TÄTIGKEITSBERICHT DATENSCHUTZ 2018

Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Hamburg

27. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2018

Herausgegeben vom
Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Straße 22
20459 Hamburg

Tel. 428 54 40 40
Fax 428 54 40 00
mailbox@datenschutz.hamburg.de

Auflage: 800 Exemplare
Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH
Foto Titelseite: Thomas Krenz
Druck: Beisner Druck GmbH & Co. KG

Diesen Tätigkeitsbericht können Sie abrufen unter
www.datenschutz-hamburg.de

Vorgelegt im Februar 2019
Prof. Dr. Johannes Caspar
(Redaktionsschluss: 31. Dezember 2018)

INHALTSVERZEICHNIS

Vorwort

Das Jahr 2018 markiert mit der Geltung der europäischen Datenschutzgrundverordnung (DSGVO) einen Meilenstein des Datenschutzes. Gleichzeitig aber fällt in dieses Jahr auch das Bekanntwerden zahlreicher in Art und Ausmaß verstörender Datenmissbräuche und Datenschutzverletzungen. Neben einzelnen, in diesem Tätigkeitsbericht näher dargelegten Vorfällen hat insbesondere der Datenskandal rund um Facebook und Cambridge Analytica vor Augen geführt, dass die Herrschaft über Daten eben nicht nur einen Schlüssel zur Vermarktung von Produkten und Dienstleistungen darstellt, sondern auch zur Beeinflussung des Wählers bei demokratischen Entscheidungen eingesetzt werden kann. Immer stärker wird sichtbar: Der intransparente und missbräuchliche Umgang mit personenbezogenen Daten durch Werbenetzwerke und Plattformen stellt ein Wirtschaftsmodell dar, das zahlenden Interessenten den Zugang zu Herz und Hirn der Wählerschaft verschafft und hilft, die Meinungsbildung nicht zuletzt durch das Verbreiten von Fake News gezielt zu manipulieren. Am Ende ist dabei nicht nur die informationelle Selbstbestimmung des Einzelnen, sondern vielmehr auch die Integrität demokratischer Institutionen gefährdet.

Der Pakt mit Werbenetzwerken wie Facebook hat seinen Preis. Ein Urteil des EuGH aus dem Juni 2018 hat festgestellt, dass jeder Betreiber einer Fanpage eine gemeinsame datenschutzrechtliche Verantwortung mit Facebook für die personenbezogenen Daten trägt, die dem Netzwerk über ihre Seiten übermittelt werden. Dass auch das Wissen um diese datenschutzrechtliche Mithaftung bislang nicht wirklich zu einem Umdenken gerade auch bei öffentlichen Stellen im Umgang mit Facebook geführt hat, muss zu denken geben. Es gilt künftig noch klarer herauszuarbeiten, dass die Nutzung von Fanpages keineswegs eine ungefährliche, allgemein übliche Form der Kommunikation darstellt. Vielmehr ist die Vereinbarung zwischen Facebook und den Fanpagebetreibern gleichzeitig eine Abrede zu Lasten Dritter, zu Lasten all jener, die häufig ohne es überhaupt zu wissen, als Webseitenbesucher Daten bei dem Netzwerk abgeben und dort Spuren hinterlassen und damit zum Gegenstand von Profilbildung und Manipulation werden können.

Der Schlüssel zum einheitlichen Vollzug der DSGVO liegt nun bei den Aufsichtsbehörden. Sie müssen über ihre gemeinsame zentrale Stelle, dem Europäischen Datenschutzausschuss, über Auslegung und Anwendung des Datenschutzrechts in Europa wachen. Dazu ge-

hört es, sachliche Fragen über die Auslegung und Anwendung der DSGVO aufzugreifen und zügig zu entscheiden, gerade wenn die zwischen der in Europa federführenden Behörde und anderen Behörden in Streit stehenden Fragen sich auf viele Millionen Nutzer in der EU - wie im Fall der Weitergabe von Daten durch WhatsApp an Facebook, bei dem allein über 30 Millionen in Deutschland betroffen sind - auswirken.

Wenn der Eindruck entsteht, dass die neuen Regelungen dazu führen, dass man die Großen laufen lässt und die Kleinen hängt, dann steht die soziale Akzeptanz und damit auch die rechtliche Geltung der DSGVO insgesamt massiv in Frage. Denn es sind gerade die kleinen und mittleren Unternehmen, wie auch Vereine und Stiftungen, die die Regelungen umsetzen müssen und die nicht die wirtschaftliche Fähigkeit haben, 500 Jahre Arbeitszeit in die Umsetzung der DSGVO zu investieren, wie dies nach eigenen Angaben bei Google der Fall war.

Eine leider im politischen Kontext weit verbreitete Sichtweise, wonach mit Blick auf die lokale Wirtschaft nur die schwache Datenschutzaufsicht eine gute Datenschutzaufsicht sei, verkennt, dass gerade für den fairen Wettbewerb auf dem gemeinsamen Markt eine Vollzugsgerechtigkeit unabdingbar ist. Besonders privilegierte Bereiche, in denen digitale Großkonzerne nicht nur einer gerechten Besteuerung entgehen, sondern sich auch keinem oder einem kaum wirksamen Vollzug der Datenschutzbestimmungen gegenübersehen, darf es in der EU nicht geben. Nur eine angemessene Ausstattung der Behörden kann hier dazu beitragen, dass auf Ebene des Europäischen Datenschutzausschusses ungerechtfertigte Privilegierungen hinterfragt werden, aber auch dass die ortsansässigen Unternehmen bei Fragen zum Datenschutz beraten werden könnten.

Dies spricht dafür, Aufsichtsbehörden zu stärken und sie in die Lage zu versetzen, die neuen Anforderungen des europäischen Datenschutzes angemessen zu erfüllen - auch und gerade aus wirtschaftlicher Sicht.

Hier bleibt gerade auch in Hamburg noch Einiges zu tun.

Prof. Dr. Johannes Caspar

Februar 2019

EINLEITUNG I.

I. EINLEITUNG

Datenschutz im Zeichen der DSGVO

1. Die Kluft zwischen Sein und Sollen wird größer

Seit 2012 wurde sie als Projekt diskutiert, lobbyiert und um sie gestritten. Seit dem 25. Mai 2018 ist sie nun in Geltung erwachsen: Die Datenschutzgrundverordnung (DSGVO) hat die Welt des Datenschutzes tiefgreifend verändert und ist weiterhin tagtäglich dabei, sie zu formen.

Das Projekt eines einheitlichen Datenschutzes in der Europäischen Union ist mit dem 25.5.2018 jedoch keinesfalls beendet, sondern vielmehr erst auf eine zweite entscheidende Stufe getreten. Auf der ersten Ebene ging es noch um die regulatorischen Fragen des einheitlichen Datenschutzes innerhalb der Europäischen Union, um weiterhin bestehende nationale Eigenheiten innerhalb der Rechtsmaterie und natürlich ganz zentral um das neu zu justierende Verhältnis zwischen datengetriebener Wirtschaft und dem wirksamen Schutz des selbstbestimmt über seine Daten entscheidenden und diese kontrollierenden Individuums.

Nun verlagert sich die Verantwortung vom Gesetzgeber auf die Exekutive. Auf dieser zweiten Stufe geht es darum, den Vorschriften des europäischen Rechts in der Rechtspraxis zur Durchsetzung zu verhelfen. Im Fokus stehen die europäischen Datenschutzaufsichtsbehörden, die gemeinsam im Europäischen Datenschutzausschuss, dem neuen zentralen Organ des Datenschutzes, auf Ebene der EU für den Vollzug des Datenschutzrechts verantwortlich sind.

Die Verantwortung befindet sich nun in den Händen von Stellen, die für Interpretation, Anwendung und Kontrolle der Regelungen, und damit auch für den Einsatz des Sanktions-

instrumentariums zuständig sind. Die Herausforderung für die Aufsichtsbehörden, die DSGVO im europäischen Binnenmarkt zu einer Erfolgsgeschichte des Schutzes von Rechten und Freiheiten betroffener Menschen in der EU zu machen, könnte größer nicht sein: Der mit der Hoffnung vieler Menschen verbundene Charakter der DSGVO als Magna Charta der digitalen Welt steht nach langjährigen Diskussionen im Gesetzgebungsprozess nun auf dem Prüfstand. Die tatsächliche Entwicklung in den Tagen und Wochen kurz vor dem 25. Mai 2018 und in der Zeit danach hat die Aufgabe des Rechtsvollzugs durch unabhängige Stellen nicht unbedingt erleichtert. Hier ist einerseits vor und nach dem Wirksamwerden der DSGVO von einem hohen Umsetzungsdefizit auszugehen. So wurde noch mit Stand Ende September 2018 durch BITKOM nach einer repräsentativen Umfrage bei Unternehmen festgestellt, dass erst ein Viertel der Unternehmen in Deutschland die DSGVO vollständig umgesetzt habe (*https://www.bitkom.org/Presse/Presseinformation/Kaum-Fortschritt-bei-der-Umsetzung-der-Datenschutz-Grundverordnung.html*).
Die Schere zwischen Sein und Soll, zwischen normativem Geltungsanspruch des Rechts und der Rechtspraxis war bereits in den Zeiten des alten Bundesdatenschutzgesetzes (BDSG) enorm. Hierfür sind viele Gründe maßgeblich. U.a. liegt dies an der defizitären personellen Ausstattung der Behörden und der fehlenden gerichtlichen Entscheidungspraxis auf dem Gebiet des Datenschutzrechts. Durch die DSGVO kommen nun als weitere Faktoren die oft unterkomplexen und unbestimmten Rechtsregelungen hinzu. Sie erschweren die Anwendung auf den Einzelfall, die wirksame Rechtsdurchsetzung sowie den Einsatz der Sanktionsbefugnisse. Damit wird sich die Kluft zwischen Sein und Sollen noch vertiefen.

In der Tat sind die Vorschriften der DSGVO nur bedingt in der Lage, eine klare Umsetzungspraxis zu gestalten. Das gilt für den Bereich des Fehlens einer E-Privacy-Verordnung mit Blick auf die Frage des Online- und Offline-Trackings, aber auch

für viele neue und zunächst als positiv empfundene Regelungen zum verbesserten Schutz von Betroffenen. Sei es das Koppelungsverbot, das künftig die Möglichkeit einschränken soll, von den Betroffenen als Gegenleistung für die Nutzung von Diensten umfassende Einwilligungen zur Verarbeitung von Daten zu erhalten, seien es die Regelungen zur Portabilität von Daten oder die Grundsätze von Privacy by Default und Privacy by Design – grundsätzlich sind die Regelungen in ihrer Reichweite unklar und benötigen eine Präzisierung.

Gleichzeitig wird der Vollzug erschwert durch eine fragmentierte aufsichtsbehördliche Landschaft, die derzeit aus 28 mitgliedstaatlichen Aufsichtsbehörden innerhalb der EU und 17 Aufsichtsbehörden (Bund/Länderaufsicht) im nationalen Bereich besteht. Gerade im europäischen Kontext sind unterschiedliche Verständnisse des Rechtsvollzugs mit jahrzehntelangen Traditionen wirksam. Dies erschwerte bereits in der Vergangenheit die gemeinsame Verabschiedung von Leitlinien und Standpunkten, die eine umfassende Information für verantwortliche Stellen leider nicht immer in rechtzeitiger Weise vor Inkrafttreten der Datenschutzgrundverordnung ermöglicht hat.

Auf europäischer Ebene macht die Bearbeitung von Beschwerden betroffener Bürgerinnen und Bürger gerade gegenüber den global agierenden Internetunternehmen und Abstimmungen viel Arbeit. Erhebliche Aufwände resultieren aus den zahlreichen Abstimmungsverfahren (sog. Kooperations- und Kohärenzverfahren) zwischen den einzelnen Aufsichtsbehörden und im Europäischen Datenschutzausschuss. Innerhalb der europäischen aufsichtsbehördlichen Strukturen ergeben sich hier durchaus überbürokratische Verfahrensgestaltungen, die erhebliche Ressourcen der Behörden binden. Die bereits in den letzten Jahren anlässlich einzelner Fallgestaltungen immer wieder auftretenden kulturellen Differenzen bei der Anwendung des Datenschutzrechts

rückt den Europäischen Datenschutzausschuss als zentrale Clearinginstanz für dessen Auslegung in eine Schlüsselrolle für einen harmonisierten Rechtsvollzug. Hier gilt es künftig, mit den entsprechenden Leitentscheidungen die Klarheit und Rechtssicherheit für Betroffene, Datenverarbeiter und für die Aufsichtsbehörden zu stärken.

2. Die neue Dimension der Eingabezahlen – Die personelle Ausstattung gerade unter der DSGVO aktuell wie nie

Die Datenschutzgrundverordnung sieht für betroffene Bürgerinnen und Bürger eine Stärkung der materiellen Datenschutzrechte, aber auch eine deutliche Stärkung ihrer Beschwerde- und Klagebefugnisse vor. Neben einer Erweiterung der bisherigen Rechte der Betroffenen im Bereich der Information, der Auskunft, aber auch der eigenen Entscheidungs- und Kontrollbefugnisse über die eigenen Daten, insbesondere dem neuen Recht auf Datenportabilität, können Betroffene die Aufsichtsbehörden im Falle der Ablehnung von Beschwerden künftig verklagen. Klagebefugt sind auch Organisationen oder Vereinigungen, die nach dem Recht eines Mitgliedstaats hierzu gegründet wurden.

Die Möglichkeiten für die Betroffenen, sich bei Aufsichtsbehörden wegen einer Verletzung ihrer Rechte zu beschweren, hat eine in ihrem Ausmaß nicht zu erwartende Akzeptanz gefunden: So haben sich die Eingaben seit dem Inkrafttreten der DSGVO im Bereich des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) im Jahr 2018 gegenüber dem Zeitraum 2017 verdoppelt. Das zeigt, dass die DSGVO im Bewusstsein vieler Bürgerinnen und Bürgern angekommen ist und in einer begrüßenswerten Weise genutzt wird, um eigene Rechte gegenüber den verantwortlichen Stellen vor den Aufsichtsbehörden geltend zu machen.

Gleichzeitig erweist sich das neue Interesse am Datenschutz doch für eine bereits vor Geltung der DSGVO unter Überlast arbeitende Datenschutzaufsichtsbehörde wie die unsere auch als eine problematische Entwicklung. Es zeigt sich, dass die Belastung sowohl in quantitativer, als auch in qualitativer Hinsicht durch neue Aufgaben, die mit der DSGVO verbunden sind, wesentlich massiver ansteigt, als die personellen Verstärkungen mit Mitarbeiterinnen und Mitarbeitern im Bereich des HmbBFDI dies an sich zulassen.

Gab es im Jahr 2017 pro Kalendertag durchschnittlich 4,4 Eingaben, so sind es seit Geltung der DSGVO 9,3 Eingaben. Wollte man die Mehrarbeit personell kompensieren, müsste die Behörde um 10 VZÄ (entspricht ausfinanzierten Vollzeitstellen) verstärkt werden.

Außerdem sind qualitativ neue Aufgaben für die Aufsichtsbehörden hinzugekommen, die weiteres Personal erfordern. Hierzu zählen etwa die gesetzlich geregelte Zusammenarbeit im Rahmen des Europäischen Datenschutzausschusses sowie die vielfältigen Kooperationen zwischen den einzelnen nationalen und europäischen Aufsichtsbehörden bei grenzüberschreitenden Datenverarbeitungen einschließlich der umfangreichen innerdeutschen Abstimmungsprozesse. Mit dem europäischen Kohärenzverfahren ist eine neue europäische Vollzugsstruktur geschaffen worden, die erhebliche zusätzliche Mehrarbeit erfordert, auch durch vorgeschaltete nationale Regelungen des BDSG (neu) (§ 17ff. BDSG), die zusätzlich ein nationales Abstimmungsverfahren vorsehen.

Daneben fordert die DSGVO u.a. die Akkreditierung von Zertifizierungsstellen. Das ist ein Instrument, das künftig neue wirtschaftliche Betätigungsfelder eröffnet und den Datenschutz als Aufgabe der freiwilligen Selbstregulierung und Generierung von Wettbewerbs- und Standortvorteilen einsetzbar macht. Die Akkreditierung von zertifizierenden

Stellen in Zusammenarbeit mit der deutschen Akkreditierungsstelle (DAkkS) bindet bereits in der Vorbereitung erhebliche Ressourcen. Als eine weitere neue Aufgabe mit großer Bedeutung erweist sich die Aufklärung der Öffentlichkeit über die Risiken, Garantien und Rechte, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten und den Maßnahmen zur Datensicherheit bestehen, wobei ein Hauptaugenmerk dabei auf speziellen Maßnahmen für Kinder liegt. Die Beschwerde- und Klagemöglichkeiten, die insbesondere nicht nur Betroffenen, sondern künftig auch Verbänden zur Verfügung stehen, dürften dazu beitragen, dass die gegenwärtige Auslastung von Aufsichtsbehörden durch entsprechende Klagen Betroffener vor den Gerichten ansteigt.

