unsere Auswertung der Befragung ergab aber auch, dass es zum Teil noch Unklarheiten in Bezug auf externe Dienste wie beispielsweise den Betrieb einer facebook-"Fanseite", die Nutzung von Office-Lösungen aus der sogenannten Cloud oder Dienste zur Datenverkehrsanalyse, wie zum Beispiel Google Analytics, gibt. Aufgrund der Nachfragen von Unternehmen zeichnet sich bisher jedoch ab, dass bei diesen inzwischen zumindest ein Problembewusstsein existiert, was die Nutzung externer Dienste betrifft.

Das Auskunftsersuchen, welches in ähnlicher Form auch von den Aufsichtsbehörden anderer Bundesländer durchgeführt worden ist, war der Auftakt für eine bundesweit einheitlich koordinierte Prüfung des internationalen Datenverkehrs im nicht öffentlichen Bereich. Im Rahmen dieser Prüfung, an der sich neben Bremen noch neun weitere Bundesländer beteiligen, wurden bundesweit 500 Unternehmen angeschrieben. Auch hier liegt der Fokus auf Datenübermittlungen in die USA, jedoch wurden nun umfangreichere und einheitliche Anfragen versandt. Mit der finalen Auswertung der koordinierten Prüfung ist im Frühjahr 2017 zu rechnen.

16.2 EU-US Privacy Shield

Bei dem EU-US Privacy Shield (EU-US Datenschutzschild) handelt es sich um ein Abkommen, welches die Europäische Kommission (EU-Kommission) zu Beginn des Berichtsjahres mit den Vereinigten Staaten von Amerika (USA) aushandelte. Das Abkommen reagiert darauf, dass der Europäische Gerichtshof (EuGH) am 6. Oktober 2015 die Safe-Harbor-Entscheidung der EU-Kommission für ungültig erklärt hatte. Nach der Absicht der Vertragsschließenden soll dieses Abkommen europäischen Unternehmen die Möglichkeit geben, personenbezogene Daten in die USA zu übermitteln, was schon Ziel der Safe-Harbor-Entscheidung gewesen war.

Der sogenannte Datenschutzschild besteht aus dem "Durchführungsbeschluss 2016/1250 der EU-Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen

Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes", welcher neben den schriftlichen Zusagen der Regierung der Vereinigten Staaten von Amerika (US-Regierung) in Bezug auf "Garantien und Beschränkungen" für den behördlichen Zugriff auf die übermittelten Daten die sieben, von den teilnehmenden US-amerikanischen Unternehmen einzuhaltenden Datenschutzgrundsätze Informationspflicht, Wahlmöglichkeit, Verantwortlichkeit für Weitergabe, Sicherheit, Datenintegrität und Zweckbindung, Auskunftsrecht sowie Rechtsschutz, Durchsetzung und Haftung enthält. Eine detaillierte Beschreibung dieser Grundsätze ist am Anhang II, Abschnitt II der "Angemessenheitsentscheidung der EU-Kommission"[3] formuliert. Außerdem gibt es nun mit einer Ombudsfrau eine Stelle, an die sich Bürgerinnen und Bürger der Europäischen Union wenden können, um beispielsweise prüfen zu lassen, ob ein zertifiziertes Unternehmen rechtswidrig handelt.

Nachdem die EU-Kommission am 12. Juli 2016 das Abkommen verabschiedet hatte, ist es für US-amerikanische Unternehmen seit dem 1. August 2016 möglich, sich nach den Regeln des EU-US Privacy Shield zertifizieren zu lassen. Dabei muss sich das Unternehmen gegenüber dem Handelsministerium der Vereinigten Staaten auf Einhaltung der Datenschutzgrundsätze verpflichten und seine Datenschutzbestimmungen offenlegen. Ähnlich wie bei der Safe-Harbor-Entscheidung der EU-Kommission gibt es unter https://www.privacyshield.gov/list/ eine vom US-amerikanischen Handelsministerium geführte Liste, auf welcher die zertifizierten Unternehmen veröffentlicht werden. Des Weiteren hat die EU-Kommission einen Leitfaden veröffentlicht, der die Datenschutzrechte betroffener Bürgerinnen und Bürger in der Europäischen Union erläutert (http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf).

Schon vor der Verabschiedung übten unter anderem auch verschiedene Bürgerrechtsorganisationen Kritik an dem geplanten Abkommen. Sie kritisierten zum Beispiel die fehlende Unabhängigkeit der Ombudsfrau, da diese Funktion von einer Beamtin des Außenministeriums der Vereinigten Staaten wahrgenommen wird. Auch den Verweis darauf, dass die anlasslosen und massenhaften Überwachungsmaßnahmen der US-Regierung einen Verstoß gegen EU-Recht darstellen, da sie auch weiterhin keiner Verhältnismäßigkeitsprüfung unterliegen, halten wir weiterhin für berechtigt. Große Teile dieser Kritik konnten bis heute nicht entkräftet werden.