Die wesentliche Bedeutungszunahme des Datenschutzes für die Rechtswahrnehmung von Betroffenen droht durch die Entwicklung hin zu einer immer stärkeren Überlastung der Aufsichtsbehörden in ihr Gegenteil umzuschlagen. Die neuen Vorschriften der Datenschutzgrundverordnung haben hier offenbar Hoffnungen geweckt, die die Praxis nicht halten kann. Derzeit sind gerade im Bereich der Eingaben- und Beschwerdebearbeitung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit die Bearbeitungszeiten so stark angestiegen, dass die Betroffene mitunter Monate auf eine Entscheidung der Behörde warten müssen. Maßnahmen, wie ein grundsätzlicher Beratungsstopp für Datenschutzanfragen von Unternehmen und die Verweisung von Beschwerden zu nachbarschaftlichen Streitigkeiten über den Betrieb von Videoüberwachungsanlagen auf den Zivilrechtsweg, sind in die Wege geleitet. Dies kann aber kaum ein tragfähiger Ansatz sein, mit dem sich die Erfüllung des gesetzlichen Auftrags durch die Behörde über die nächsten Jahre hinweg absichern lässt.

Für die Zeit nach Inkrafttreten der DSGVO hatte der HmbBfDI 18 neue Stellen gefordert. Ein von den Datenschutzbehörden

in Auftrag gegebenes Rechtsgutachten hatte einen durchschnittlichen Mehrbedarf sogar in Höhe von 24 – 33 Stellen ausgewiesen. Im Haushalt 2019/2020 sind leider unter dem Strich nur 5 neue Stellen bewilligt worden. Alle Stellenanteile werden dazu genutzt, um bereits vorhandene befristete Stellen in unbefristete umzuwandeln. Real ist daher für die beiden kommenden Jahre kein personeller Zuwachs zu verzeichnen. Eine gegenüber dem Haushaltsausschuss nochmals gesenkte Verstärkung um 5 neue Stellen wurde leider ebenfalls nicht berücksichtigt und wird ins neue Jahr mitgenommen.

Es ist daher alternativlos, im Verlauf des Frühjahrs 2019 eine erneute umfassende Evaluation der Arbeitssituation der Behörde einzuleiten. Mit dem Jahrestag der DSGVO sollte es dann möglich sein, nach Maßgabe der aktuellen Fallzahlentwicklung eine unterjährige Bewerbung von weiterem Personalmitteln einzuleiten. Zudem steht der HmbBfDI in Kontakt mit anderen Aufsichtsbehörden, deren Situation ähnlich angespannt ist. Hierbei gilt es, Handlungsoptionen zu besprechen, wie eine angemessene Personalausstattung künftig durchgesetzt werden kann.

3. DSGVO im (Zerr-)spiegel der Öffentlichkeit

Die enorm gestiegene Nachfrage nach datenschutzrechtlicher Beratung sowie die datenschutzrechtlichen Beschwerden stellen einen wesentlichen, im Grundsatz positiven Aspekt der gegenwärtigen Entwicklung dar. Ein anderer in der Öffentlichkeit zu beobachtender Trend ist eine Berichterstattung über die Anwendung der DSGVO, in deren Mittelpunkt die Aufsichtsbehörden leider kein durchgehend gutes Bild vermitteln: Berichte über Fehlentwicklungen im Zusammenhang mit der DSGVO haben in den letzten Monaten für den Eindruck gesorgt, die DSGVO stehe als Synonym für bürokratische, weltfremde und gleichzeitig als ungerecht empfundene Ergebnisse. Das ist für das Anliegen des Datenschutzes

schädlich und schwächt zudem die soziale Akzeptanz der Rechtvorschriften gerade bei den Stellen, die verantwortlich für deren Einhaltung sind.

Die Liste der Negativ-Legenden, die sich im Zuge dieser Berichterstattung ergaben, ist lang. Sie reicht über Schulzeugnisse, die künftig nicht mehr per EDV, sondern nur noch per Hand durch die Lehrer geschrieben werden dürften, über Gruppenfotos von Kindergartenkindern, bei denen andere Kinder wegretuschiert werden müssten, über Klingelschilder, auf denen künftig die Namen von Bewohnern nicht mehr ausgewiesen werden dürften, bis hin zu einer Abmahnwelle, die den Mittelstand überrollt. Befürchtungen über das Ende der Fotografie in der Öffentlichkeit und von Handwerkern, die ohne die Nutzung von WhatsApp künftig ihren zentralen Kommunikationskanal verlieren, runden das entworfene Zerrbild ab.

Derartige Beispiele zeigen eine tiefe Verunsicherung über die teilweise allgemeinen und in ihrer Auslegung offenen Bestimmungen der Datenschutzgrundverordnung. Auch wenn die Datenschutzaufsichtsbehörden in Fällen, in denen absurde Konsequenzen durch die Datenschutzgrundverordnung in der Öffentlichkeit kolportiert wurden, meist sehr schnell Entwarnung gaben, hat dies nicht immer zur Beruhigung der Öffentlichkeit und der betroffenen Kreise geführt. Das liegt sicherlich auch daran, dass es in vielen Beiträgen gar nicht so sehr um Aufklärung und Information ging, sondern darum, die Datenschutzgrundverordnung insgesamt in einem negativen Licht darzustellen und sie realsatirisch zu überhöhen.

4. Der größte Feind des Datenschutzes ist dessen Überbürokratisierung

Klar und unumstritten ist jedoch auch, dass die Kritik an der DSGVO zu einem Teil berechtigt ist. So folgen aus den im Wesentlichen gleichermaßen für alle Verarbeiter geltenden

Vorschriften der DSGVO erhebliche bürokratische Hürden gerade für Vereine und kleine Unternehmen. Im Kern zielt die Datenschutzgrundverordnung dann auch auf große, international agierende Verarbeiter ab. Den Aufsichtsbehörden wurden gegenüber diesen Unternehmen stärkere Sanktionsinstrumente in die Hand geben. Hierzu gehört insbesondere die Erhöhung des Bußgeldrahmens auf 20 Millionen Euro, d.h. das Siebenundsechzigfache der bisher maximalen Bußgeldhöhe bis hin zu 4% des jährlichen Umsatzes eines Unternehmens.

Dass derartige Sanktionsmöglichkeiten künftig eingesetzt werden könnten, wird gerade dort befürchtet, wo es schwer fällt, die Vorschriften umzusetzen. Mit Blick auf die linear, d.h. unabhängig von Wirtschaftskraft sowie der Zahl der zu verarbeitenden Daten in den jeweiligen Unternehmen geltenden Regelungen etwa zu Transparenz-, Informations- und Auskunftspflichten ist festzuhalten, dass vor allem kleinere Verarbeiter befürchten, ungerechtfertigt im Fokus der Aufsichtsbehörden zu stehen. Ein Nachsteuern im Zuge der künftigen Evaluation der DSGVO zu einer angemesseneren Pflichtenverteilung nach Maßgabe der jeweiligen Verarbeitungsrisiken dürfte denn auch künftig zu diskutieren sein. Der unterschiedlichen Ausgangslage bei der Umsetzung und den Risiken trägt der HmbBfDI derzeit als Aufsichtsbehörden insofern Rechnung, als eine anlassunabhängige Prüfung bei kleinen Unternehmen und Vereinen derzeit nicht geplant ist. Gleichzeitig ist aber auch zu berücksichtigen, dass bei entsprechenden Beschwerden von Betroffenen regelmäßig eine aufsichtsbehördliche Prüfung einzuleiten ist.

Auch ein weiterer Aspekt der Kritik muss in diesem Zusammenhang sehr ernst genommen werden: die in der Öffentlichkeit verbreitete Meinung, der Vollzug der Datenschutzgrundverordnung werde an unterschiedlichen Maßstäben gemessen. Während kleinere Unternehmen, wie etwa Handwerksbetriebe, fürchten müssten, unter der Datenschutz-

grundverordnung ins Visier genommen zu werden, bleibe der Vollzug bei internationalen Datenkonzernen bislang trotz erheblicher Datenskandale in den letzten Monaten weitgehend folgenlos. Tatsächlich haben international agierende Unternehmen durch die Aufstellung ihrer Hauptniederlassung in Europa die Möglichkeit, sich die für ihre Datenverarbeitung europaweit federführende Aufsichtsbehörde „auszusuchen". Das erscheint aus Sicht von Unternehmen auch rational, denn unterschiedliche Vollzugsstandards sind innerhalb der EU auch unter der Geltung der DSGVO nicht wegzudiskutieren.

Es wird daher künftig ganz entscheidend sein, im Vollzug innerhalb der EU einheitliche Standards zu etablieren. Zentrales Gremium hierfür ist der Europäische Datenschutzausschuss. Es ist in der Tat unbefriedigend, wenn vor Geltung der DSGVO ein Austausch der Daten der Nutzer von WhatsApp zu Facebook durch entsprechende Anordnungen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit unterbunden werden konnte, seit Wirksamwerden der DSGVO das Unternehmen WhatsApp, das wie der Mutterkonzern Facebook in Irland ansässig ist, jedoch ganz offen über einen umfangreichen Datenaustausch mit Facebook informiert und die Daten zu bestimmten Zwecken dorthin weitergibt.

Allein die Harmonisierung der Rechtsvorschriften reicht nicht aus, um eine einheitliche Anwendung der europäischen Normen abzusichern. Es liegt in der zentralen Verantwortung des Europäischen Datenschutzausschusses, in dem alle Aufsichtsbehörden der Mitgliedstaaten vertreten sind, über strittige Fragen zwischen federführenden und betroffenen Aufsichtsbehörden verbindlich zu entscheiden und die Anwendungsstandards des Rechts zu vereinheitlichen. Diese Aufgabe ist zum Schutz von Betroffenen und ihren Rechten und Freiheiten von herausragender Bedeutung.

Darüber hinaus ist ihre Erfüllung aber gleichsam zentrale Voraussetzung für einen fairen Wettbewerb auf dem digitalen Markt innerhalb der EU. Letztlich müssen datenverarbeitende Unternehmen unabhängig davon, ob diese mit ihrem Hauptsitz in Dublin, Hamburg oder andernorts in der EU ansässig sind, sich auch einer gleichen Verwaltungspraxis gegenüber sehen.

Befürchtungen hinsichtlich einer fehlenden Vollzugsgleichheit haben somit einen ernsten Hintergrund. Das Ziel muss es sein, durch die nationalen Vertreter im Europäischen Datenschutzausschuss darauf hinzuwirken, dass die Standards der DSGVO im europäischen Kontext nicht verwässert werden. Dabei geht es insbesondere darum, einen angemessenen Ausgleich zwischen der Unabhängigkeit von Datenschutzaufsichtsbehörden einerseits und der Funktion des Europäischen Datenschutzausschusses als entscheidender Instanz bei der Auslegung des europäischen Datenschutzrechts andererseits zu schaffen. Die Durchführung sogenannter Kohärenzverfahren in diesem Gremium ist daher keineswegs gegen die Unabhängigkeit der Aufsichtsbehörden gerichtet oder dazu angetan, diese an den Pranger zu stellen. Vielmehr gilt es, eine Rechtsanwendungsgleichheit innerhalb der EU zu schaffen, die notwendigerweise auch strittige Verfahren vor diesem Gremium erforderlich machen. Nur wenn es gelingt, Unternehmen einheitlich zu behandeln, und Datenschutzwüsten in Europa zu verhindern, wird das Projekt der DSGVO erfolgreich verlaufen.

PRÜFUNGEN II.

1. Feuerwehr: Noch immer kein Schutz von Funkdaten bei der Notallalarmierung

Der im September 2016 festgestellte Mangel besteht auch zwei Jahre später immer noch.

Im 26. Tätigkeitsbericht hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBFDI) darüber berichtet, dass die Feuerwehr Hamburg personenbezogene Daten von Bürgerinnen und Bürgern im Zuge der Notfall-Alarmierung von Rettungsfahrzeugen per Funk unverschlüsselt an die Empfänger übermittelt. Diese sensiblen Daten wurden von Unbekannten abgehört und zeitweilig im Internet veröffentlich. Im Zuge des ersten illegalen Abhörvorfalles und der Veröffentlichung der Notfalldaten im Internet hatte die Feuerwehr als erste Maßnahme den übertragenen Datensatz gekürzt. Da auch in dem verbleibenden gekürzten Datensatz nach wie vor sensible personenbezogene Daten übertragen werden, müssen auch diese verkürzten Datensätze verschlüsselt werden. Die Feuerwehr hatte uns Ende Oktober 2017 mitgeteilt, dass diese Verschlüsselung im 2. Quartal 2018 realisiert wird (vgl. 26. TB II. 3).

Bei Redaktionsschluss besteht der Mangel im IT-Verfahren der Feuerwehr immer noch. Die Notfalldaten werden weiterhin unverschlüsselt übertragen.

Im April 2018 hatte uns die Feuerwehr auf Nachfrage noch mitgeteilt, dass ab dem 01.07.2018 eine verschlüsselte Übertragung an die Erstversorgungskräfte erfolgen soll. Erst Anfang Juli 2018 haben wir dann von der Feuerwehr die Information erhalten, dass aufgrund technischer Schwierigkeiten bei der Funkübertragung der Start der verschlüsselten Übertragung auf den 01.11.2018 verschoben werden musste. Bei

Tests der verschlüsselten Übertragung stellte sich heraus, dass in verschiedenen Bereichen Hamburgs die Funkübertragung nicht mit ausreichender Sicherheit gewährleistet werden konnte. Auf unsere Nachfrage vom Ende September 2018 hat die Feuerwehr dann angedeutet, dass die technischen Schwierigkeiten bei der verschlüsselten Funkübertragung nach wie vor groß seien und ein Vermerk zum Stand und zur weiteren Planung in Kürze folgen werde. Erst am 08.11.2018 hat uns die Feuerwehrleitung in Kenntnis gesetzt, dass der Termin 01.11.2018 aufgrund der technischen Schwierigkeiten nicht gehalten werden konnte. Seit Dezember 2018 liegt nun eine erste Beschreibung des neuen technischen Konzepts der Feuerwehr vor, wie die Verschlüsselung der Notfalldaten unter Nutzung einer Internet-gestützten Übertragung auf die privaten Smartphones der zu informierenden Personen erfolgen soll. Der avisierte Realisierungstermin der Feuerwehr ist das Ende des ersten Quartals 2019. Aus dieser Beschreibung geht hervor, dass für diese Lösung noch Entwicklungsarbeiten eines Dienstleisters erforderlich sind. Mit Blick auf die betroffenen Bürgerinnen und Bürger werden wir uns weiterhin dafür einsetzen, dass dieser Termin gehalten wird.

Um eine größere Ausfallsicherheit der Übertragung der Notfalldaten zu erreichen, plant die Feuerwehr als zweiten produktiven Übertragungsweg mittelfristig auch hierfür den BOS-Digitalfunk zu verwenden. Bereits im August 2017 haben die Leitung der Feuerwehr und der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Einigkeit darüber hergestellt, dass die Ertüchtigung des BOS-Netzes parallel mit Hochdruck vorangetrieben werden sollte, um dieses schnellstmöglich nutzen zu können. Leider wurde dieser zweite Ansatz von der Feuerwehr nicht wie besprochen mit der dafür erforderlichen Kapazität verfolgt.

2. Teilprüfung OK-EWO Melde-Pass-Personalausweisregister

700.000 Dokumente wurden im Personalausweis- und Passregister nicht fristgerecht gelöscht. Bei Änderungen der rechtlichen Vorgaben für die Datenverarbeitung muss die eingesetzte Software zeitgerecht rechtskonform angepasst werden.

Die Eingabe eines Bürgers haben wir zum Anlass genommen, Teile des IT-Verfahrens OK-EWO zu prüfen, das für die Verarbeitung der Melde-, Pass- und Personalausweisdaten und die Führung der jeweiligen Register hamburgweit genutzt wird. Dabei haben wir erhebliche Mängel festgestellt. Da die Verantwortlichen die Beseitigung der festgestellten Mängel umgehend zugesagt hatten und diese zum Teil auch bereits erfolgt ist, konnten wir nach § 25 Abs. 2 Hamburgisches Datenschutzgesetz a.F. (HmbDSG a.F.) von einer Beanstandung absehen.

- **Melderegister**
  Gemäß § 13 Abs. 1 des am 01.11.2015 in Kraft getretenen Bundesmeldegesetzes (BMG) sind nach Wegzug oder Tod die Daten zu hoheitlichen Dokumenten nicht mehr im Melderegister zu speichern. Diese Veränderung war im März 2018 im IT-Verfahren OK-EWO noch nicht umgesetzt. Damit wurden über fast 2,5 Jahre Daten im Melderegister verarbeitet, für die es seit dem Inkrafttreten des BMG am 01.11.2015 keine Rechtgrundlage mehr gab. Dem für dieses Verfahren federführenden Bezirksamt Harburg war diese Tatsache bereits seit Ende 2015 bekannt.

  Erst zum 01.05 2018 wurde dieser Mangel mit einer neuen Version des IT-Verfahrens behoben. Die für das IT-Verfahren Verantwortlichen haben uns mitgeteilt, dass mit

dem Hersteller der Standardsoftware vereinbart wurde, dass zukünftig die vom Kunden gemeldeten Rechtsfehler mit Priorität 1 zur jeweils nächstmöglichen Version behoben werden.

- **Personalausweisregister und Passregister**
  Nach § 23 Abs. 4 S. 1 Personalausweisgesetz (PAuswG) sind personenbezogene Daten im Personalausweisregister mindestens bis zur Ausstellung eines neuen Ausweises, höchstens jedoch bis zu fünf Jahren nach dem Ablauf der Gültigkeit des Ausweises, auf den sie sich beziehen, zu speichern und dann zu löschen.

  Durch die Eingabe eines Bürgers, für den diese fünfjährige Höchstfrist seit langem abgelaufen war, ist deutlich geworden, dass dennoch – wenn auch nicht mehr alle – Personalausweisdaten gespeichert waren. Nach § 23 Abs. 4 S. 1 PAuswG und der entsprechenden Regelung in § 21 Abs. 4 Passgesetz (PassG) sind nach Ablauf der Höchstfrist jedoch sämtliche Daten zu löschen. Auf Nachfrage haben wir vom Bezirksamt Harburg erfahren, dass es für solche Fälle zwar ein Löschprogramm vom Softwarehersteller gibt, welches jedoch nicht zuverlässig läuft und deshalb keine Freigabe für den Produktivbetrieb hatte. Die Daten konnten bis zum Prüfungszeitpunkt nur manuell gelöscht werden. Dies unterblieb jedoch unzulässiger Weise. Insgesamt standen Anfang März 2018 ca. 700.000 Datensätze von Betroffenen, deren Daten im Personalausweisregister und im Passregister entgegen der bestehenden Löschvorschriften und damit ohne Rechtsgrundlage gespeichert waren, zur Löschung an. Die Löschung der Dokumente erfolgte in zwei Schritten. Im März 2018 ist die Löschung von 417.058 Fällen im Personalausweis-/Passarchiv erfolgt. Die Löschung der weiteren Dokumente im aktuellen Personalausweis- und Passregister wurde im August 2018 durchgeführt.

Datentrennung – Gemeinsames Verfahren

Im IT-Verfahren OK-EWO werden die Daten des Melde-, des Pass- und des Personalausweisregisters durch die Melde-, Pass-, und Personalausweisbehörden der Bezirksämter und durch die Behörde für Inneres und Sport (BIS) verarbeitet.

Mit Geltung der DSGVO regelt Art. 26 DSGVO Verfahren mit gemeinsam für die Verarbeitung Verantwortlichen. Danach haben diese eine Vereinbarung zu schließen, aus der in transparenter Form hervorgeht, wer von ihnen in welcher Form die Verpflichtungen aus der DSGVO erfüllt. Darüber hinaus ist nach § 7 HmbDSG n.F. die Einrichtung eines automatisierten Abrufverfahrens oder einer gemeinsamen automatisierten Datei, in oder aus der mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten, nur zulässig, soweit dies unter Berücksichtigung der Rechte und Freiheiten der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist und durch technische und organisatorische Maßnahmen Risiken für die Rechte und Freiheiten der betroffenen Personen vermieden werden können. Wir haben den Verantwortlichen daher aufgegeben, den Anforderungen nach § 7 HmbDSG n.F. nachzukommen und die nach Art. 26 DSGVO notwendige Vereinbarung zu treffen. Eine solche Vereinbarung liegt uns im Entwurf vor. Hierzu sind wir in konstruktiven Gesprächen mit den Verantwortlichen.

3. Data Warehouse JUS-IT

Die verantwortliche Stelle hat die erforderliche Löschung von sensiblen Sozialdaten fast 1,5 Jahre nach Erhalt des datenschutzrechtlichen Prüfberichts immer noch nicht umgesetzt.

Die Behörde für Arbeit, Soziales, Familie und Integration (BASFI) nutzt für die fachliche Unterstützung der Jugendhilfe das IT-Verfahren JUS-IT. Um neben der Facharbeit auch die Ablaufprozesse effektiv zu unterstützen und eine verbesserte operative und ministerielle Steuerung des Hilfegeschehens zu ermöglichen, wurde ergänzend das Data Warehouse JUS-IT eingeführt. Das Konzept für dieses Data-Warehouse sieht vor, dass monatlich eine Auswahl von Datenelementen jedes Einzelfalls aus dem Fachverfahren extrahiert wird.

Im Konzept des JUS-IT Data Warehouse ist festgelegt, dass ausschließlich anonymisierte Daten verarbeitet werden sollen. Unsere Prüfung des Data Warehouse hat ergeben, dass diese Aussage bei genauerer Betrachtung nicht haltbar ist. An zwei Stellen wird deutlich, dass ein Personenbezug hergestellt werden kann. Zum einen werden die Daten lediglich pseudonymisiert und zum anderen können Betroffene dadurch identifiziert werden, dass sie nicht in einer ausreichend großen Menge von Datensätzen verborgen sind.

Das Konzept sieht folgende Vorgehensweise beim Beladen des Data Warehouse vor:
Vor dem Beladen ins Data Warehouse werden die eindeutigen Kennzeichnungen von Betroffenen gehasht und das Geburtsdatum des Hauptbeteiligten auf den Ersten des Monats gesetzt. Zur Fehlerbereinigung existiert ein Prozess, wie diese Pseudonymisierung rückgängig gemacht werden kann. Administratoren bei Dataport nutzen dazu im Auftrag

des Jugendhilfeträgers eine Zuordnungstabelle, in der die gehashten Fallreferenzen aus dem Data Warehouse den Fallreferenzen aus dem Fachverfahren zugeordnet sind.

Die Auslagerung der Zugriffe auf einen Auftragsverarbeiter und ihre Begrenzung ändert nichts an der Tatsache der bloßen Pseudonymisierung, da die Zugriffe des Auftragsverarbeiters auf die Zuordnungstabelle dem Jugendhilfeträger als Verantwortlichem zuzurechnen sind. Die Zugriffsbeschränkung auf Dataport – und nicht auf die Fachliche Leitstelle unmittelbar – ist vielmehr lediglich als eine wichtige Maßnahme einzuordnen, die eine Beschränkung des Missbrauchs dieser Zuordnungsmöglichkeiten zum Ziel hat, nicht aber zu einer Anonymisierung führt. Die Prüfung hat ergeben, dass die zuständigen Mitarbeiter des Auftragsverarbeiters Dataport sowohl Zugang zur Depseudonymisierungskomponente als auch zum Fachverfahren JUS-IT und zum Data Warehouse haben. Sie können somit für jeden Datensatz des Data Warehouses die Identität eines Betroffenen selber ermitteln.

Unsere Prüfung hat auch ergeben, dass die Daten, die im Data Warehouse gespeichert sind, nicht mehr gelöscht werden. Im Gegensatz dazu unterliegen dieselben Daten im Fachverfahren JUS-IT einem differenzierten Löschkonzept. Da ausgewählte Daten aus dem Fachverfahren JUS-IT regelmäßig überführt werden, jedoch keine Löschung dieser einmal überführten Daten erfolgt, sobald die jeweilige Löschfrist im Fachverfahren greift, bleiben diese Daten im Data Warehouse gespeichert.

Nach mehreren Gesprächen über den Prüfbericht und die sich daraus ergebenden Konsequenzen hat uns die verantwortliche Stelle im September 2018 dargelegt, dass im Data Warehouse zukünftig pseudonymisierte Daten verarbeitet werden sollen. Es wurde schlüssig erläutert, dass die im Data Warehouse verarbeiteten Daten primär der Wahrnehmung

der Fachaufsicht und der allgemeinen fachlichen Steuerung der Jugendhilfe dienen und die technische Grundlage für das Berichtswesen der „Fachanweisung Allgemeine Soziale Dienste“ ist. Die damit verbundene Speicherung, Veränderung oder Nutzung ist i.S.d. § 67c Abs. 3 S. 1 SGB X erforderlich, um die fachaufsichtlichen Zwecke zu erfüllen. Diese Regelung verlangt keine unverzügliche Anonymisierung.

Die bestehenden Löschungsverpflichtungen sollen nach Zusage der verantwortlichen Stelle zukünftig auch im Data Warehouse genauso eingehalten werden wie die weiteren Anforderungen, die sich aus der DSGVO ergeben.

Das von der BASFI ursprünglich bis Oktober 2018 angekündigte Löschkonzept lag dem HmbBfDI aufgrund ergänzender behördlicher Klärungs- und Begründungsbedarfe zum Redaktionsschluss noch nicht vor. Inwieweit daher die Löschung derjenigen Sozialdaten im Data Warehouse, für die es teilweise schon lange keine Rechtsgrundlage der Verarbeitung mehr gibt, noch wie geplant bis Ende 2018 erfolgt, ist fraglich. Im Zeitpunkt des Redaktionsschlusses stehen die Umsetzung des veränderten Konzeptes und die Löschung jedenfalls weiterhin aus.

4. Prüfung Windows 10 auf den BASIS-Rechnern der FHH

Wir haben Windows 10 für den Behördeneinsatz datenschutztechnisch untersucht und unsere Empfehlungen für den Betrieb an Dataport gegeben.

Im Rahmen der Windows 10-Einführung für die gesamte FHH durch Dataport haben wir uns mit der Frage auseinandergesetzt, ob Windows 10 Enterprise aus Datenschutzperspektive

für den behördlichen Einsatz tauglich ist. Im Vordergrund stand hierbei die Frage, inwieweit ein Tracking durch Microsoft, mit dem eine einzelne Nutzerin oder Nutzer oder ein bestimmtes Gerät identifizierbar wird, vermieden werden kann, soweit dies nicht unbedingt für den Betrieb notwendig ist.

Wir vertreten die Position, dass ein Betriebssystem als Plattform für die Arbeit mit Computern keinerlei für den Nutzer nachteilige Funktionen aufweisen darf, die nicht erforderlich sind und für die keine Rechtsgrundlage besteht. Hierbei stehen insbesondere die Funktionen im Fokus, die für den Betrieb des Gerätes nicht notwendig sind, wie Nutzungstelemetrie, Benutzertracking, Werbung oder die erzwungene Bereitstellung unerwünschter Software.

Hiervon ausgenommen sind erforderliche Funktionen, die die Sicherheit gewährleisten wie die regelmäßige Prüfung auf und Installation von Systemupdates oder die Verfolgung des Netzwerkverkehrs durch eine lokal operierende Firewall und die Systemprotokollierung.

Windows 10 steht seit seiner Einführung in der Kritik von Datenschützern und IT-Fachleuten, da es neben einer Reihe von Software, die unabhängig vom Nutzungsbedarf installiert wird und deren Entfernung zum Teil unmöglich ist, auch umfangreiche Telemetriedaten an Microsoft sendet und dabei auf Pseudonyme setzt, um die Installation oder die Nutzerinnen und Nutzer wiedererkennen zu können. Diese Funktionalität steht einem datenschutzgerechten Einsatz im Weg und ist daher regelmäßig Gegenstand von Untersuchungen.

Wir haben die BASIS-Konfiguration geprüft, die von Dataport für die öffentliche Verwaltung der Freien und Hansestadt Hamburg betrieben wird. Eine Analyse sollte klären, ob die BASIS-Konfiguration einen datenschutzgerechten Betrieb für den HmbBfDI und die FHH ermöglicht.

Zur Beantwortung dieser Frage haben wir einen Laboraufbau erstellt, in dem der Datenverkehr eines in BASIS-Konfiguration betriebenen Windows 10 über mehrere Tage bei normaler Benutzung beobachtet und ausgewertet werden konnte. Für die Erstellung einer BASIS-Konfiguration wurde dieser Testlauf von Dataport unterstützt.

Im Rahmen des Tests konnte zunächst diagnostiziert werden, dass die Vorarbeit von Dataport bei der datenschutzfreundlichen Konfiguration von Windows 10 bereits einen großen Teil der im Vergleichstest mit einer Standardkonfiguration beobachteten Datenströme abstellt. Jedoch konnte im Testverlauf weiterer Datenverkehr beobachtet werden, der bei genauerer Inspektion auch personenbezogene und solche Daten enthielt, die eine Installation von Windows individuell wiedererkennbar machen.

Im weiteren Testverlauf konnten wir durch gezielte Anpassung der Systemkonfiguration den beobachteten Datenverkehr deutlich reduzieren. Die vorgenommenen Änderungen wurden dokumentiert und in Form eines Abschlussberichts mit Konfigurationsempfehlungen an die Senatskanzlei und Dataport übergeben. Der verbleibende Datenverkehr nach diesen Anpassungen ist nach bisherigem Kenntnisstand frei von Benutzer- und Maschinentracking und teilweise für den Betrieb von Windows erforderlich.

Da Windows 10 zweimal jährlich ein Feature-Update erfährt und sich jedes Mal auch das Systemverhalten und Konfigurationsoptionen ändern, stellt dieser Test nur eine Momentaufnahme der Windows 10 Version 1803 dar und sollte im Auftrag der Senatskanzlei vom Dienstleister Dataport regelmäßig für die nachfolgenden Versionen wiederholt werden. Der HmbBfDI wird sich mit diesem Thema weiter beschäftigen.

Der gesamte Prozess der Einführung von Windows 10 wurde vom HmbBfDI kritisch begleitet. Die einseitige Abhängigkeit der Dataport-Trägerländer von Microsoft-Produkten wird die öffentliche Verwaltung in diesen Ländern immer wieder in Situationen führen, in denen technisch-organisatorische Maßnahmen gegen das zugrundeliegende Geschäftsmodell ergriffen werden müssen. Daher befürwortet der HmbBfDI jeden Versuch, sich aus dieser Abhängigkeit zu lösen und durch den Einsatz freier Software neben besserem Datenschutz auch Transparenz und Offenheit gegenüber Bürgerinnen und Bürgern herzustellen. Wir werden uns mit diesem Thema weiter beschäftigen, und entsprechende Vorschläge einbringen.

5. Zugriff auf Dienstrechner der FHH durch Vorgesetzte

Auch dienstliche E-Mails von Behördenmitarbeiterinnen und -mitarbeitern unterliegen dem Fernmeldegeheimnis, sodass Vorgesetzte darauf in der Regel nicht zugreifen dürfen.

Die Freie und Hansestadt Hamburg erlaubt ihren Beschäftigten die Nutzung der dienstlichen Infrastruktur in moderatem Umfang auch zu privaten Zwecken. Dies folgt aus der Vereinbarung nach § 94 Hamburgisches Personalvertretungsgesetz (HmbPersVG) zur Bürokommunikation. Private Tätigkeiten in großem Umfang stellen hingegen eine missbräuchliche Nutzung der Dienstzeit dar. Durch die Antwort des Senats vom 5.8.2018 auf eine Kleine Anfrage in der Bürgerschaft haben wir erfahren, dass seit 2010 in mindestens dreizehn Fällen Vorgesetzte auf Dienstrechner zugegriffen haben, um eine missbräuchliche Nutzung der Arbeitszeit nachzuweisen.

Indem die Behörden die private Nutzung des Internetzugangs erlauben, werden sie für ihre Beschäftigten zu Telekommunikationsanbietern. Als solche haben sie das Fernmeldegeheimnis zu achten, das unbefugte Zugriffe auf Kommunikationsinhalte untersagt. Insbesondere E-Mail-Inhalte sind durch § 88 TKG geschützt. Eine den Zugriff gestattende Erlaubnis kann durch Einwilligung des Beschäftigten abgegeben werden, die jedoch im Dienst- und Arbeitsverhältnis mangels hinreichender Freiwilligkeit nur selten wirksam ist. Die praktikablere Alternative sind daher Personalvereinbarungen, in denen der weisungsfrei agierende Personalrat stellvertretend für die Belegschaft Zugriffe auf Kommunikationsinhalte wirksam erlauben kann. Für den nichtöffentlichen Bereich hat der Arbeitskreis Beschäftigtendatenschutz im Jahr 2016 unter Vorsitz Hamburgs eine Orientierungshilfe zur datenschutzgerechten Nutzung von E Mail und anderen Internetdiensten am Arbeitsplatz erarbeitet (*https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf*).

Hamburgische Behörden stützen ihre Zugriffe zur Kontrolle der missbräuchlichen Arbeitszeitnutzung in der Regel auf Ziff. 4 Abs. 5 der § 94er-Vereinbarung zur Bürokommunikation. Zwar ist diese Personalvereinbarung grundsätzlich geeignet, Einschränkungen des Fernmeldegeheimnisses zuzulassen. Die darin enthaltene Erlaubnisklausel gestattet jedoch nur in seltenen Fällen einen Zugriff auf wenige Metadaten. Danach dürfen „ausschließlich Verbindungs- und Nutzungsdaten" ausgewertet werden, wenn bereits zuvor ein konkreter Verdacht eines Dienstvergehens bzw. einer Verletzung des Arbeitsvertrags besteht. Die Begriffe „Verbindungs- und Nutzungsdaten" sind dem TKG bzw. dem TMG entnommen und bezeichnen dort technische Daten, die für den Verbindungsaufbau und dessen Abrechnung durch den Provider benötigt werden. Inhalte der E-Mail-Kommunikation fallen nicht unter diese engen Begriffe.