Die "Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten" (Artikel-29-Gruppe), die ein Zusammenschluss der datenschutzrechtlichen Aufsichtsbehörden der Mitgliedstaaten ist, veröffentlichte bereits im April 2016 eine Stellungnahme, in der sie dem damaligen Entwurf des EU-US Privacy Shield zwar im Vergleich zur Safe-Harbor-Entscheidung einige Verbesserungen attestierte. Gleichzeitig

[3] http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

formulierte die Artikel-29-Gruppe in anderen Punkten noch erhebliche Bedenken. Der Bitte, auf die Bedenken zu reagieren und entsprechende Änderungen sicherzustellen, kam die EU-Kommission nicht nach. Der Beschluss der EU-Kommission zum EU-US Privacy Shield kann nur vom Europäischen Gerichtshof für ungültig erklärt werden, was zur Folge hat, dass Daten aus Europa an entsprechend zertifizierte Unternehmen in den USA zunächst übermittelt werden dürfen. Der Gerichtshof hat allerdings festgestellt, dass die datenschutzrechtlichen Aufsichtsbehörden die Möglichkeit erhalten müssen, sich bei Zweifeln an Datenübermittlungsmechanismen an den Europäischen Gerichtshof zu wenden. Auch deshalb kann nicht ausgeschlossen werden, dass dem EU-US Privacy Shield in der derzeitigen Fassung das gleiche Schicksal droht wie der Safe-Harbor-Entscheidung. Eine Bürgerrechtsorganisation hat bereits Nichtigkeitsklage beim Europäischen Gerichtshof eingereicht (Aktenzeichen T-670/16).

16.3 Auswirkungen des Safe-Harbor-Urteils des Europäischen Gerichtshofs auf andere Rechtsgrundlagen

Im Urteil des Europäischen Gerichtshofs (EuGH) vom 6. Oktober 2015, welches das Safe-Harbor-Abkommen für ungültig erklärte, finden sich interessante Ausführungen allgemeiner Natur, welche sich auch auf die verbleibenden Rechtsgrundlagen für den Datentransfer in die Vereinigten Staaten von Amerika (USA) auswirken können. Bei diesen Rechtsgrundlagen handelt es sich um die EU-Standardvertragsklauseln, verbindliche Unternehmensregelungen (Binding Corporate Rules, BCR), die Einwilligung der Betroffenen und Auftragsdatenverarbeitungsverträge nach dem Bundesdatenschutzgesetz und den EU-US Privacy Shield (EU-US Datenschutzschild).

In seinem Urteil begründete das Gericht die Ungültigkeit der Safe-Harbor-Entscheidung der EU-Kommission unter anderem damit, dass sowohl der Wesensgehalt des durch Artikel 7 der Grundrechtecharta garantierten Grundrechts auf Achtung des Privatlebens als auch der Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz nach Artikel 47 der Grundrechtecharta verletzt seien. Das Gericht bestätigte damit die von den deutschen Datenschutzaufsichtsbehörden schon länger vertretene Auffassung zur Safe-Harbor-Entscheidung. Die aus den Enthüllungen Edward Snowdens gewonnenen Erkenntnisse über die anlasslose und massenhafte Speicherung sämtlicher Daten durch die Geheimdienste trugen ihren Teil dazu bei.

Da vorerst nicht damit zu rechnen ist, dass die USA ihre Regelungen zum Datenschutz in der Form ändern, dass sie dem EuGH-Urteil entsprechendem Datenschutzniveau genügen, lassen die Ausführungen des Gerichts auch an den oben aufgeführten Rechtsgrundlagen Zweifel aufkommen. Eine Regelung, die es Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, verletzt nach Auffassung des Europäischen

Gerichtshofs das Grundrecht auf Achtung des Privatlebens. Die Erfahrungen der letzten Jahre haben gezeigt, dass ein Großteil der anlasslosen und massenhaften Überwachung stattfindet, ohne dass betroffene Unternehmen oder Bürgerinnen und Bürger darüber informiert werden. In anderen Fällen werden die US-amerikanischen Unternehmen informiert, müssen kooperieren und werden per Gesetz zum Stillschweigen verpflichtet. Problematisch ist, dass sich die Unternehmen nicht gleichzeitig an europäisches und an US-amerikanisches Recht halten können. Dieses Dilemma kann keine der oben aufgeführten Rechtsgrundlagen umschiffen. Daraus ergibt sich auch das Fehlen einer Möglichkeit für die Betroffene beziehungsweise den Betroffenen, mittels eines Rechtsbehelfs Zugang zu ihren beziehungsweise seinen personenbezogenen Daten zu erlangen oder die Berichtigung oder Löschung zu erwirken. Auch dies verletzt nach Auffassung des Europäischen Gerichtshofs das Grundrecht auf wirksamen gerichtlichen Rechtsschutz. Um den Ansprüchen des Gerichts gerecht werden zu können, ist es unabdingbar, dass technische Maßnahmen ergriffen werden, welche den Inhalt elektronischer Kommunikation so schützen, dass die Schutzziele Vertraulichkeit und Integrität gewahrt bleiben. Die sicherste Lösung, personenbezogene Daten ausschließlich in der Europäischen Union zu verarbeiten, wird insbesondere von Unternehmen, deren Mutterkonzerne sich in den USA befinden, nicht umzusetzen sein.

16.4 Richtlinie über die Verwendung von Fluggastdaten

Die Richtlinie (EU) 681/2016 verpflichtet die Mitgliedstaaten der Europäischen Union (EU) und damit auch Deutschland, bis zum 25. Mai 2018 eine zentrale Stelle einzurichten, der alle Fluggesellschaften, deren Flüge entweder in einem Mitgliedstaat starten und in einem Drittland landen oder umgekehrt, Daten über die Passagiere vor dem Abflug zu übermitteln. Hierzu gehören neben Namen der Reisenden und Flugdaten sämtliche von der Fluggesellschaft verarbeitete Daten, wie zum Beispiel Zahlungsinformationen, Angaben zum Gepäck, zum Reisebüro und zu Mitreisenden. Diese Daten müssen ab ihrer Übermittlung für fünf Jahre in einer Datenbank vorgehalten werden. Erst nach Ablauf von sechs Monaten ist der Teil der Daten, der eine unmittelbare Identifizierung des Fluggastes ermöglicht, unkenntlich zu machen. Im Einzelfall können diese Daten aber mit Zustimmung einer hierfür zuständigen Behörde wieder hergestellt werden. Die hierdurch gewonnenen Daten dürfen zur Überprüfung, ob die Fluggäste möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sein könnten, verwendet werden. Außerdem dürfen die Daten zur Rasterfahndung ausgewertet werden, indem sie dazu genutzt werden, allgemeine Kriterien zu aktualisieren oder aufzustellen, nach denen Personen ermittelt werden, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sein könnten. Bei Bedarf und auf Anforderung können die so ermittelten Daten nicht nur durch die zuständigen Behörden der Mitgliedstaaten und das Europäische Polizeiamt Europol

verwendet werden, sondern auch durch die Zentralstellen und zuständigen Behörden der anderen Mitgliedstaaten.

Neben Drittlandsflügen können die nationalen Gesetzgeber auch Flüge zwischen Mitgliedstaaten und Reisen mit anderen Transportmitteln wie Bussen oder Zügen der Datenspeicherung und Datenübermittlung unterwerfen. Der Rat der Europäischen Union hat bereits am 18. April 2016 erklärt, dass aufgrund der derzeitigen Sicherheitslage in Europa die Mitgliedstaaten von dieser Möglichkeit in vollem Umfang Gebrauch machen wollen. Zudem verpflichteten sich die Mitgliedstaaten hierdurch nach ihrem jeweiligen nationalen Recht die Erhebung von PNR-Daten auf Unternehmen auszuweiten, die Dienstleistungen im Zusammenhang mit Reisen erbringen. Hiermit wären auch Flüge von und nach Bremen und damit die den Flughafen Bremen anfliegenden Fluggesellschaften, Bremer Reisebüros und Reiseveranstalter sowie viele Menschen im Land Bremen in besonderem Maße von den Vorgaben der Richtlinie betroffen.

Aufgrund der langen Speicherfristen, der intensiven Auswertung, des vorgesehenen Abgleichs mit anderen Datenbanken und der Übermittlung der Daten an andere Stellen, sowie der Erhebung umfangreicher Datenmengen pro Person ohne Anlass oder Verdacht führt die Umsetzung der Richtlinie zwingend zu einem starken Eingriff in die informationelle Selbstbestimmung aller Reisenden. Im Gegenzug steht bis heute jeglicher konkreter Beweis dafür aus, dass eine solche anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet, erforderlich und angemessen ist, Terrorismus oder schwere Kriminalität zu verhindern oder zu verfolgen. So hat zum Beispiel die Überprüfung des Fluggastdatenabkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika (USA) im Jahr 2013 gezeigt, dass von 110 Millionen Flugreisenden in die USA im Jahr 2012 nur 4.200 und damit 0,0038 Prozent (zunächst) die Einreise unter Verwendung von Fluggastdaten (PNR) verweigert wurde. Die Einreiseverweigerung wurde in diesen Fällen allerdings vornehmlich auf Visaverstöße und ungültige Reisedokumente, also nicht auf schwere Kriminalität oder Terrorismus gestützt. Insofern handelte es sich bei den Ergebnissen des Abgleichs um sogenannten Beifang, zu dessen Verfolgung die Fluggastdatensätze auch verwendet werden dürfen. Die Ahndung von Visaverstößen und des Mitführens ungültiger Reisedokumente kann aber im Hinblick auf die Entscheidungen des Bundesverfassungsgerichts und des Europäischen Gerichtshofs zur Vorratsdatenspeicherung einen solch massiven Eingriff in die im Grundgesetz, in der Europäischen Menschenrechtskonvention und in der Grundrechtecharta der Europäischen Union gewährleisteten Freiheitsrechte und des Rechts auf Schutz der Privatsphäre nicht rechtfertigen.

Die Auswertung der Flugpassagierdaten auch nach Abschluss der Reise für Zwecke der Rasterfahndung genügt den Anforderungen, die das Bundesverfassungsgericht in seinem

Urteil vom 4. April 2006 aufgestellt hat, nicht, da das Gericht auf eine konkrete Gefahr für hochrangige Rechtsgüter abstellt und eine allgemeine Bedrohungslage nicht genügen lässt. Zudem ist fraglich, inwieweit die Auswertung der Reisedaten überhaupt geeignet ist, Kriterien zu entwickeln, die eine sichere Prognose zulassen, dass ein bestimmter Flugpassagier terroristische oder andere schwere Straftaten begehen wird oder begangen hat.

Weiterhin fehlt es an einem schlüssigen Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit, welches die Grundrechte der Betroffenen hinreichend gewährleistet (siehe hierzu die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. und 17. März 2011 "Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!" unter der Ziffer 20.5 des 34. Jahresberichts).