Wenn der Senat sich entschließt, seinen Beschäftigten die private Nutzung des dienstlichen E-Mail-Accounts zu erlauben, hat er auch deren Privatsphäre zu achten. Da von vornherein nicht zwischen dienstlichen und privaten E-Mails differenziert werden kann, entziehen sich sämtliche Kommunikationsinhalte der Kontrolle des Arbeitgebers.
Wir haben mit den Senatsbehörden Kontakt aufgenommen hinsichtlich der Grenzen des Zugriffs auf E-Mail-Accounts und mögliche Lösungswege für die Zukunft.

6. Hamburger Informationsmanagement 2.0

Das Hamburger Informationsmanagement wurde weiterentwickelt und soll, im Gegensatz zur Vorgängerversion, nun auch für die Verarbeitung von Daten mit hohem Schutzbedarf einsetzbar sein. Nach bisherigem Stand bestehen jedoch noch Zweifel, dass die getroffenen organisatorischen und technischen Schutzmaßnahmen ausreichen, den hierfür erforderlichen Schutz zu gewährleisten.

Mit der Einführung der elektronischen Vorgangsverarbeitung, dem Workflow des Hamburger Informationsmanagements (HIM-Workflow), können Entscheidungs-, Genehmigungs- und Abstimmungsprozesse der Verwaltungseinheiten elektronisch erfolgen und medienbruchfrei in die elektronische Akte (ELDORADO) übernommen werden. Zudem wird durch verfügbare Suchfunktionen das Auffinden elektronischer Geschäftsvorgänge erleichtert.

In Abhängigkeit von der jeweiligen Aufgabe können die in den Geschäftsgang einzubeziehenden Dokumente personenbezogene Daten unterschiedlicher Sensibilität beinhalten. Die Behörden haben dann durch technische und organisatorische Maßnahmen sicherzustellen, dass diese Daten im

gesamten Verarbeitungsprozess vor unberechtigten Zugriffen geschützt sind.

Die neue Version HIM 2.0 soll, im Gegensatz zur Vorgängerversion, nunmehr auch für die Verarbeitung von Daten mit hohem Schutzbedarf ausgelegt und einsetzbar sein.
Hinsichtlich der Bewertung der getroffenen Schutzmaßnahmen, welche diesen Schutz gewährleisten sollen, befinden wir uns derzeit noch im Austausch mit der Senatskanzlei, da wir im Vorwege der Einführung nicht einbezogen wurden. Nach bisherigem Stand haben wir Zweifel, dass die erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO getroffen worden sind.

In Art. 5 Abs. 2 DSGVO ist die Rechenschaftspflicht festgeschrieben. Danach muss der Verantwortliche nachweisen können, dass die Anforderungen der DSGVO eingehalten werden, also beispielsweise auch belegen können, dass nur Berechtigte auf die Inhalte zugegriffen haben.

Eine Zugriffsprotokollierung ist in HIM bislang nicht vorgesehen, da die Berechtigungen beim Erstellen des Workflows vom System ausschließlich für die berechtigten Personen gesetzt würden und damit nur berechtigte Personen zugreifen könnten.

Um im Bedarfsfall die Vertretung wahrnehmen oder die Aufgabe einem anderen Beschäftigten zuweisen zu können, werden derzeit jedoch automatisch den Vorgesetzten des jeweils aktuellen Workflowschrittverantwortlichen die gleichen Rechte erteilt wie dem Workflowschrittverantwortlichen, wobei lesende Zugriffe ebenfalls nicht protokolliert werden. Die Vorgesetzten werden hierbei standardmäßig aus dem HamburgService- Informationssystem (HaSI) übernommen und sind durch die Beschäftigten nicht änderbar. Sie können lediglich weitere fachliche Vertretungen einrichten.

Eine Möglichkeit, einen Vorgang außerhalb der Standardvertretungsrechte abzuwickeln („Vertraulichkeitsfunktion"), ist in HIM 2.0 bislang nicht verfügbar. Eine solche Beschränkung erfolgt z.B., wenn eine E-Mail verschlüsselt wird und dadurch auch der Stellvertreter regelhaft keinen Zugriff mehr hat.

Für Mitarbeiter, die neben ihren „normalen" dienstlichen Aufgaben eine vertrauliche Sonderfunktion wahrnehmen, wie Personalräte oder behördliche Datenschutzbeauftragte, sind die aus HaSI übernommenen Vorgesetzten i.d.R. nicht die Vertreter und es darf diesen mithin auch kein Zugriffsrecht eingeräumt werden. Zur Wahrung der Vertraulichkeit dürften diese Mitarbeiter Workflows im Rahmen ihrer Sonderfunktion daher derzeit nur mit gesonderten Kennungen ohne Standardvertretungsrechte initiieren und zudem nur Mitarbeiter in den Workflow einbinden, bei denen dies ebenfalls gewährt ist. Da die Zugriffsrechte auf der Empfängerseite nicht transparent sind, ist dieser Weg nicht datenschutzgerecht, da die Vertraulichkeit nicht gewährleistet werden kann.
Die Senatskanzlei teilte kurz vor Redaktionsschluss mit, dass die Umsetzung und Einführung einer Vertraulichkeitsfunktion für 2019 eingeplant ist.

Der HIM-Workflow ist in das FHHportal, das auf Microsoft Sharepoint basiert, integriert. Auch die Schutzmaßnahmen für das FHHportal waren bislang – mit Ausnahme der Schutzmaßnahmen für SecureSites – auf die Verarbeitung von Daten mit normalem Schutzbedarf abgestimmt. Die Risikobetrachtung für das FHHportal wird laut Mitteilung der Senatskanzlei derzeit aktualisiert und soll uns nach Fertigstellung im 1. Quartal 2019 übersandt werden.

Entsprechend der aktuellen Unterlagen soll künftig Nutzern außerhalb des FHHNet über das Internet Zugriff auf geschützte Seiten ermöglicht werden (ZUVEX).

Für solche Zugriffe sind die Anforderungen, die die EU eIDAS-Verordnung vorgibt und in der Richtlinie des BSI TR 03107-1 konkretisiert sind, einzuhalten. Werden Zugriffe auf Daten mit hohem Schutzbedarf ermöglicht, ist ein hohes Vertrauensniveau erforderlich. Dies setzt entsprechend sichere Authentisierungsverfahren voraus. Dies sind nach der TR ausschließlich Verfahren, bei denen eine Zwei-Faktor-Authentisierung zum Einsatz kommt. Der Einsatz einer Zwei-Faktor-Authentisierung ist laut Mitteilung der Senatskanzlei für Hamburg bisher jedoch nicht vorgesehen. Es wurde jedoch in Aussicht gestellt, dass im Jahr 2019 weitere zusätzliche Schutzmechanismen für ZUVEX analysiert werden sollen, welche die Sicherheit weiter verbessern sollen.

Bis zum Redaktionsschluss konnten noch nicht alle offenen Punkte geklärt werden. Wir werden uns weiter für eine datenschutzgerechte Lösung einsetzen.

7. PC einer Schule mit personenbezogenen Daten im Müllcontainer gefunden

Uns wurde ein PC übergeben, der nach dem Brand in einer Schule im Müllcontainer aufgefunden worden war. Wir konnten darauf personenbezogene Daten von Schülerinnen und Schülern, Erziehungsberechtigter und weiterer Dritter auslesen und auch auf den E-Mail-Posteingang zugreifen.

Im Juli des vergangenen wurde uns durch einen Bürger ein Computer übergeben. Nach eigenen Angaben hatte er diesen zuvor aus einem öffentlich zugänglichen Müllcontainer einer Schule entnommen, in dem sich Renovierungsmüll nach einem Gebäudebrand befand.

Der äußerlich unbeschadete Computer wies im Inneren zwar eine erhebliche Rußbelastung auf, war aber funktionsfähig. Nach Ent- und Inbetriebnahme der eingebauten Festplatte an einem Laborgerät konnten wir auf das Nutzerprofil des Hauptnutzers zugreifen und Inhaltsdaten sichten. Durch forensische Analyse des freien Speichers konnte Zugriff auf weitere, auch bereits gelöschte Dokumente erlangt werden. Ebenfalls wiederherstellen ließen sich Teile des Benutzerprofils inklusive Browserhistorie und persönlicher Arbeitszeitabrechnungen des Hauptbenutzers.

Die Analyse ergab auch, dass der Computer nach dem Brand nicht mehr länger in Benutzung war und offenbar direkt entsorgt wurde. Ebenso war erkennbar, dass vor der Entsorgung Dateien mit potentiell personenbezogenen Daten logisch gelöscht, jedoch nicht überschrieben wurden, wodurch sich ein großer Teil dieser Dateien wie beschrieben wiederherstellen ließ.

Ein datenschutzkonformes Löschen der auf dem Rechner gespeicherten Daten hätte vorausgesetzt, dass der in Baustein B 1.15 des IT-Grundschutz-Katalogs des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschriebene oder ein vergleichbarer dem Stand der Technik entsprechender Löschungs- und Entsorgungsstandard eingehalten wurde. Werden Datenträger nicht mehr benötigt, wie hier wegen brandbedingt eingeschränkter Reproduktionsfähigkeit der darauf aufbewahrten Daten, so sind die darauf gespeicherten Daten sicher zu löschen oder die Datenträger datenschutzgerecht zu vernichten. Die Art der Löschung bzw. der Vernichtung hängt dabei von der Art der Datenträger und von der Schutzklasse der gespeicherten Daten ab, aus der sich die anzuwendende Sicherheitsstufe ableitet. Je sensibler die zu vernichtenden Daten sind, desto höhere Anforderungen sind gemäß Art. 32 DSGVO an die technisch-organisatorischen Maßnahmen zur Datenträgervernichtung zu stellen.

Vorliegend ist unter Berücksichtigung der besonderen Schutzbedürftigkeit von Schülerinnen und Schülern und der Sensibilität von Zeugnisdaten, Beschäftigtendaten u.a. von einem hohen Schutzbedarf der in dem aufgefundenen Rechner gespeicherten personenbezogenen auszugehen. Daraus folgt eine Zuordnung zur Schutzklasse 2. Datenträger mit personenbezogenen Daten der Schutzklasse 2 sind gemäß DIN 66399 grundsätzlich mindestens nach der Sicherheitsstufe 4 zu vernichten. Eine Reproduktion solcher mit Sicherheitsstufe 4 gelöschter Daten ist nur mit außergewöhnlich hohem Aufwand möglich. Den Aufwand, den wir zum Wiederherstellen der Daten betreiben mussten, war dagegen begrenzt.

Auf Grundlage des geschilderten Sachverhalts sind somit personenbezogene Daten in einer dem Verantwortlichkeitsbereich der Behörde für Schule und Berufsbildung (BSB) zuzuordnenden staatlichen Schule unter Verstoß gegen § 8 HmbDSG a. F. i. V. m. § 101 HmbSG a. F. und § 3 Abs. 1 SchulDSV HA 2006 gelöscht und entsorgt worden. Da der Rechner nach Angaben des Anzeigenden erst am 11.07.2018 aus dem Müllcontainer entnommen wurde, hat der Datenschutzverstoß auch nach Inkrafttreten der DSGVO angedauert. Folglich liegt zugleich auch ein Verstoß gegen Art. 32 DSGVO vor.

Der PC wurde daraufhin mit der Aufforderung datenschutzgerechter Entsorgung an die BSB ausgehändigt. Zugleich erging im Hinblick auf den Verstoß ein Hinweis gemäß Art. 58 Abs. 1 lit. d) DSGVO an die Behörde.

Angesichts der Tatsache, dass noch nicht abschließend geklärt werden konnte, ob die rechtswidrige Entsorgung des Schul-PCs von einer zur Entsorgung des Schulinventars beauftragten, externen Firma zu verantworten ist, hat der HmbBfDI darüber hinaus keinen Gebrauch von seinen Befugnissen nach Art. 58 Abs. 2 DSGVO gemacht.

8. Videoüberwachung durch das Iranische Konsulat

Vom Generalkonsulat der Islamischen Republik Iran in Hamburg aus wurden der öffentliche Straßenraum und die dort zum Schutz des Konsulats abgestellten Polizeivollzugsbediensteten gefilmt.

In diesem Fall hatte sich die Polizei Hamburg an uns gewandt und um unsere Mithilfe gebeten. Das Gebäude des Generalkonsulats der Islamischen Republik Iran in der Bebelallee wurde mit Videokameras überwacht, die an Stelen befestigt waren. Diese waren zum Teil auf den Bürgersteig gerichtet und eine Kamera war so angebracht, dass sie wie eine Angel auf den Fußgängerweg reichte und direkt über den Polizeivollzugsbediensteten hing, die zum Schutz des Generalkonsulats abgestellt waren und damit direkt unter den Kameras ihren Dienst verrichten mussten. Sie waren bei ihrer täglichen Arbeit einer Überwachung durch einen ausländischen Staat ausgesetzt, die nach deutscher Rechtsprechung nicht einmal durch den eigenen Arbeitgeber zulässig gewesen wäre.

Das Generalkonsulat der islamischen Republik Iran unterfiel nicht dem damals noch anwendbaren Bundesdatenschutzgesetz und unterlag daher auch nicht unserer Kontrolle. Gleichzeitig hatte die Polizei uns eindringlich um Hilfe gebeten, weil man den eigenen Vollzugsbediensteten nicht zumuten wollte, unter derartigen Bedingungen Dienst leisten zu müssen. Mangels Hoheitsbefugnissen haben wir uns mit einem Schreiben direkt an den Generalkonsul gewandt. Wir fragten an, ob es nicht trotz der angespannten Sicherheitslage im Hinblick auf das Gebäude des Generalkonsulats möglich sei, eine Lösung zu finden, die Sicherheitsbelange des Generalkonsulats angemessen zu schützen und dabei die Rechte unbescholtener Bürgerinnen und Bürger sowie der

ihren Dienst ausübenden Polizeibeamten, die ja auch für die Sicherheit des Generalkonsulats sorgen, so weit wie möglich zu wahren. Zwar haben wir auf unser Schreiben nie eine Antwort erhalten. Allerdings hat uns die Polizei einige Zeit später mitgeteilt, dass die „Angel-Kamera" nicht mehr direkt über den diensthabenden Polizeivollzugsbediensteten schwebt und diese sich nicht mehr einem durchgehenden und geradezu physischen Überwachungsdruck ausgesetzt sehen.

Der Fall zeigt das Datenschutzbewusstsein unserer Kolleginnen und Kollegen von der Polizei in diesem Fall und die Tatsache, dass man manchmal auch ohne Hoheitsbefugnisse mit einem höflichen, aber im Kern deutlichen Anschreiben einiges erreichen kann.

9. Videoüberwachung zur Durchsetzung von Diesel-Fahrverboten

Nach jahrelanger Passivität trotz überschrittener Grenzwerte schaltet die Politik auf Bundesebene nun um auf hektische Aktivität. Würden die angekündigten Pläne eines umfassenden KFZ-Screenings Realität, bliebe der Datenschutz auf der Strecke.

Der von der Bundesregierung eingebrachte Gesetzentwurf eines „Neunten Gesetzes zur Änderung des Straßenverkehrsgesetzes", enthält den Vorschlag, die Einhaltung von Verkehrsbeschränkungen für Diesel-Fahrzeuge mit der automatisierten Erfassung aller Verkehrsteilnehmer durch den Einsatz von intelligenter Videoüberwachungstechnik durchzusetzen. Die geplanten Regelungen sollen den Behörden erlauben, automatisiert zu überprüfen, ob gegen Durchfahrtsbeschränkungen für Diesel-Fahrzeuge verstoßen wird. Hierzu sollen diese künftig durch intelligente Videoüberwachung

die Fahrzeugmerkmale und -kennzeichen sowie ein Bild des Fahrzeugs und des Fahrers speichern und verwenden. Ferner ist der Zugriff auf Daten des Zentralen Fahrzeugregisters zugelassen.

Eine Kontrolle von Fahrverbotszonen setzt danach den Aufbau einer umfassenden Überwachungsstruktur zum automatisierten Scannen von Kraftahrzeugen in den von Fahrverboten betroffenen Gebieten voraus. Dies wird mit massenhaften Eingriffen in das Grundrecht der informationellen Selbstbestimmung bei einer Vielzahl von betroffenen Bürgerinnen und Bürgern einhergehen. Denn nur bei einer unverzüglichen und rückstandslosen Löschung im Nichttrefferfall entfällt nach der Rechtsprechung des Bundesverfassungsgerichts zum automatisierten Kfz-Scanning ein solcher grundrechtlicher Eingriff. Das mag bei dem automatischen Abgleich mit dem Zentralen Fahrzeugregister für entsprechend zugelassene Kfz umzusetzen sein. Für die Personengruppe, die aus anderen Gründen von der Durchfahrtsbeschränkung ausgenommen werden, gilt dies hingegen nicht. Ausdrücklich erlaubt der Gesetzentwurf eine Speicherung der Daten bis zu sechs Monaten, soweit sich nicht klären lässt, ob die Befahrung im konkreten Fall rechtmäßig erfolgte. Eine massenhafte Speicherung von Ausnahmen wäre zu befürchten. Die hier vorgesehene Speicherfrist überschreitet im Übrigen die dreimonatige Verjährungsfrist für OWi-Verfahren im Straßenverkehr.

Das Bundesverwaltungsgericht hatte in seinen beiden Diesel-Urteilen Anfang des Jahres 2018 darauf hingewiesen, dass Fahrverbote für Autobesitzer nicht unverhältnismäßig sein dürfen. Danach muss es Ausnahmen für davon betroffene Personengruppen geben. Das Gericht hat ausdrücklich bestimmte Anwohnergruppen und Handwerker genannt. In Hamburg etwa werden alle Anlieger von den Regelungen zur Durchfahrtsbeschränkung ausgenommen. Der hier geltende

Luftreinhalteplan beziffert diese Ausnahmen mit einem Umfang von immerhin 20% des betroffenen Verkehrsaufkommens. Darunter fallen etwa Anwohner sowie deren Besucher, Kunden und Beschäftigte von ansässigen Geschäften, Büros, Praxen oder Kanzleien, Krankenwagen, Müllautos, Handwerker sowie der gesamte Lieferverkehr innerhalb des betroffenen Straßenabschnitts. Die Befreiung für Anlieger gilt unmittelbar durch ein zusätzliches Verkehrszeichen und muss nicht gesondert beantragt werden.

All diese Personen und alle sonstigen Fahrzeugführer würden bei jeder einzelnen Durchfahrt vom Kamerasystem erfasst und – ergibt die Abfrage im Fahrzeugregister, dass sie kein Fahrzeug fahren, dessen Typenzulassung die Befahrung erlaubt – erst einmal gespeichert. Im weiteren Verlauf könnten dann OWi-Verfahren eingeleitet werden, in deren Verlauf sich die Betroffenen auf eine Anliegerregelung berufen müssten.

Die geplante Regelung für erlaubte Durchfahrten bezieht sich nur auf Kfz-Typen, nicht aber auf das persönliche Anliegen der Fahrer. Dass die automatisierte Videoüberwachung massenhaft Verdachtsfälle gegenüber Personen, für die ein Durchfahrtsrecht besteht, produziert, ließe sich nur verhindern, wenn zusätzlich durch die Bundesländer zum direkten Abgleich Datenbanken geschaffen würden, die entsprechende Kfz-Kennzeichen mit den jeweiligen Befreiungstatbeständen enthalten. Spontane Besucher von Anwohnern oder kurzfristig bestellte Handwerker könnte diese Regelung aber kaum erreichen. Der bürokratische Aufwand einer zum Abgleich erforderlichen Anliegerkontrolldatei ist zudem immens und würde aus Datenschutzsicht noch weit über die bisher diskutierten Pläne hinausgehen. Ein staatliches Anmeldeverfahren für alle in Betracht kommenden Ausnahmen vom Patienten über den Handwerker bis hin zum Besucher ist mangels Erforderlichkeit und Angemessenheit abzulehnen und mit dem Grundsatz der Datensparsamkeit unvereinbar. Das System

des automatischen Diesel-Scannings zur Durchfahrtkontrolle führt erkennbar in eine unverhältnismäßige staatliche Überwachungs- und Kontrollspirale hinein und steuert damit verfassungsrechtlich direkt in eine Sackgasse.

Auch der Bundesrat hat die Problematik des Entwurfs erkannt und in seiner Sitzung am 14. Dezember 2018 erhebliche datenschutzrechtliche Bedenken geltend gemacht und den Gesetzentwurf abgelehnt.

10. Google Standortdaten

Google verschleiert das Ausmaß der Verarbeitung von Standortdaten und erhält so auf rechtlich sehr fragwürdiger Basis erhebliche Mengen dieser wirtschaftlich wertvollen Informationen.

Die Daten über den jeweiligen Standort eines mobilen Geräts sind von großer datenschutzrechtlicher Relevanz, da sie insbesondere über den Zeitverlauf hinweg ein umfassendes Bild über die Lebensgewohnheiten des Nutzers geben. Dementsprechend groß ist auch das Interesse an diesen Daten und die Möglichkeit ihrer kommerziellen Verwertung.

Die Betriebssysteme der gängigen Handys ermöglichen dem Nutzer die Kontrolle über die Erfassung und Verwendung von Standortdaten in den zentralen Einstellungen. Bei den von Google betriebenen Android-Systemen besteht (im Detail abhängig von der Version des Betriebssystems) grundsätzlich die Möglichkeit, die Lokalisierung komplett zu deaktivieren sowie unter verschiedenen Lokalisierungsmethoden auszuwählen. Hierfür kommen im Wesentlichen einerseits das eingebaute GPS-Modul (bzw. allgemein sog. GNSS-Dienste, also Dienste, die globale Navigationssatellitensysteme ver-

wenden) in Frage und andererseits sämtliche andere Sensoren und Signale, die zur Ortung benutzt werden können, wie etwa WLAN-Signale, die empfangen werden können, Informationen über Mobilfunkzellen und Beschleunigungssensoren.

Als weitere Option steht die Speicherung des Standortverlaufs zur Verfügung, mit der die Nutzer festlegen können, ob Google eine Historie der verschiedenen Standortbestimmungen festhält. Dies kann die Navigation vereinfachen oder zusätzliche Empfehlungen ermöglichen.

Diese umfassenden Konfigurationsmöglichkeiten erzeugen bei den Nutzern berechtigterweise den Eindruck, das Erheben und Sammeln von Lokalisierungsinformationen mit diesen Einstellungen abschließend kontrollieren zu können. Dem ist aber nicht so. Vielmehr existiert eine weitere Einstellmöglichkeit, die tief in den vielen Optionen des Google-Kontos verborgen ist, mit denen das Android-Gerät verbunden ist. Über ein solches Konto verfügen nahezu alle Android-Handys, da nur so dessen volle Funktionalität, insbesondere die Installation von Apps aus dem Google Playstore, verfügbar ist.

Die dort unter „Aktivitätseinstellungen“ verfügbare Option „Web- & App-Aktivitäten“ steuert u. a. ob Google bei bestimmten Aktivitäten den Standort speichert. Dies betrifft etwa die Benutzung des Kartendienstes von Google oder Suchanfragen über die Suchmaschine von Google. Die Einstellung ist standardmäßig aktiviert, und die Speicherung erfolgt auch wenn das Gerät offline ist.

Diese Situation ist für den Nutzer kaum zu durchschauen und insgesamt irreführend. Es bestehen daher berechtigte Zweifel an der Rechtmäßigkeit der Erhebung und Speicherung der entsprechenden Lokalisierungsdaten. Da alle Android-Nutzer in Europa in gleicher Weise betroffen sind, handelt es sich um einen Fall der grenzüberschreitenden Datenverarbeitung. Wir

haben daher diesen Fall über die in der DSGVO vorgesehenen Wege an die nach unserer Auffassung federführend zuständige Aufsichtsbehörde in Irland herangetragen. Diese hat die Übernahme aber mit dem Hinweis abgelehnt, dass eine solche Federführung aktuell nicht bestehe, da Google keine Hauptniederlassung in Europa habe (siehe auch III 6).

Die insofern unklare Situation über die Zuständigkeit der Datenschutzaufsichtsbehörden spielt Google in die Hände. Denn das rechtliche Risiko der Bearbeitung durch eine einzelne lokale Aufsichtsbehörde liegt klar bei dieser, einschließlich des Verlusts der Zuständigkeit, sobald eine federführende Behörde gefunden wurde.

Erfreulicherweise wurde mittlerweile von Verbraucherschutzorganisationen ein europaweit koordiniertes Verfahren in dieser Sache eröffnet (siehe *https://fil.forbrukerradet.no/wp-content/uploads/2018/11/complaint-google-27-november-2018-final.pdf*). Dies macht von der Möglichkeit des Art. 80 DSGVO Gebrauch, eine Beschwerde über eine Organisation an die jeweilige Datenschutzbehörde heranzutragen. Soweit uns bekannt, sind deutsche Verbraucherschutzorganisationen an dieser Aktion nicht beteiligt.

Kurz vor Redaktionsschluss hat Google angekündigt, dass vorausichtlich ab Ende Januar 2019 die Hauptniederlassung in Irland eingerichtet sein wird (dazu unter III 6).

11. Google Plus

Das soziale Netzwerk Google+ bot über Jahre die Möglichkeit, in erheblichem Umfang auf Nutzerdaten zuzugreifen. Dies wurde mittlerweile behoben.

Über das soziale Netzwerk „Google+“, das seit dem Jahr 2011 angeboten wird, wurde im Oktober 2018 bekannt, dass Anbieter von Apps auf Google+ über weitreichende Zugriffsrechte verfügten, die mehr Daten umfassten als durch die Einstellungen der Nutzer vorgegeben war.

Google hat den Fehler, der zu dieser Möglichkeit geführt hat, nach eigenen Angaben selbst entdeckt und im März 2018 behoben. Das Unternehmen geht davon aus, dass App-Anbieter von der Möglichkeit keinen Gebrauch gemacht haben, da sie ihnen nicht bekannt war. Nach Ansicht von Google sind daher auch keine Persönlichkeitsrechtsverletzungen eingetreten.

Das Unternehmen hat die Angelegenheit zum Anlass genommen, das Angebot des sozialen Netzwerks im Jahr 2019 für Individualnutzer zu beenden.

Wir haben die öffentlich zugänglichen Informationen zum Anlass genommen, mehr Details über die Natur, die Ausmaße und die Behebung des Fehlers bei Google+ zu prüfen und in diesem Zug Google zur Beantwortung eines Fragenkatalogs aufgefordert. Dies ist erfolgt und zeigt im Ergebnis, dass die Einschätzungen von Google, was einen konkreten unzulässigen Datenzugriff durch App-Anbieter angeht, grundsätzlich nachvollziehbar sind.

Eine gewisse Parallele zu dem Cambridge-Analytica-Fall bei Facebook (siehe IV 2) ist nicht zu übersehen. In beiden Fällen konnten App-Anbieter in großem Stil auf Nutzerdaten

zugreifen und diese dann für eigene Zwecke nutzen. Als glücklicher Umstand stellt sich bei Google+ heraus, dass dessen Attraktivität für App-Anbieter wie für Nutzer offenbar deutlich geringer ist als Facebook und somit tatsächliche unzulässige Übermittlungen ausgeblieben sind.

12. Data Breach bei der FIFA

Der Fußball-Weltverband unterliegt nun unserer Aufsicht, da er einen Unionsvertreter mit Sitz in Hamburg gewählt hat.

Während der laufenden Fußball-Weltmeisterschaft in Russland haben wir eine Datenpanne bei der FIFA untersucht. Hintergrund waren unberechtigte Zugriffe Dritter auf das Akkreditierungsportal des Turniers. Betroffen waren die Daten von rund 2.800 Personen, die sich als freiwillige Helfer angemeldet hatten. Wir haben darauf hingewirkt, dass sämtliche Betroffenen von der FIFA individuell auf verständliche Weise über den Missbrauch ihrer Daten informiert wurden. Eine Sanktionierung kam gemäß § 43 Abs. 4 BDSG aufgrund der ordnungsgemäßen Meldung nicht in Betracht.

Der Verband hatte den Fall bei uns angezeigt, weil sein Unionsvertreter in Hamburg sitzt. Auch Verantwortliche außerhalb der Europäischen Union haben die Anforderungen der DSGVO einzuhalten, wenn sie im Binnenmarkt Waren und Dienstleistungen anbieten. In dem Fall haben sie gemäß Art. 27 DSGVO einen Vertreter in der Union zu benennen, der die Erreichbarkeit für hiesige Betroffene und Behörden sicherstellt. Neben weiteren global agierenden Unternehmen hat auch der Fußball-Weltverband eine juristische Person als Vertreter benannt, die in Hamburg ihren Sitz hat. Es handelt sich um einen Anbieter, der sich darauf spezialisiert hat, als

Unionsvertreter für Drittlands-Unternehmen zu fungieren. Dabei nutzt er in Hamburg eine minimale Infrastruktur mit einer Postanschrift in einem hiesigen Gemeinschaftsbüro und ohne eigenes Personal, das regemäßig vor Ort ist. Eine solche im rechtlichen Graubereich angesiedelte Einrichtung ist nur dann ausreichend, wenn die Vertretung des Verantwortlichen tatsächlich sichergestellt ist. Solange – wie hier – die Kommunikation mit den aus der Schweiz agierenden Mitarbeitern des Vertreters reibungslos funktioniert und im Bedarfsfall Treffen in der Hamburger Bürogemeinschaft abgehalten werden, wird die Hamburger Niederlassung dem Zweck des Art. 27 DSGVO gerecht.

13. Private Fahndung im Einzelhandel

Die Veröffentlichung von Bildern vermeintlicher Diebe aus Videoüberwachungsanlagen in Schaufenstern von Einzelhandelsgeschäften ist datenschutzrechtlich nicht zulässig.

Durch zwei Beschwerden von Bürgerinnen wurden wir auf ein Einzelhandelsunternehmen aufmerksam, das in den Schaufenstern seiner Geschäfte „Fahndungsfotos" von Personen aushängte, die in den Geschäften Diebstähle begangen haben sollen. Die vermeintlichen Diebinnen und Diebe wurden im Geschäft von Videoüberwachungskameras gefilmt. Aus diesem Videomaterial wurden Einzelbilder erstellt und – mit der Überschrift „Wanted" versehen – in den Schaufenstern ausgehängt.

Der Geschäftsführer des Unternehmens teilte uns mit, dass man häufig Opfer von professionellen Diebesbanden sei und es jährlich Inventurdifferenzen im sechsstelligen Bereich gegeben habe. Nach seinem Eindruck seien die Anzahl der Diebstähle nach dem Aushängen der Fotos zurückgegangen und hätten insofern eine abschreckende Wirkung.

Gegen eine Videoüberwachung der Verkaufsflächen von Einzelhandelsgeschäften bestehen keine grundlegenden datenschutzrechtlichen Bedenken, wenn es, wie in diesem Fall, in der Vergangenheit immer wieder Diebstähle gab, die zu hohen Inventurdifferenzen führten und deshalb auch in Zukunft mit Diebstählen zu rechnen ist. Die Bilder von möglichen Täterinnen und Täter dürfen auch an die für die Strafverfolgung zuständigen Behörden weitergegeben werden.

Fotos der vermeintlichen Täterinnen und Täter in den Schaufenstern der Geschäfte auszuhängen ist nach unserer Auffassung weder erforderlich noch angemessen. Weder das Bundesdatenschutzgesetz, noch die Datenschutzgrundverordnung oder das Kunsturhebergesetz erlauben eine solche private Öffentlichkeitsfahndung. Es ist nicht die Aufgabe privater Unternehmen, Straftaten zu verfolgen. Dies obliegt allein den Sicherheitsbehörden, die unter den engen Voraussetzungen der Vorschriften der Strafprozessordnung eine Öffentlichkeitsfahndung durchführen dürfen. Eine abschreckende Wirkung kann eine Videoüberwachung auch dann entfalten, wenn die ohnehin bestehenden Informationspflichten durch deutlich sichtbare Schilder im Eingangsbereich des Geschäfts und im Geschäft selbst umgesetzt werden. Der Aushang von Fotos der vermeintlichen Täterinnen und Täter ist zur Erzielung eines abschreckenden Effekts nicht erforderlich.

Ferner sind die Risiken einer solchen Selbstjustiz nicht unerheblich. Einzelhändler können sich bei der Beurteilung einer Situation irren. Personen könnten in der Folge fälschlich des Diebstahls verdächtigt und im Schaufenster angeprangert werden. Zudem ist die Qualität der Aufnahmen in vielen Fällen so mangelhaft, dass Verwechslungen mit völlig unbeteiligten Personen nicht ausgeschlossen werden können.

Das Gefühl der Hilflosigkeit gegenüber professionellen Diebesbanden hatte den Geschäftsführer wohl zu diesem

ungewöhnlichen Vorgehen bewogen. Er hat die „Fahndungsfotos“ unmittelbar nach unserer Kontaktaufnahme aus den Schaufenstern entfernen lassen. Diese umgehende Reaktion des Geschäftsführers werden wir bei der Entscheidung über die Abhilfebefugnisse, von denen wir in diesem Fall Gebrauch machen werden, mildernd berücksichtigen.