Es ist daher sehr wahrscheinlich, dass das Bundesverfassungsgericht und der Europäische Gerichtshof auch die EU-Richtlinie zur Vorratsdatenspeicherung von und Rasterfahndung mittels Fluggastdaten beziehungsweise ihre Umsetzungsregelungen für verfassungswidrig und EU-rechtswidrig erklären. Diese Einschätzung stützt sich auch auf die Schlussanträge des Generalanwalts des Europäischen Gerichtshofs vom 8. September 2016 zu einem Gutachtenauftrag des Europäischen Parlaments, in welchen er vergleichbare Regelungen des Fluggastdatenabkommens zwischen der EU und Kanada für nicht konform mit EU-Recht erklärte. Dass auch der Europäische Gerichtshof selbst die Verwendung von Fluggastdaten in der vorgesehenen Weise für problematisch hält, offenbarte sich in den kritischen Fragen und Anmerkungen des berichterstattenden Richters im Anhörungstermin am 5. April 2016. Diese bezogen sich auch auf Punkte, die für die Richtlinie zur Verwendung von PNR relevant sind, wie die lange Speicherfrist der Daten, die fehlenden Limitierungen des Abgleichs mit anderen Datenbanken und die Eignung der Verwendung der Fluggastdaten zum Zweck der Terrorismusbekämpfung und Bekämpfung schwerer Straftaten. Im Hinblick auf das in Kürze zu erwartende Gutachten des Europäischen Gerichtshofs zu dem Fluggastdatenabkommen zwischen der Europäischen Union und Kanada und das sich hierfür abzeichnende Ergebnis wurden bereits vorsorglich die Verhandlungen zu einem Fluggastdatenabkommen zwischen der Europäischen Union und Mexiko ausgesetzt. Von einer schnellen Umsetzung sollte daher auch im Hinblick auf die mit der Umsetzung verbundenen hohen Kosten von EU-weit geschätzt mindestens 500 Millionen Euro abgesehen werden.

17. Ordnungswidrigkeiten/Zwangsmittelverfahren

17.1 Meldungen von Datenpannen

Stellt eine nicht öffentliche Stelle fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten,

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,

3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder

4. personenbezogene Daten zu Bankkonten oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach § 42 a Bundesdatenschutzgesetz unverzüglich der Aufsichtsbehörde sowie der oder dem Betroffenen mitzuteilen. Die Benachrichtigung der Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten.

Im Berichtsjahr waren wir mit drei Meldungen nach § 42 a Bundesdatenschutzgesetz befasst. In einem der Fälle informierte uns ein Bremer Kreditinstitut über die unzulässige Erhebung von Daten seiner Kundinnen und Kunden aus Ausdrucken von Kreditanträgen für Anschaffungsdarlehen in über 20 Fällen. Die Daten wurden missbraucht, um bei anderen Instituten Kreditkarten zu beantragen und Bargeld abzuheben. Dadurch wurden die Kundinnen und Kunden bei dem sich bei uns meldenden Kreditinstitut belastet. Die erhobenen Daten umfassten die Identifikationsdaten Name, Anschrift, Geburtsdatum und Geburtsort, relativ genaue Angaben zum monatlichen Gehalt, bis hin zu den aktuell gültigen Ausweisdokumenten. Alle Fälle wurden von dem Kreditinstitut angezeigt und von der Polizei als zusammenhängender Fall bearbeitet.

In einem weiteren Fall teilte uns ein Unternehmen aus dem Bereich der Kinobranche mit, dass dort ein ehemaliger Mitarbeiter in mehreren Fällen unzulässigerweise Daten des Unternehmens gestohlen habe. Bei den Daten habe es sich vermutlich um Beschäftigtendaten und Daten von Kundinnen und Kunden sowie Daten aus der Videoaufzeichnung gehandelt. Das Unternehmen hatte bereits vor seiner Meldung den ehemaligen Mitarbeiter aufgefordert, die betreffenden Daten zurückzugeben, seine Beschäftigten informiert, dass ihre Daten eventuell betroffen sein könnten und die Mitarbeiterinnen und Mitarbeiter zum korrekten Datenumgang belehrt, insbesondere im Hinblick auf die Wahrung des Datengeheimnisses.

In einem dritten Fall informierte uns ein Verein, der sich die Betreuung und Unterstützung behinderter Menschen zur Aufgabe gemacht hat, dass auf einem Dienstcomputer von einem Mitarbeiter des Vereins unzulässigerweise gefertigte Videoaufzeichnungen von

Bewohnerinnen und Bewohnern einer Pflegeeinrichtung gespeichert wurden. Bereits vor der Meldung hatte der Verein die Filmaufnahmen auf dem Dienstcomputer gelöscht und die Daten für die Strafverfolgung gesichert. Die Betroffenen beziehungsweise deren gesetzliche Vertreterinnen und Vertreter oder Betreuerinnen und Betreuer waren über die Aufzeichnungen umgehend und detailliert in Kenntnis gesetzt sowie darüber informiert worden, dass sie gegen den betreffenden Mitarbeiter der Einrichtung Strafanzeige erstatten können. Der Mitarbeiter war vom Verein außerordentlich gekündigt und aufgefordert worden, Datenkopien restlos und sicher zu löschen.