BERICHTE III.

1. „Informationsportal Neutrale Schulen Hamburg“ der AfD

Das „Neutralitätsportal“ der AfD-Fraktion mit dem zur Meldung übermäßig AfD-kritischer Lehrer an Hamburger Schulen aufgerufen wird, unterliegt als parlamentarische Handlung nicht unserer Kontrollzuständigkeit. Der Fall zeigt die Problematik einer lückenhaften Datenschutzgesetzgebung.

Die Fraktion der AfD in der Hamburgischen Bürgerschaft hatte in Hamburg ein Portal eingerichtet, über das Jedermann „Ideologieprogramme“ an Hamburger Schulen an die AfD melden konnte, die zu einer AfD-kritischen „Indoktrination“ von Schülerinnen und Schülern führen sollten. Das Portal sorgte deutschlandweit für Aufsehen und führte zu Nachahmern in anderen Bundesländern sowie zahlreichen Beschwerden bei uns. Lehrerinnen und Lehrer, Schülerinnen und Schüler sowie deren Angehörige waren besorgt, dass dies zu einer Bespitzelung und zu datenschutzrechtlich fragwürdigen Datenverarbeitungen der gemeldeten Lehrerinnen und Lehrer führe.

Leider findet die DSGVO hier keine Anwendung. Die Datenschutzgrundverordnung kann das Datenschutzrecht nur soweit regeln wie eine Kompetenz der Union besteht, was für Parlamente nicht der Fall ist. Tätigkeiten der Abgeordneten und der Fraktionen, die auf die parlamentarisch-politische Willensbildung des Parlaments bezogen sind, unterliegen daher nicht der DSGVO und damit auch nicht unserer Aufsicht. Nach der herrschenden Meinung in der juristischen Literatur ist dies nicht auf die Kerntätigkeiten des Parlaments (also die Gesetzgebung und Regierungskontrolle) beschränkt, sondern umfasst auch die Entwicklung und Umsetzung eigener Standpunkte, Initiativen und Konzepte, sowie die Öffentlichkeitsarbeit der Abgeordneten und Fraktionen.

Als „parlamentarische Arbeit" findet auf das Neutralitätsportal der AfD lediglich die Datenschutzordnung der Bürgerschaft Anwendung. Diese bietet Betroffenen nicht die gleichen Rechte wie die DSGVO. Ferner unterliegen die Fraktionen nicht der Datenschutzordnung der Bürgerschaft, die sich die Bürgerschaft selbst gegeben hat. Soweit Fraktionen betroffen sind, überwachen diese die von Ihnen selbst durchgeführte Datenverarbeitung in eigener Verantwortung. Dies bedeutet nicht, dass die Fraktionen hier frei nach ihrem Belieben vorgehen können. So bestehen ein datenschutzrechtlicher Auskunftsanspruch gegenüber der Fraktion sowie ein Anspruch der Betroffenen auf Löschung der Daten nach Maßgabe der Bürgerschaftlichen Datenschutzordnung. Die Betroffenen sind jedoch darauf angewiesen, ohne Unterstützung durch eine datenschutzrechtliche Beschwerdeinstanz ihre Rechte selbst gegenüber den Verantwortlichen gerichtlich durchzusetzen. Wollen Betroffene weitere Datenschutzrechte, insbesondere Informations- oder Widerspruchsrechte, geltend machen, wie sie die DSGVO vorsieht, könnten sich diese direkt aus ihrem Grundrecht auf informationelle Selbstbestimmung ergeben.

Der vorliegende Fall zeigt, dass die datenschutzrechtliche Sonderstellung den Schutz von Betroffenenrechten erschwert. Die Regelungen sollen an sich die Unabhängigkeit der Parlamente und insbesondere der Fraktionen in datenschutzrechtlicher Hinsicht gewährleisten und die parlamentarische Tätigkeit von einer externen aufsichtsbehördlichen Kontrolle freistellen, gleichzeitig aber auch dem Datenschutz Rechnung tragen. Dies kann gerade im politischen Wettbewerb nur funktionieren, wenn eine maßvolle und eigenverantwortliche Wahrnehmung der mit diesen Ausnahmebestimmungen verbundenen Befugnisse durch die Fraktionen erfolgt, die die datenschutzrechtlichen Rechte und Freiheiten von Bürgerinnen und Bürgern achtet.

2. dSmartDesk und datWLAN – Kommunikation der Senatskanzlei mit dem HmbBfDI muss besser werden

Die unzureichende Dokumentation von technischen und organisatorischen Maßnahmen führt zu einem erhöhten Risiko für Schwachstellen im Sicherheitskonzept der FHH.

Für Zugriffe von mobilen Geräten auf die Outlook-Exchange Installation nutzt die FHH seit 2012 die mobile Business Plattform „DME-Exciter". Seit Januar 2017 ist die FHH bemüht diese durch eine neue Lösung zu ersetzen. Der DME (Dynamic Mobile Exchange) Container hat immer wieder zu Schwierigkeiten auf mobilen Geräten geführt und soll durch eine möglichst integrierte Plattform ersetzt werden. Dieses Projekt ist Anfang 2017 unter den Namen „MobileWorkplace" gestartet und heißt seit Juli 2018 „dSmartDesk".

Schon die Einführung des DME-Containers wurde kritisch seitens des HmbBfDI sowohl an inhaltlichen Entscheidungen als auch am Verfahren selbst begleitet. Drei der Hauptkritiken, die im 25. Tätigkeitsbericht des HmbBfDI festgehalten sind (vgl. 25. TB, VI 1.3), waren das Fehlen eines restriktiven Mobile Device Managements, eine mangelhafte Dokumentation des Verfahrens und die sehr spärliche Kommunikation der damals zuständigen Finanzbehörde mit dem HmbBfDI. So wurde der HmbBfDI an mehreren Schritten des Verfahrens nicht beteiligt und konnte sich daher nicht in der notwendigen Tiefe einbringen.

Die Einführung von dSmartDesk ist bisher von neuen technischen und organisatorischen Problemen begleitet. Leider scheinen sich die Kommunikationsschwierigkeiten mit dem HmbBfDI zu wiederholen.

Projektziel von dSmartDesk ist die Schaffung einer Infrastruktur für sogenanntes ultramobiles Arbeiten in der FHH auf einer iOS-Plattform der Firma Apple. Durch ein zentrales Management aller beteiligten Geräte, das diese Plattform herstellerseitig unterstützt, ist es der FHH möglich, ultramobile Endgeräte in die BASIS-Infrastruktur einzubringen und auf diesen eine strikte Trennung zwischen dienstlichen und anderen Inhalten zu erzwingen.
Der HmbBfDI begrüßt ausdrücklich die Schaffung einer integrierten, zentral verwalteten Plattform auf Basis von iOS. Der im Vergleich zu den meisten Android Geräten deutlich längere Supportzeitraum und die strikte Isolierung einzelner Apps auf iOS-Geräten sowie die tiefe Integration einer zentralen Managementinfrastruktur in iOS bieten eine gute Grundlage für ein wirtschaftlich sinnvolles und sicheres Mobile-Exchange Verfahren, wenn der Verantwortliche dies entsprechend konfiguriert.

Obwohl sich dSmartDesk bereits in der erweiterten Pilotierung und damit im Echtbetrieb befindet, liegt noch keine vollständige Dokumentation vor. Ohne eine vollständige Dokumentation erfüllt der Verantwortliche die in Art. 5 Abs. 2 DSGVO festgeschriebene Rechenschaftspflicht nicht. Insbesondere zum Managementkonzept von iOS und der angestrebten strikten Trennung von dienstlichen und privaten Daten hat der HmbBfDI noch keine Informationen. Ohne eine vollständige Dokumentation darf ein Verfahren nicht in den Echtbetrieb gebracht werden.

Im Falle von dSmartDesk kommt zum Tragen, dass einige rechtliche Rahmenbedingungen ungeklärt sind. So widersprechen sich die Endgeräterichtlinie der FHH und die vorgelegten Nutzungsanweisungen für dSmartDesk z. B. in Fragen der Installation „privater" Software (Apps) auf dienstlich zur Verfügung gestellten Geräten und es fehlt gänzlich am notwendigen Vertragswerk mit der Firma Apple, um das erklärte

Ziel der gleichzeitigen Nutzung dienstlicher und privater Daten auf demselben Gerät zu ermöglichen. Auch enthalten die Nutzungsanweisungen einige Punkte, deren Rechtmäßigkeit ungeklärt ist; an anderen wird unnötig die Verantwortung für Datenschutz- und Sicherheitsfragen auf die Anwenderinnen und Anwender übertragen, anstatt zentrale Vorgaben zu erzwingen.

In diesen Fragen stehen der HmbBfDI und die Senatskanzlei im Austausch, dennoch werden wir immer wieder über Änderungen am Verfahren nicht oder zu spät informiert oder erst auf Nachfrage in neue Verfahrensschritte eingebunden.

In einer ähnlichen Situation befindet sich das FHH Projekt „datWLAN" mit dem Ziel, in behördlicher Infrastruktur ein offenes WLAN für die freie Nutzung zur Verfügung zu stellen. Auch hier war der HmbBfDI ursprünglich in das Verfahren eingebunden und an der Abnahme der Dokumentation beteiligt. Noch während der Erstellung dieser Dokumentation wurde „datWLAN" jedoch sehr plötzlich in Echtbetrieb genommen. Mehrfache Anfragen unsererseits an die Senatskanzlei mit der Bitte um Übermittlung einer vollständigen Dokumentation bleiben seit Mitte August 2018 unbeantwortet. Stattdessen erhalten wir vertröstende Antworten zurück und ein Vierteljahr nach Inbetriebnahme von „datWLAN" liegt immer noch keine gesetzlich vorgeschriebene vollständige Dokumentation vor.

Der HmbBfDI bekräftigt immer wieder seine Bereitschaft und seinen Willen, sich in neuen Projekten der FHH beratend einzubringen, insbesondere auch bei Projekten mit behördenübergreifenden Auswirkungen. Die derzeitige Kommunikationskultur und die Vorgehensweise bei der Inbetriebnahme neuer Verfahren bei der Senatskanzlei ist eindeutig verbesserungswürdig. Es fehlt die Bereitschaft, qualitätssichernde und vorgeschriebene Verfahrensschritte einzuhalten wenn sie der schnellen Veröffentlichung neuer Funktionen im Wege stehen.

Durch mangelnde oder unzureichende Dokumentation entsteht unnötigerweise ein erhöhtes Risiko für Schwachstellen im Sicherheitskonzept der FHH.

3. Email-Verschlüsselung zwischen Jugendamt und externen Stellen

Um die bisher unverschlüsselt stattfindende Kommunikation zwischen Jugendämtern und externen Stellen sicherer zu gestaltet, wird die FHH demnächst eine Multikanal-Kommunikationsplattform einsetzen.

Im vergangenen Tätigkeitsbericht berichteten wir über die Prüfung beim Allgemeinen Sozialen Dienst (ASD). Hierbei wurde festgestellt, dass der ASD unverschlüsselt mit externen Stellen kommuniziert. Unverschlüsselte Mails sind insbesondere deshalb keine gangbare Lösung zur Kommunikation im Sozialbereich, da nach §78a SGB X jede datenverarbeitende Sozialleistungsstelle verpflichtet ist, technische Maßnahmen zu treffen, die den Datenschutz sicherstellen. Die personenbezogenen Sozialdaten betroffener Kinder und Jugendlicher sind grundsätzlich einem hohem Schutzbedarf zuzuordnen. Zum Schutze derart sensibler Informationen ist eine Ende-zu-Ende-Verschlüsselung erforderlich (vgl. 26. TB, II. 6).

Die zuständige Behörde für Arbeit, Soziales, Familie, Integration (BASFI) hat zwischenzeitlich mit der Senatskanzlei der FHH an einer Lösung zur sicheren Kommunikation gearbeitet und sich konkrete Angebote vorlegen lassen. Hierzu gab es Anfang des Jahres ein Treffen von Mitarbeitern der Senatskanzlei (SK) als zuständige Behörde für die IT-Infrastruktur der FHH, der BASFI und des HmbBfDI, währenddessen unterschiedliche Ansätze abgewogen wurden. Es wurde sich schließlich auf eine Lösung verständigt.

Der aktuelle Stand Ende 2018 sieht vor, eine Multikanal-Kommunikationsplattform zu betreiben, die die gängigen Nachrichten-Transportkanäle der öffentlichen Verwaltung verarbeiten kann und mit verschlüsselten Nachrichten arbeitet. Die BASFI und die SK haben sich auf den Betrieb des Governikus MultiMessenger (GMM) verständigt, der u.a. De-Mail und PGP-verschlüsselte Mails unterstützt und diese im Intranet der FHH verteilt.
Die SK stellt bereits das für den Betrieb notwendige virtuelle Postfach für den GMM bereit und wartet auf Mitteilungen der BASFI, welcher Personenkreis freigeschaltet werden soll. Die BASFI sieht hierbei Hürden bei der Nutzung des Hamburg-Gateways, da dieses im Verlauf des Jahres 2019 durch das sogenannte Service-Konto abgelöst wird und somit nach Aussage der BASFI eine erneute Registrierung notwendig werden würde. Diesem Standpunkt können wir uns nicht anschließen.

Es obliegt nun zum einen dem ASD, an die Eltern und die freien Träger der Jugendhilfe heranzutreten und sie auf die neuen Kontaktwege aufmerksam zu machen sowie bei der Umstellung des bisherigen Kommunikationsweges zu unterstützen. So können entweder De-Mail-Postfächer angelegt werden oder auch virtuelle Postfächer im Hamburg Service Gateway beantragt werden; die sogenannte Elektronische Poststelle.

Nach Aussagen der SK und BASFI besteht aktuell noch Bedarf nach nutzerfreundlicher Dokumentation zur Einrichtung und zum Betrieb, um sämtliche Beteiligte bei der veränderten Nutzungsweise zu unterstützen. Hier wird Dataport gemeinsam mit der SK eine bebilderte Anleitung erstellen.

Ein Nachteil, der auch von Seiten des HmbBfDI angesprochen worden ist, liegt in der Funktionsweise des GMM, so ist für den Übergang der Nachrichten aus dem Internet ins Intranet (und umgekehrt) sowie die Prüfung von Nachrichten auf Viren

eine Entschlüsselung der Inhaltsdaten notwendig. Dadurch ist ausdrücklich keine echte Ende-zu-Ende-Verschlüsselung gewährleistet, denn die Mails liegen so für den Zeitraum der Verarbeitung im GMM unverschlüsselt vor. So wäre es bspw. Administratoren des GMM möglich, auf die Inhaltsdaten der Mails zuzugreifen. Der HmbBfDI sieht hier das potentielle Risiko der Verletzung der Schutzziele Integrität und Vertraulichkeit; geht aber zugleich von einer Verbesserung des aktuellen Status aus, da das Missbrauchspotential somit verringert und auf den GMM begrenzt wird.

Zudem haben wir die BASFI darauf hingewiesen, dass für die Nutzung über die browserbasierte Elektronische Poststelle eine 2-Faktor-Authentisierung notwendig sein wird, da es sich unzweifelhaft um Daten mit hohem Schutzbedarf handelt. Da die BASFI auf Nachfrage betont, den Weg über die Elektronische Poststelle lediglich als „kostengünstige und weniger aufwendige Alternative" zu nutzen, sofern „externe Teilnehmer noch nicht über Zertifikate verfügen", gehen wir davon aus, dass weiterhin die erstgenannte Lösung bevorzugt werden wird.

Im Unterausschuss Datenschutz im Dezember 2018 wurde die aktuellste Entwicklung nochmals dargestellt. Die BASFI wird neben Workshops zu dem Thema auch einen Pilotbetrieb im Januar 2019 durchführen.

4. Internet am Arbeitsplatz

Die Arbeitsplätze der FHH sollen 2019 einen sicheren Zugang zum Internet erhalten.

Die Stadt Hamburg betreibt seit mehreren Jahren eine Windows-Terminalserver-Farm für Arbeitsplätze mit hohem Schutzbedarf. Diese Geräte haben keinen direkten Zugang zum Internet, sondern nutzen für den Internetzugang den vom Terminalserver bereitgestellten Internet Explorer aus der Ferne, sodass Schäden durch Malware aus dem Internet auf dem jeweiligen Terminalserver gekapselt sind und sich nicht auf die Arbeitsplätze der Mitarbeiterinnen und Mitarbeiter ausbreiten.

Terminalserver sind eine Technologie aus den Frühzeiten vernetzter Computer und bringen in der alltäglichen Nutzung einige Nachteile mit sich. Darüber hinaus skaliert dieser Ansatz sehr schlecht mit der Anzahl seiner Nutzerinnen und Nutzer, hat generelle Performanceprobleme und sehr hohe Kosten für die Stadt. Daher gibt es seit einigen Jahren Bestrebungen innerhalb der FHH, diese Lösung durch ein flexibleres, moderneres Produkt zu ersetzen, das möglichst viele der Nachteile eines Terminalservers eliminiert und trotzdem ein vergleichbares Sicherheitsniveau bietet. Diese Bestrebungen sind im Jahr 2018 unter der aktiven Mitwirkung des HmbBfDI endlich konkret geworden und münden derzeit in einer Ausschreibung für ein neues Webbrowser-Produkt.

Dieser Ausschreibung ging ein ca. einjähriges Bedarfs–feststellungsverfahren voraus, in dem die vom HmbBfDI vorgeschlagenen Produkte getestet und daraus eine Liste erforderlicher Features erstellt wurde. Hierbei haben die Senatskanzlei, Dataport und der HmbBfDI gemeinsam daran gearbeitet, einen Katalog von Sicherheits- und Datenschutz-

anforderungen zu erarbeiten, der der derzeit stattfindenden Ausschreibung als Grundlage dient.

Nach Ablauf dieser Ausschreibung Anfang 2019 kann mit dem Aufbau einer Infrastruktur begonnen werden, sodass die bisherige Terminalserverinfrastruktur in naher Zukunft zugunsten der neuen Lösung schrittweise abgebaut werden kann.

Der HmbBfDI will sich weiterhin in diesem Projekt einbringen und fordert unter anderem mit der Inbetriebnahme dieser Infrastruktur auch die stadtweite Nutzung von Werbeblockern, um das Risiko einer Spy- oder Malware-Infektion weiter zu reduzieren und durch Einsparung von Bandbreite und Bildschirmfläche der gesamten städtischen Verwaltung eine schnellere und produktivere Internetnutzung zu ermöglichen.

5. Google Suchmaschine (Recht auf Vergessenwerden)

Der HmbBfDI berät und prüft als zuständige Aufsichtsbehörde in Deutschland bei Beschwerden in Fällen, in denen es die Google LLC abgelehnt hat, Suchergebnisse zu entfernen bzw. zu blockieren, die bei Eingabe der Namen von Betroffenen in der Internetsuchmaschine des Unternehmens angezeigt werden.

Widersprüche von Betroffenen gegen Suchergebnisse zu deren Namen prüft auch nach den Vorgaben der DSGVO zunächst die Google LLC als für die Datenverarbeitung verantwortliche Stelle. Das seit Mai 2014 öffentlich zugängliche Online-Formular zur Beantragung der Sperrung von Suchergebnissen ist unter der URL *https://www.google.com/webmasters/tools/legal-removal-request* abrufbar.

Vom 28.05.2014 bis zum 05.11.2018 wurden in Deutschland zu 468.125 URLs Ersuchen an die Google LLC gestellt, von denen 48% entfernt bzw. 52% nicht entfernt wurden (in Europa insgesamt wurden 44% von 2.831.775 URLs entfernt bzw. 56% nicht entfernt). Die meisten Ersuchen wurden in Frankreich zu 566.724 URLs gestellt, von denen 49,1% entfernt bzw. 50,9% nicht entfernt wurden. Nach Frankreich wurden in Deutschland die meisten Ersuchen gestellt. In den anderen europäischen Ländern wurden deutlich weniger Ersuchen gestellt (vgl. Großbritannien: 380.485 URLs oder Spanien: 229.839 URLs). Der aktuelle Transparenzbericht des Unternehmens ist unter der URL https://transparencyreport.google.com/eu-privacy/overview?hl=de einsehbar. Wir haben weiterhin und insbesondere seit Anwendbarkeit der DSGVO Ende Mai 2018 fortlaufend viele Eingänge von Eingaben und Beschwerden (2018: mehr als 300). Dadurch und aufgrund der zu geringen personellen Ausstattung bestehen leider erhebliche Wartezeiten für die Betroffenen.

Auch bei Anwendbarkeit der DSGVO seit dem 25.05.2018 ist der HmbBfDI in Deutschland als Aufsichtsbehörde weiterhin dafür zuständig, sich mit bei ihm eingereichten Beschwerden wegen Google Suchergebnissen zu befassen, wenn deren Gegenstand betroffene Personen nur aus Deutschland erheblich beeinträchtigt.

Bei der Prüfung von Beschwerden in Fällen, in denen die Google LLC Widersprüche gegen Suchergebnisse abgelehnt hat, hören wir das Unternehmen an, wenn unsere Prüfungen und Abwägungen ergeben, dass die Voraussetzungen zur Entfernung von Suchergebnissen vorliegen. In diesen Fällen werden nach erneuter Prüfung durch das Unternehmen häufig Suchergebnisse blockiert. Wird dies abgelehnt, prüfen wir, unter Berücksichtigung der Stellungnahme des Unternehmens weiter, ob die Voraussetzungen zur Entfernung von Suchergebnissen gegeben sind und eine Anordnung in Betracht kommt.

Wir sind weiterhin regelmäßig in Kontakt mit anderen deutschen und europäischen Datenschutzbehörden und den gemeinsamen europäischen Datenschutzgremien, insbesondere zu Fragen bei grenzüberschreitenden Fällen, Zuständigkeiten, inhaltlichen Prüfungen und Abwägungen zwischen dem Recht auf informationelle Selbstbestimmung mit dem öffentlichen Informationsinteresse und der Meinungsfreiheit.

Bei verschiedenen Fragen, die dem EuGH zur Vorabentscheidung aus Frankreich vorgelegt wurden, u.a. ob die Entfernung von Suchergebnissen wegen europäischem Datenschutzrecht weltweit zu erfolgen hat und zur Bedeutung besonderer Kategorien personenbezogener Daten, wie Informationen zur Gesundheit, politischen Meinungen und Straftaten, wurden bislang noch keine Entscheidungen veröffentlicht.

Das Verwaltungsgericht Hamburg hat im Jahr 2017 drei Klagen abgewiesen, in denen die Kläger begehrten, den HmbBfDI zu verpflichten, anzuordnen, dass Google Suchergebnisse entfernt werden. In einem Fall ist die Klage bereits rechtskräftig als unzulässig abgewiesen worden. Das Hamburgische Oberverwaltungsgericht wird voraussichtlich Anfang 2019 die beiden Fälle, in denen Berufungen eingelegt wurden, verhandeln. Der HmbBfDI ist der Ansicht, dass auch bei der nun anzuwendenden DSGVO beide Berufungen zurückzuweisen sind.

In dem Fall einer Verfassungsbeschwerde gegen eine zivilgerichtliche Entscheidung, die eine Klage der Beschwerdeführerin gegen einen Internet-Suchmaschinenanbieter auf Unterlassung der Anzeige eines bestimmten Treffers bei Eingabe ihres Namens abwies (1 BvR 276/17, „Recht auf Vergessen II“), hat der HmbBfDI auf Anforderung des Bundesverfassungsgerichts Anfang des Jahres 2018 eine Stellungnahme abgegeben. Zudem ist eine Verfassungsbeschwerde gegen zivilgerichtliche Entscheidungen anhängig, die die Klage

des Beschwerdeführers gegen ein Nachrichtenmagazin auf Unterlassung der Berichterstattung über Jahrzehnte zurückliegende Straftaten des Beschwerdeführers, abwiesen („Recht auf Vergessen"). In diesem Fall hatten wir bereits im Jahr 2014 eine Stellungnahme abgegeben. Diese Verfahren sind auf der Internetseite des Gerichts angegeben (*https://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2018/vorausschau_2018_node.html*).

6. Google-Hauptniederlassung

Eine zentrale Datenschutzaufsicht für Google in Europa bestand bislang nicht.

Die Datenschutzgrundverordnung (DSGVO) sieht bei Verantwortlichen, die in mehreren europäischen Ländern tätig und niedergelassen sind, regelmäßig die Bestimmung einer Hauptniederlassung vor (Art. 4 Nr. 16 DSGVO). Welche dies im Einzelfall ist, richtet sich nach bestimmten objektiven Kriterien. Als Rechtsfolge wird die Aufsichtsbehörde am Sitz der Hauptniederlassung bei grenzüberschreitender Verarbeitung federführend tätig.

Gerade bei großen Anbietern ist dieses One-Stop-Shop-Verfahren eine tragende Säule der DSGVO. Nicht nur erleichtert es ihnen die Einhaltung der datenschutzrechtlichen Anforderungen. Gleichzeitig sichert es auch einen einheitlichen Vollzug und eine Zentralisierung der Aufsicht im Rahmen der Kohärenzverfahren nach Kap. VII der DSGVO.

Unmittelbar vor der Anwendbarkeit der DSGVO im Mai 2018 hatte das Unternehmen gegenüber den europäischen Aufsichtsbehörden erklärt, dass beabsichtigt sei, in Irland eine europäische Hauptniederlassung – gegebenenfalls neben der

Verkaufsförderung auch hinsichtlich der Verantwortlichkeit für Online-Dienste bezogen auf Betroffene in Europa – einzurichten. Allerdings wurde dies später revidiert, da die dazu erforderlichen unternehmerischen Umstrukturierungen bislang nicht vollständig durchgeführt wurden.

Der Versuch, die Frage der Hauptniederlassung und federführenden Behörde für Google auf Ebene des Europäischen Datenschutzausschusses EDSA klärend zu entscheiden, war nicht erfolgreich. Verfahren, die wir in der Annahme der Federführung an die irische Datenschutzaufsicht herangetragen hatten, wurden von dieser an uns zurückverwiesen.

Dies bedeutet, dass die jeweils für eine einzelne Niederlassung zuständige Aufsichtsbehörde auch bei grenzüberschreitenden Fällen tätig wird, die Zuständigkeit jedoch zu dem Zeitpunkt, wo Google die erforderlichen unternehmerischen Umstrukturierungen schließlich vollzogen hat, wieder verliert. Diese Situation führt leider zu erheblicher Rechtsunsicherheit und im Ergebnis zu einer erkennbaren Zurückhaltung aufsichtsbehördlicher Tätigkeit bei einem der großen Anbieter in Europa.

Nun hat das Unternehmen angekündigt, dass bei Google Online-Diensten für Betroffene in Europa voraussichtlich ab Ende Januar 2019 in Irland eine Hauptniederlassung bestehen wird. Dies betrifft allerdings nicht die datenschutzrechtliche Verantwortlichkeit bei der Internetsuchmaschine Google bzw. den Index der Suchmaschine aufgrund von Dritten im Internet allgemein zugänglich gemachten Inhalten. Insoweit ist weiterhin das US Unternehmen Google LLC die verantwortliche Stelle, die über Mittel und Zwecke der Datenverarbeitungen entscheidet.

7. Facebook Custom Audience und Facebook SDK

Über Werkzeuge wie Custom Audience oder das Facebook SDK liefern Dritte oft Daten von Kunden oder Nutzern an Facebook aus, z.B. für zielgerichtete Werbung. Hierbei drohen Verstöße gegen die DSGVO.

Unter dem Namen „Custom Audience" offeriert Facebook Unternehmen und Werbekunden mehrere Optionen, um den Werbeerfolg bei Facebook zu steigern. Datenschutzrechtlich besonders kritisch ist das Angebot, E-Mail-Adressen oder Telefonnummern aus der eigenen Kundendatenbank zu Facebook hochzuladen, um mit Hilfe dieser Informationen die Werbung gezielt zu steuern, beispielsweise verstärkt Facebook-Mitglieder auf der Facebook-Plattform zu bewerben. Ebenso können gezielt nur solche Facebook-Mitglieder umworben werden, die bislang noch nicht Kunden des Unternehmens sind.
Im Rahmen des Uploads der Kundenliste gelangen zwangsläufig auch Daten von Personen an Facebook, die bislang – und ggf. auch bewusst – nicht Mitglieder des Netzwerks sind. Zwar werden die Daten für die Übermittlung durch Umwandlung in einen sog. „Hashwert" quasi verschlüsselt, da den Schlüssel dafür aber Facebook selbst vergibt, kann nicht von einer Unumkehrbarkeit und damit nicht von einer Anonymisierung ausgegangen werden.

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hatte daher einem bayerischen Online-Shop untersagt, das Angebot „Facebook Custom Audience über die Kundenliste" weiterhin einzusetzen, solange dieser von den Kunden keine Einwilligung einholt, was der Betreiber verweigerte. Die Unterlassungsanordnung wurde gerichtlich sowohl in der 1. Instanz als auch im Hauptsacheverfahren nunmehr in 2. Instanz vom Bayerischen Verwaltungsgerichtshof für rechtmäßig

befunden (VGH München, Urteil vom 26.09.2018). Auch wir sehen als zulässige Rechtsgrundlage für die Übermittlung von Kundendaten an Facebook im Rahmen eines Kundenlisten-Uploads regelmäßig nur die explizite Einwilligung an. Dies gilt für alle Kunden – Facebook-Mitglieder wie auch solche, die nicht bei Facebook registriert sind.

Facebook-Mitglieder können übrigens in den Kontoeinstellungen selbst einsehen, welche Unternehmen Kundenlisten mit ihren Daten an Facebook übermittelt haben. Eine Anleitung findet sich hier: *https://www.lda.bayern.de/media/pm2018_18_anhang.pdf*

Weiterhin ermöglicht Facebook Unternehmen das Einbinden eines sog. „Facebook Pixel" in das eigene Online-Angebot. Damit wird Facebook in die Lage versetzt, das Verhalten von Besuchern auf der Firmenwebseite oder im Online-Shop zu erfassen und auszuwerten. Hierbei können u. a. Facebook-Mitglieder unter den Besuchern identifiziert und somit auch außerhalb des Netzwerks beobachtet werden. Bei der Einbindung des „Facebook Pixel" sind dabei die gleichen Anforderungen umzusetzen, die auch für andere Tracking-Werkzeuge gelten. Unter anderem ist der Einsatz in der Datenschutzerklärung der Website offenzulegen.

Speziell an die Entwickler von Apps, Spielen oder Webanwendungen richtet sich das Angebot „Facebook SDK". Das Kürzel „SDK" steht dabei für die branchenübliche Bezeichnung „Software Development Kit" und umfasst ein Bündel von Werkzeugen, welche Entwicklern die Erstellung von Programmen erleichtern. Facebook ermöglicht u.a. den Einbau von Komponenten in Apps oder Spiele, über die Entwickler den Erfolg und die Nutzung ihres Produktes erfassen und messen können. Die Untersuchung einer englischen Datenschutzorganisation (abrufbar unter *https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report*)

dokumentiert, dass entsprechende Apps Nutzungsdaten an Facebook übermitteln, unabhängig davon, ob die App-Nutzer Facebook-Mitglieder sind und regelmäßig ohne deren Einwilligung. Durch die Integration derartiger Komponenten in ihre Apps sorgen Entwickler also dafür, dass Facebook Daten zufließen, die das Unternehmen dann für eigene Zwecke verwenden kann.

Wir werden die Themen Facebook Custom Audience und SDK in Zukunft verstärkt ins Visier nehmen. Die Verarbeitung oder Weitergabe von Daten ohne Rechtsgrundlage ist gemäß Art. 83 Abs. 5 DSGVO bußgeldbewährt.

8. Abhör-Verdacht bei Smartphone Apps

Im Laufe des vergangenen Jahres erhielten wir mehrere Eingaben von Personen, die sich von ihrem Smartphone im Alltag belauscht fühlen. Hintergrund ist oft Werbung, die auf dem Gerät angezeigt wird und einen direkten inhaltlichen Bezug auf ein zuvor geführtes Gespräch oder eine gesehene Fernsehsendung hat.

Moderne Smartphones zwingen Apps dazu, sich vor Zugriff auf das Mikrofon eine Genehmigung der Nutzerin einzuholen. Dies geschieht einmalig, meist bei Installation der App bzw. vor deren erstem Zugriff auf das Mikrofon und gilt ab dann, sofern diese Berechtigung nicht später wieder manuell entzogen wird.

Apps, die regulär aus den jeweiligen Stores der Anbieter installiert werden, sollten diese Einschränkung nicht umgehen können. Dennoch werden immer wieder Fälle bekannt, in denen das aufgezeichnete gesprochene Wort ohne das Wissen der Nutzerin an Server im Internet übertragen wird. Mittlerweile gibt es eine kleine Gruppe von Werbeanbietern, die – unter Nutzung der genannten Berechtigungen – in der Umgebung

der Nutzerin nach Werbespots im Fernsehen lauschen. Nach Angaben der Anbieter wird hierbei nur das Ziel verfolgt, konsumierte Inhalte z. B. auf dem Fernseher mit Werbeinhalten auf mobilen Plattformen zu kombinieren. Um sich derartigen und anderen Praktiken zu entziehen, empfiehlt der HmbBfDI generell die restriktive Vergabe und regelmäßige Durchsicht der erteilten Berechtigungen für installierte Apps.

Die von Betroffenen an uns herangetragenen Beschwerden sind meist detailreich und glaubhaft. Sie sind als anekdotische Einzelfälle jedoch kaum zu systematisieren, und ihre wahre Natur, ihr Umfang und die dahinterstehenden Verantwortlichen sind auch aus einer Vielzahl von Fällen schwer zu identifizieren. Auch die in jüngerer Vergangenheit vermehrte journalistische Befassung mit diesem Phänomen konnte hieran bislang nichts ändern. Um der gehäuften Menge an Anfragen gerecht werden und dem Phänomen auf den Grund gehen zu können, haben wir ein Projekt ins Leben gerufen, das sich mit der Frage der Audioüberwachung durch Smartphones beschäftigt.