Im Jahr 2015 hatten wir von einem Einzelhandelsunternehmen, die Meldung erhalten, dass in einer Filiale des Unternehmens in Bremerhaven Lastschriftbelege entwendet worden waren. In einem anderen Fall unterrichtete uns ein Unternehmen der Hafenwirtschaft darüber, dass dort unter anderem ein Notebook gestohlen worden sei, auf dem auch personenbezogene Daten für die Abrechnung der Lohnsteuer von Mitarbeiterinnen und Mitarbeitern gespeichert waren. Schließlich bekamen wir die Meldung eines Vereins, der sich die Betreuung von Säuglingen zur Aufgabe gemacht hat, dass in einer Straßenbahn in Bremen Unterlagen mit besonders sensiblen personenbezogenen Daten liegen geblieben seien. In allen Fällen wurden von den betreffenden Stellen, teilweise schon vor der Meldung an uns, angemessene Abhifemaßnahmen getroffen.

Informiert wurden wir im Berichtsjahr auch über eine Datenpanne, die nicht zu einer Abhilfemaßnahme nach § 42 a Bundesdatenschutzgesetz verpflichtete. Der Herausgeber einer Fachzeitschrift für Motorradfahrer informierte uns, dass bei einer Werbeaktion, bei der per E-Mail Produktinformationen an die Abonnenten der Zeitschrift versandt wurden, bei der Empfängerangabe versehentlich das BCC-Feld mit dem CC-Feld verwechselt wurde. Dies führte dazu, dass in hoher Anzahl die Abonnentendaten an andere Personen weitergegeben wurden. Neben der E-Mail-Adresse wurde somit unter den Abonnenten auch bekannt, wer außerdem Abonnent der Zeitschrift ist. Nach der Versendung der E-Mail beklagten sich zahlreiche Abonnenten bei dem betreffenden Unternehmen über die unzulässige Datenweitergabe. Wir stellten fest, dass in diesem Fall eine Pflicht zur Meldung nach § 42 a Bundesdatenschutzgesetz nicht bestand, da die pflichtbegründenden Tatbestandsmerkmale nicht vorlagen. Zugleich forderten wir den Herausgeber der Zeitschrift auf, sich bei den Empfängerinnen und Empfängern um eine Löschung der fraglichen E-Mail-Adressdaten zu bemühen, sich bei ihnen für den Fehler zu entschuldigen und künftig bei der Versendung von E-Mails sorgfältiger zu sein. Der Nachrichtenversender versprach, unserer Aufforderung nachzukommen.

17.2 Ordnungswidrigkeitsverfahren nach dem Bundesdatenschutzgesetz

Auch im Berichtsjahr 2016 wurden von uns wieder mehrere Ordnungswidrigkeitsverfahren betrieben, die der Ahndung von Verstößen gegen das Bundesdatenschutzgesetz dienten.

In einem der Fälle hatte ein Mitarbeiter eines Handelsunternehmens an weit über 100 Empfängerinnen und Empfänger eine E-Mail mit dem Betreff "Offene Rechnung" versandt. Die E-Mail-Adressen eines Großteils der Empfängerinnen und Empfänger waren personalisiert und ließen Namen und gegebenenfalls Vornamen, darüber hinaus zum Teil Unternehmens- oder Vereinszugehörigkeiten für jede Empfängerin beziehungsweise jeden Empfänger der E-Mail erkennen. Mit der E-Mail wurden deren zugleich auch unzulässigerweise über die Kundeneigenschaft und das Bestehen einer Forderungsschuld der anderen Empfängerinnen und Empfänger informiert. Eine Einwilligung der Inhaberinnen und Inhaber einer E-Mail-Adresse in die vielfache Weitergabe der sie betreffenden Informationen an andere lag ebenfalls nicht vor (siehe hierzu Ziffer 15.1 dieses Berichts). Es wurden somit unbefugt personenbezogene Daten übermittelt, was von uns mit einer Geldbuße geahndet wurde. Der betreffende Mitarbeiter bezahlte das Bußgeld kurz nachdem unser Bußgeldbescheid ergangen war.

In einem weiteren Fall erteilte uns die Geschäftsführerin eines Energieberatungsunternehmens trotz mehrmaliger Aufforderung nicht die von uns für die Wahrnehmung unserer aufsichtsbehördlichen Tätigkeit benötigten Auskünfte zum unternehmensinternen Umgang mit den dort gespeicherten Daten sowie der Umsetzung gesetzlich vorgeschriebener Anforderungen im Hinblick auf die Führung eines Verfahrensverzeichnisses im Unternehmen und die Bestellung einer beziehungsweise eines betrieblichen Datenschutzbeauftragten. Wir eröffneten deshalb ein Bußgeldverfahren, das ebenfalls zur Verhängung einer Geldbuße führte. Obgleich unser Bußgeldbescheid noch im Frühjahr des Berichtsjahres rechtskräftig wurde, bezahlte die Geschäftsführerin des Energieberatungsunternehmens das Bußgeld nicht. Daher leiteten wir ein Vollstreckungsverfahren ein.

Auch in einem dritten Fall wurden uns die für unsere Tätigkeit erforderlichen Auskünfte nicht erteilt. Trotz mehrmaliger Aufforderung, uns richtige und vollständige Auskünfte im Hinblick auf Videoüberwachungsmaßnahmen in den Firmenräumlichkeiten des Unternehmens zu erteilen, teilte uns die Geschäftsführerin eines Pflegeunternehmens nicht korrekt mit, wieviel Videoüberwachungskameras eingesetzt werden und an welchen Orten die Kameras installiert wurden. Wir leiteten daher ein Bußgeldverfahren ein und erließen einen Bußgeldbescheid. Die Geschäftsführerin des Pflegeunternehmens legte gegen unseren Bußgeldbescheid Einspruch ein. Da wir diesem nicht abhelfen konnten, gaben wir den Vorgang zur weiteren Bearbeitung an die zuständige Staatsanwaltschaft ab.

Zum Ende des Berichtsjahres leiteten wir noch Ordnungwidrigkeitsverfahren gegen den Geschäftsführer eines Wohnungsverwaltungsunternehmens wegen unzulässiger Übermittlung personenbezogener Daten, gegen den Geschäftsführer eines Unternehmens der Automobilbranche wegen der unterlassenen Bestellung einer oder eines betrieblichen Datenschutzbeauftragten und gegen den Geschäftsführer eines Handelsunternehmens wegen unzulässiger Videoaufzeichnungen und der Nichtbestellung einer oder eines betrieblichen Datenschutzbeauftragten ein. Über den Fortgang dieser Verfahren werden wir im nächsten Jahr berichten.

17.3 Zwangsmittelverfahren

In mehreren Fällen wurden im Berichtsjahr Zwangsmittelverfahren betrieben. Diese Verfahren betrafen wie in den Vorjahren insbesondere die Nichterteilung von Auskünften durch unserer Aufsicht unterliegende Stellen oder Personen. In einem der Fälle war der Geschäftsführer einer Diskothek nicht bereit, uns für unsere aufsichtsbehördliche Tätigkeit Auskünfte zu der in den Gasträumen seiner Einrichtung betriebenen Videoüberwachung zu erteilen. Wir setzten wiederholt Zwangsgelder fest, deren Gesamthöhe sich mittlerweile auf 10.900 Euro beläuft. Da er die erforderlichen Auskünfte nicht erteilte und auch die Zwangsgelder nicht bezahlte, leiteten wir gegen den Geschäftsführer Vollstreckungsverfahren zum Einzug der offenstehenden Beträge ein. In einem anderen Fall, der sich auf die Nichterteilung von Auskünften hinsichtlich der unterlassenen Bestellung einer oder eines betrieblichen Datenschutzbeauftragten eines Unternehmens der Automobilbranche bezieht, mussten wir vor der Erteilung der benötigten Auskünfte ebenfalls ein Zwangsgeld festsetzen, dessen Höhe sich auf 800 Euro belief. Das Zwangsgeld wurde von dem Geschäftsführer des Unternehmens bezahlt. In mehreren anderen Fällen führte erst die Androhung der Verhängung eines Zwangsgelds zur Erteilung der erforderlichen Auskünfte.

18. Die Entschließungen der Datenschutzkonferenzen im Jahr 2016

18.1 Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016)

Nach vier Jahren intensiver Diskussion ist der Text der Europäischen Datenschutz-Grundverordnung nun zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmt. Mit der Grundverordnung verfügt die Europäische Union (EU) über ein weiterentwickeltes, einheitliches

Datenschutzrecht, das für Unternehmen und Behörden in Deutschland weitgehend Kontinuität gewährleistet. Überall in Europa soll künftig dasselbe Schutzniveau für das Grundrecht auf Datenschutz gelten. Ebenso wird feststehen, dass sich auch außereuropäische Anbieter, die ihre Waren und Dienstleistungen auf dem europäischen Markt anbieten, an das europäische Datenschutzrecht halten müssen.

Wichtige datenschutzrechtliche Prinzipien wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit sind in den Verhandlungen weitgehend erhalten geblieben.

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Absatz 11, 32 Bundesdatenschutzgesetz (BDSG) (Artikel 88 in Verbindung mit Erwägungsgrund [EG] 155),

- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Artikel 9 Absatz 4 in Verbindung mit EG 53, letzte beide Sätze),

- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Artikel 58 und 83 Absatz 7 in Verbindung mit EG 150, vorletzter Satz),

- jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Artikel 6 Absatz 2, 25, 32),

- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Artikel 6 Absatz 4),

- Beibehaltung der Verpflichtung in § 4 f Absatz 1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen (Artikel 37 Absatz 4).

18.2 Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016)

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sogenannte Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sogenannte Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, sodass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können.

Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei

Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen beziehungsweise pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).

- Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.

- Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungsverhältnissen und Versicherungsverhältnissen.

- Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.

- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden

sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

18.3 Datenschutz bei Servicekonten

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016)

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung sogenannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So ist dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.

Hiervon abgesehen müssen jedenfalls die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

- Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.

- Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.

- Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen.

- Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.

- Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von "Digital by Default" eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.

- Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die Länder übergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle beziehungsweise zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.

- Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken beziehungsweise zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.

- Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betroffenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob sie die eID-Funktion freischalten

und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

18.4 Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. und 7. April 2016)

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.

Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.

Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.

Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell[4], dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran messen lassen müssen, ob sie für

[4] Entschließung der 62. Datenschutzkonferenz am 25. und 26. Oktober 2001 in Münster
Entschließung der 72. Datenschutzkonferenz am 26. und 27. Oktober 2006 in Naumburg
Entschließung der 82. Datenschutzkonferenz am 28. und 29. September 2011 in München
Entschließung der 89. Datenschutzkonferenz am 18. und 19. März 2015 in Wiesbaden

dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

18.5 Klagerecht für Datenschutzbehörden – EU-Kommissionentscheidungen müssen gerichtlich überprüfbar sein

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 20. April 2016)

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher gegebenenfalls gegen den rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der Europäischen Union (EU) übermittelten personenbezogenen Daten enthalten. Im Rahmen eines sogenannten EU-US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den Vereinigten Staaten von Amerika (USA) sein und damit als Nachfolgeregelung für die Safe-Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den "EU-US Privacy Shield" bestehen jedoch nach Auffassung der Artikel-29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel-29-Datenschutzgruppe hat zum "EU-US Privacy Shield" zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkonferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der "EU-US Privacy Shield" in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche "angemessene Datenschutzniveau" in den USA zu gewährleisten.

Der Europäische Gerichtshof (EuGH) stellt in seiner oben genannten Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermöglichen, sodass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können.

Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (Bundesrats-Drucksache 171/16), in der nochmals deutlich gemacht wird, "dass das vom Europäischen Gerichtshof (EuGH) in seinem Urteil vom 6. Oktober 2015 (Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbehörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist".

18.6 EU-Datenschutzgrundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25. Mai 2016)[5]

Am 14. April 2016 hat das Europäische Parlament dem neuen Rechtsrahmen für den Datenschutz in Europa zugestimmt. Wesentlicher Teil des Rechtsrahmens ist die EU-Datenschutzgrundverordnung, deren Text am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde. Die Verordnung ist am 25. Mai 2016 in Kraft getreten und zwei Jahre später verbindlich in allen Mitgliedstaaten der Europäischen Union anzuwenden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist darauf hin, dass mit der EU-Datenschutzgrundverordnung eine Reihe neuer beziehungsweise erweiterter Aufgaben auf sie zukommen. Hierzu gehören insbesondere:

- Bearbeitung von Beschwerden und Beratung Betroffener sowie datenschutzrechtliche Beratung und Kontrolle von Unternehmen nunmehr unter Beachtung des erweiterten räumlichen Anwendungsbereichs der Verordnung (Marktortprinzip),

- verpflichtende Beratung von Behörden und Unternehmen bei der Datenschutz-Folgenabschätzung, insbesondere im Rahmen der vorherigen Konsultation der Aufsichtsbehörde, sowie Beratung bei der Umsetzung neuer Anforderungen wie

[5] Enthaltung Bayern (Bayerischer Landesbeauftragter für den Datenschutz und Bayerisches Landesamt für Datenschutzaufsicht)

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy By Design, Privacy By Default),

- Aufbau und Anwendung eines Kooperationsverfahrens zwischen Datenschutzbehörden in Europa bei grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop), Verpflichtung zur gegenseitigen Amtshilfe und umfassender Austausch von Informationen zwischen federführenden und betroffenen Aufsichtsbehörden jeweils mit kurzen Bearbeitungsfristen,

- Etablierung eines Kohärenzverfahrens zwischen den Datenschutzbehörden in Europa zur Gewährleistung der europaweit einheitlichen Anwendung der Verordnung, Mitwirkung im Europäischen Datenschutzausschuss,

- europaweit einheitliche Auslegung der Grundverordnung in Bezug auf fehlende Regelungen (zum Beispiel zur Videoüberwachung oder zum Scoring) und neue Anforderungen (zum Beispiel Recht auf transparente Information oder Recht auf Datenübertragbarkeit),

- Erarbeitung von Stellungnahmen und Billigung von branchenspezifischen Verhaltensregeln zur ordnungsgemäßen Anwendung der Verordnung, Erarbeitung von Zertifizierungskriterien, gegebenenfalls Durchführung von Zertifizierungen, Erarbeitung von Kriterien für die Akkreditierung von Zertifizierungsstellen, gegebenenfalls Durchführung der Akkreditierung,

- Bearbeitung von gerichtlichen Rechtsbehelfen Betroffener gegen Entscheidungen von Aufsichtsbehörden,

- Ausübung neuer beziehungsweise erweiterter Befugnisse der Datenschutzbehörden zur Erteilung von Anordnungen gegenüber den Verantwortlichen nunmehr auch im öffentlichen Bereich sowie Berücksichtigung zusätzlicher Tatbestände für Ordnungswidrigkeiten und eines erweiterten Bußgeldrahmens.

Die Europäische Datenschutzgrundverordnung verpflichtet die Mitgliedstaaten, die Aufsichtsbehörden zur Gewährleistung ihrer Unabhängigkeit mit den erforderlichen personellen, finanziellen und technischen Ressourcen auszustatten (Artikel 52 Absatz 4 Datenschutzgrundverordnung). Aus Sicht der Datenschutzkonferenz ist es für die Bewältigung der neuen Aufgaben zwingend erforderlich, für die Datenschutzbehörden in Deutschland erweiterte personelle und finanzielle Ressourcen vorzusehen. Dies gilt bereits für die jetzt laufende Vorbereitungsphase, in der die Weichen für eine funktionierende Umsetzung der Datenschutzgrundverordnung gestellt werden. Die Konferenz appelliert deshalb an die Gesetzgeber in Bund und Ländern, rechtzeitig die haushaltsrechtlichen

Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen. Nur so lassen sich die zusätzlichen Aufgaben der Datenschutzgrundverordnung von den Datenschutzbehörden in Deutschland effektiv wahrnehmen.

18.7 Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf – Konsequenzen für polizeiliche Datenverarbeitung notwendig

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9. und 10. November 2016)

Die Datenschutzbeauftragten des Bundes und der Länder Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte "Falldatei Rauschgift" (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

- Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Absatz 2 BKAG (Negativprognose) vorliegen.

- Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.

- Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.

- Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Absatz 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:

1. Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.

2. Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.

3. In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der Falldatei Rauschgift die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.

18.8 "Videoüberwachungsverbesserungsgesetz" zurückziehen!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 9. und 10. April 2016)

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein "Videoüberwachungsverbesserungsgesetz" Änderungen des Bundesdatenschutzgesetzes (BDSG) einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[6] abgelehnt. Der Gesetzesentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe

[6] bei Enthaltung der Bundesbeauftragten für Datenschutz und Informationsfreiheit

auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzesentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6 b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Absatz 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.

Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes-

und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzesentwurf zurückzuziehen.

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

19.1 Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 13. und 14. September 2016)

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit ("Kopplungsverbot", Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),
- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

20. Die Europäische und die Internationale Datenschutzkonferenz

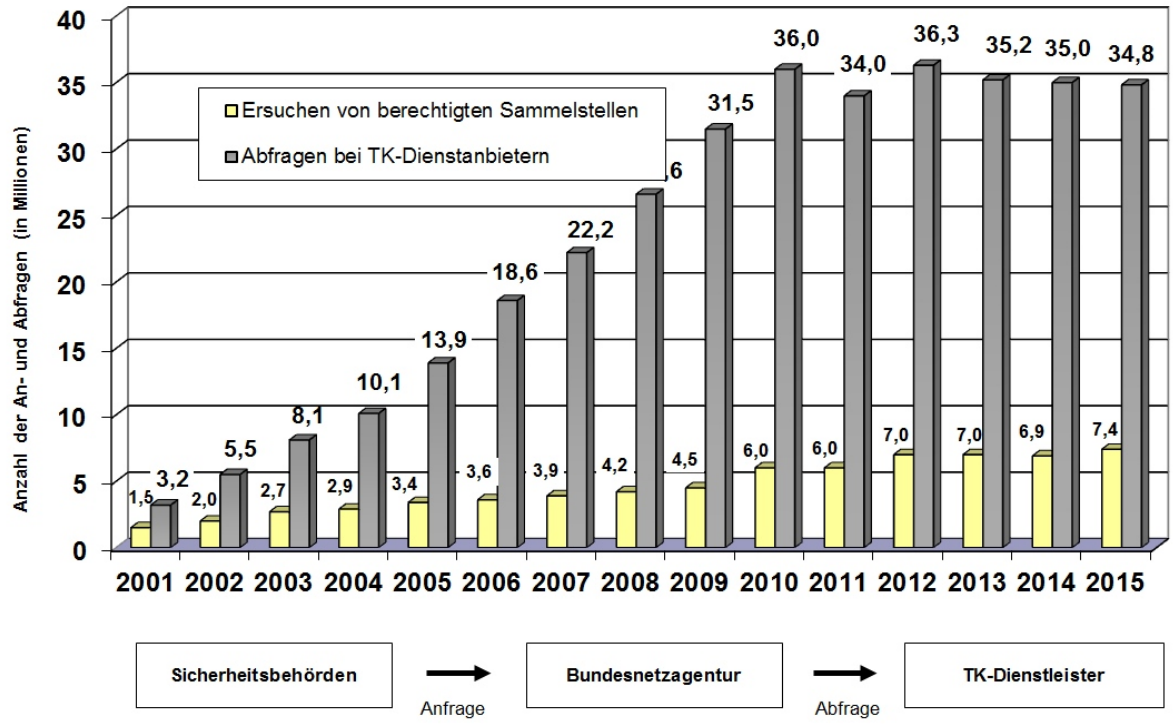
Die Entschließungen der Europäischen Datenschutzkonferenz im Jahr 2016 stehen auf der Seite der Bundesbeauftragten für Datenschutz und Informationsfreiheit unter http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/EuDSK/_functions/EuDSK_table.html zur Verfügung. Informationen zu den Entschließungen der 38. Internationalen Datenschutzkonferenz am 18. Oktober 2016 in Marrakesch sind auf der Seite der

International Conference of Data Protection and Privacy Commissioners (ICDPPC) in englischer Sprache unter https://icdppc.org/document-archive/adopted-resolutions/ zu finden.

21. Anhang

21.1 Automatisierte Auskunftsverfahren gemäß § 112 Telekommunikationsgesetz

Sicherheitsbehörden erhalten gemäß § 112 Telekommunikationsgesetz (TKG) über die Bundesnetzagentur von Telekommunikationsdiensteanbietern Auskünfte aus deren Kundendateien (Namen und Anschriften der Inhaber von Rufnummern). Derzeit erhalten etwa 150 berechtigte Stellen und mehrere tausend hieran angeschlossene Abfragestellen der Strafverfolgungsbehörden automatisiert entsprechende Bestandsdaten bei den Telekommunikationsdiensteanbietern.



Quelle: Jahresbericht 2015 der Bundesnetzagentur

21.2 Liste des verfügbaren Informationsmaterials

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

21.3 Index

A **Ziffer**

B

C

D

K

M

N

O

P

R

S