Ausgehend von den bekannten Anbietern für sogenanntes „Ad retargeting“, also der Kombination verschiedener Medien in der Auslieferung personalisierter Werbung, wollen wir zunächst ein besseres Verständnis der Funktionsweise dieser Apps gewinnen. Dieses kann anschließend helfen, auch in anderen Apps entsprechendes Verhalten zu identifizieren. Neben der technischen Analyse wird hierbei auch die rechtliche Bewertung eine wichtige Rolle spielen.

Das Projekt befasst sich mit einer Reihe offener Fragestellungen rund um Geräte, die für viele von uns seit langem zum Begleiter auf Schritt und Tritt geworden sind. Welche Antworten wir erzielen und welche der Fragen sich letztlich überhaupt werden beantworten lassen, ist in der frühen Phase, in der das Projekt aktuell steht, noch nicht abzusehen.
Wir werden daher weiter über dieses Projekt berichten.

9. EuGH zu Facebook Fanpages – Nationales Datenschutzrecht doch auf Facebook anwendbar

Der EuGH bestätigt die langjährige Auffassung des HmbBfDI in seinem Urteil zu den Fanpages, dass das nationale Datenschutzrecht auf Facebook Anwendung findet, da Facebook eine Niederlassung in Hamburg hat.

Die Rechtsprechung des Europäischen Gerichtshofs (EuGH) zu Fanpages (Urteil vom 05. Juni 2018 - C 121/16, „Wirtschaftsakademie“) betrifft in der vom EuGH behandelten Sache die Rechtslage vor Inkrafttreten der DSGVO und bestätigt zunächst unsere langjährige Rechtsauffassung bezüglich der Anwendbarkeit des nationalen Rechts. Der HmbBfDI hatte eine Anordnung gegen Facebook wegen des Massenaustausches von Daten mit WhatsApp erlassen. Die hiergegen seitens Facebook eingelegten Rechtsbeschwerden wurden in zwei Instanzen im einstweiligen Rechtsschutzverfahren durch das VG Hamburg und das OVG Hamburg abgewiesen. In einem langjährigen Streit um die Anwendung des nationalen Rechts ist damit eine Entscheidung getroffen worden, die die Auffassung des HmbBfDI bestätigt. Ein Wermutstropfen ist jedoch, dass dieses Urteil zu einem Zeitpunkt erlassen wurde, als die nationalen Regelungen, die gegen Facebook in Ansatz gebracht werden konnten, gar nicht mehr bestanden, da nach der DSGVO die nunmehr federführende Zuständigkeit bei Irland liegt.

Gleichzeitig bestätigt das Urteil die langjährige Rechtsauffassung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, die auch der HmbBfDI stets teilte, dass Fanpage-Betreiber hinsichtlich der Datenverarbeitung mit Facebook eine gemeinsame Verantwortung verbindet, so

dass die Auffassung der Betreiber von Fanpages, für die Art und Weise der Datenverarbeitung durch Facebook keine eigene Verantwortung zu haben, rechtlich nicht zutreffend ist.

Im Nachgang zu dieser Entscheidung hat sich die Datenschutzkonferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder (DSK) zu der EuGH-Rechtsprechung in einem Beschluss und einer Entschließung positioniert (*https://www.datenschutzkonferenz-online.de/media/en/20180605_en_fb_fanpages.pdf, https://www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_facebook_fanpages.pdf*). Es gilt nun, unter den Aufsichtsbehörden abzustimmen, wie künftig mit Fanpages umzugehen ist. Hierzu haben manche Bundesländer bereits Fragebögen erstellt, die im Folgenden auszuwerten sind. Es ist damit zu rechnen, dass das Thema Fanpages weiterhin rechtlich auf der Agenda steht.

Parallel dazu wird diese Frage in der am 15. Mai 2018 neu eingesetzten Social Media Subgroup thematisiert, die sich als Fachuntergruppe des Europäischen Datenschutzausschusses (EDSA) – vormals die Artikel 29 Datenschutzgruppe – mit dem Themenkreis soziale Medien und ihre Auswirkungen auseinandersetzt und entsprechende Leitlinien, Stellungnahmen sowie bewährte Verfahren ausarbeitet. Der HmbBfDI nimmt als reguläres Mitglied an dieser Subgroup teil und stimmt die Ergebnisse mit den nationalen Behörden ab.

Das Mandat der Social Media Group erstreckt sich darüber hinaus auch auf die Analyse der bereits bestehenden oder sich erst entwickelnden Funktionen, die von sozialen Medien angeboten werden, einschließlich der Betrachtung der zugrundeliegenden Verarbeitungsvorgänge und den daraus resultierenden Risiken für Rechte und Freiheiten der betroffenen Personen.

In diesem Zusammenhang wurden auch die Rechtsprechung des EuGH sowie die Erfahrungen der Einflussnahme auf Wählermeinungen über soziale Medien im Rahmen dieser Subgroup zum Anlass genommen, das Thema Targeting der Nutzer sozialer Medien näher zu beleuchten. Ziel ist die Entwicklung von Leitlinien für einen rechtskonformen Einsatz der Funktionalitäten, die zu einer gezielten Ansprache der Nutzer in einem werblichen, aber auch politischen Kontext eingesetzt werden.

10. Nachhaltiges Webtracking – und immer noch keine ePrivacy-Verordnung in Sicht

Mehr Rechtssicherheit im Bereich der Telemedien würde durch die Anwendung der sich aktuell noch im Entwurfsstadium befindlichen ePrivacy-Verordnung – sowohl auf nationaler als auch auf internationaler Ebene – geschaffen werden.

Ursprünglich sollte gleichlaufend mit der Datenschutzgrundverordnung (DSGVO) auch die ePrivacy-Verordnung am 25. Mai 2018 Geltung erlangen. Die ePrivacy-Verordnung soll speziell im Bereich der elektronischen Kommunikation Regelungen zum Schutz personenbezogener Daten treffen und ginge somit grundsätzlich dem Anwendungsbereich der DSGVO vor. Bereits Anfang des Jahres war jedoch absehbar, dass sich das europäische Gesetzgebungsverfahren erheblich verzögern wird und mit einem Inkrafttreten der ePrivacy-Verordnung zum avisierten Zeitpunkt nicht mehr zu rechnen ist. Da mit Geltungserlangung der DSGVO das Telemediengesetz (TMG) als nationale Vorschrift zwar fortbesteht, aber dessen datenschutzrechtlichen Vorschriften des 4. Abschnitts nicht mehr anwendbar sind, haben die Aufsichtsbehörden am 26. April 2018 ein Positionspapier –

https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai 2018/Positionsbestimmung-TMG.pdf – Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 – beschlossen.

Hieraus geht unter anderem hervor, dass die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden können; es gilt die DSGVO direkt. Daher bedarf es einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Das bedeutet, dass eine informierte Einwilligung i. S. d. DSGVO, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, also beispielsweise bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

An der Positionsbestimmung wurde vorrangig von Vertretern der Wirtschaft sowie der Medien- und Verlagsbranche teils heftige Kritik geübt. So fordert die Positionsbestimmung, entgegen der bisher gelebten Praxis des sogenannten Opt-Out-Verfahrens, also eine Widerspruchslösung für das Verarbeiten personenbezogener Daten im Internet, nunmehr ein Opt-In-Verfahren, also eine vorherige informierte Einwilligung in die Verarbeitung personenbezogener Daten. Dies führe nach Ansicht der Medienvertreter u.a. zu erheblichen Einnahmeverlusten im Bereich der Werbefinanzierung und bedrohe so den Journalismus insgesamt.

Aufgrund der Tragweite der Positionsbestimmung hat die Datenschutzkonferenz ein Konsultationsverfahren eröffnet, in dem Verbände und Unternehmen schriftlich zur behördlichen Positionsbestimmung bis zum 29. Juni 2018 Stellung nehmen konnten. Im weiteren Verlauf schloss sich eine mündliche Konsultation an, die am 16. Oktober 2018 in Berlin stattgefunden hat. Im Rahmen des Konsultationsverfahrens konnte insbesondere zu der Frage, welche Verarbeitungstätigkeiten im Rahmen des Webtrackings einer Einwilligung bedürfen und welche auf eine Interessenabwägung gestützt werden können, kein Konsens gefunden werden.

Die Aufsichtsbehörden haben sich darauf verständigt, eine Konkretisierung der Positionsbestimmung in Form einer Orientierungshilfe zu verabschieden. Die in dem Positionspapier zum Ausdruck gebrachten Anforderungen sind bereits jetzt zu berücksichtigen. Dies gilt insbesondere vor dem Hintergrund, dass weiterhin offene Fragen in Bezug auf den Entwurf der ePrivacy-Verordnung unter den Mitgliedstaaten bestehen und somit eine Verabschiedung der Verordnung bis Mai 2019 immer unwahrscheinlicher wird.

11. Arbeitspapier Biometrische Analyse steht bald bereit

Die Unterarbeitsgruppe „Biometrische Analyse" veröffentlicht die erste Version eines abgestimmten Positionspapiers der Datenschutzbeauftragten von Bund und Länder und bietet somit eine Handreichung und klare Rahmenbedingungen zum Einsatz biometrischer Systeme.

Im Herbst 2017 konstituierte sich die Unterarbeitsgruppe (UAG) Biometrische Analyse der Datenschutz-Aufsichtsbehörden des Bundes und der Länder. Ziel der UAG ist die

Veröffentlichung eines Positionspapiers, das die aktuellen technischen Entwicklungen in Bereich der Biometrie rechtlich einordnet und Handlungsempfehlungen für Anwender solcher Systeme bereitstellt. Anlass zur Gründung dieser UAG waren Prüfungen aus den Häusern der Berliner Beauftragten für Datenschutz und Informationsfreiheit, des Bayerischen Landesamt für Datenschutzaufsicht und der Bundesbeauftragten für Datenschutz und Informationsfreiheit. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat den Arbeitskreis Technik und die Arbeitsgruppe Videoüberwachung mit dem Thema der Verarbeitung von biometrischen Daten durch Sensorik und Videotechnik beauftragt.

Wir sind in dieser Unterarbeitsarbeitsgruppe auf Fachebene vertreten und schreiben an dem Positionspapier mit. Zudem wurden Experten auf dem Gebiet in die Treffen der Arbeitsgruppe miteinbezogen, um das Papier an der Entwicklung in Forschung und Wirtschaft orientieren zu können. Die erste Version des Papiers umfasst biometrische Systeme, die auf Basis optischer Sensoren arbeiten.

Als Zwischenergebnis beinhaltet diese erste Version nun eine einführende Beschreibung der technischen Grundlagen solcher Systeme und eine Definition gängiger Begriffe im Kontext der Biometrie. Ein wesentlicher Abschnitt bildet die Darstellung der Sensoren und die darauf aufbauende Sammlung möglicher Einsatzszenarien, sogenannter „Use Cases“, die sich eng an den bisherigen Fragestellungen der Datenschutzbehörden zur Biometrie orientiert. So sind beispielsweise auch Ansätze thematisiert worden, die sich in den Bereich des Emotional Decoding einordnen lassen. Abschließend wird die rechtliche Bewertung zu allen beispielhaften Fällen dargestellt und als Schlussfolgerung eine Auswahl von Maßnahmen zur Verfahrensgestaltung aufgezeigt.

Das Ziel dieser ersten Version des Papiers ist die Herausgabe einer durch die Datenschutzbehörden des Bundes und der Länder abgestimmten deutschlandweit einheitlichen Beurteilungsrichtlinie bei biometrischen Systemen. Diese Handreichung zeigt Verantwortlichen klare Rahmenbedingungen zum Betrieb biometrischer Systeme auf.

Die UAG hat nun den Arbeitsauftrag, weitere Themenbereiche wie bspw. weitere Sensortypen interdisziplinär zu behandeln und wird mit fortschreitenden Versionen der Positionspapier noch umfassendere Darstellungen zu dem Themengebiet Biometrie bieten.

Grundsätzlich ist festzustellen, dass im vergangenen Jahr gehäuft sowohl Beschwerden als auch Anfragen von Unternehmen bei den Datenschutzbeauftragten von Bund und Länder eingingen. Der Einsatz biometrischer Systeme gewinnt zunehmend an Bedeutung in den Bereichen Wirtschaft, Sicherheit und Forschung. Dem muss sich auch der Datenschutz bewusst werden; nach unserer Ansicht ist die Arbeit der Unterarbeitsgruppe daher ein wichtiger Bestandteil zur Auseinandersetzung mit dieser Thematik, da somit auch Konsens zwischen den bisher unterschiedlichen Auffassungen der deutschen Aufsichtsbehörden hergestellt werden kann.

Bei Redaktionsschluss zu diesem Tätigkeitsbericht stand die erste Version des Positionspapiers kurz vor der Fertigstellung, sodass mit einer Veröffentlichung im ersten Quartal 2019 zu rechnen ist und dann auch von unserer Internetseite abgerufen werden kann. Die Fortschreibung des Papiers ist nun die weitere Aufgabe der Unterarbeitsgruppe.

RECHTSVERBINDLICHE ANORDNUNGEN UND BUSSGELDVERFAHREN IV.

1. Polizei: Gesichtserkennungssoftware/ Videmo

Der HmbBfDI hat gegenüber der Behörde für Inneres und Sport, als Aufsichtsbehörde der Polizei Hamburg, den Einsatz einer Gesichtserkennungssoftware durch die Polizei im Rahmen von strafrechtlicher Ermittlungstätigkeit zunächst beanstandet und dann konkret die Löschung der durch diese Software erstellten Datenbank angeordnet.

1.1 Gesichtserkennungssoftware „Videmo 360“

Der im Zuge der strafrechtlichen Aufarbeitung der Geschehnisse rund um den im Juni 2017 in Hamburg stattgefundenen G20-Gipfel ins Leben gerufenen Sonderkommission „Schwarzer Block“ der Polizei Hamburg liegen insgesamt 100 Terabyte Bild- und Videomaterial vor. Sie sollen laut Angaben der Polizei örtlich und zeitlich in Verbindungen zu strafrechtlich relevanten Geschehnissen im Zusammenhang mit dem G20-Gipfel stehen. Seit November 2017 verwendet diese Sonderkommission eine sog. Gesichtserkennungssoftware („Videmo 360“) zur Verarbeitung von zumindest Teilen dieses Materials. Mit Stand August wurden mit „Videmo 360“ ca. 17 Terabyte bzw. 30.000 Dateien, Tendenz steigend, verarbeitet. Davon stammen fast 10.000 Dateien von einem im Nachgang zum Gipfel von der Polizei bereitgestellten Hinweisportal, welches der Bevölkerung ermöglichte, Bild- und Videodateien mit „G20-Relevanz“ hochzuladen. Die übrigen Bild- und Videodateien setzten sich zusammen aus von der Polizei selbst hergestelltem Material, sowie aus Material von Überwachungskameras aus acht S-Bahnhöfen über mehrere Tage, den Medien und dem Internet. Während das Material aus dem öffentlichen Nahverkehr ohne vorherige Sichtung in die

Software eingespielt wurde, wurde das von Privatpersonen hochgeladene Material grob gesichtet. Aufnahmen, die ganz offensichtlich keine örtliche oder zeitliche Verbindung zum G20-Gipfel aufwiesen, wie Pornos oder Katzenvideos wurden gelöscht. Strafrechtlich relevantes Verhalten war ausdrücklich kein Kriterium für die Einführung in „Videmo 360".

Bei der durch „Videmo 360" durchgeführten Gesichtserkennung wurden zunächst menschliche Gesichter in Bild- sowie Videodateien lokalisiert. Sodann berechnet „Videmo 360" die charakteristischen Eigenschaften dieser menschlichen Gesichter (z. B. Augenabstände, Nasenform, Ohr-zu-Ohr-Abstand). Diese Merkmale des menschlichen Gesichts werden für jedes Gesicht in einer mathematischen Form in einer sog. Referenzdatenbank abgespeichert, den sog. Templates. Diese abgespeicherten Templates können dann in einem weiteren Schritt untereinander abgeglichen werden, was das Auffinden einer Person in sämtlichen zur Verfügung stehenden Dateien ermöglicht. So können der Aufenthaltsort, das Verhalten und soziale Kontakte einer Person über mehrere Tage auf großen Teilen des Hamburgischen Stadtgebietes rekonstruiert werden.

1.2 Maßnahmen durch den HmbBfDI

Die Polizei Hamburg geht davon aus, dass die unter 1.1. geschilderte Verarbeitung lediglich eine Hilfestellung bei der Durchsicht des Datenmaterials darstellt, also vergleichbar mit der optischen Nutzung durch einen menschlichen Beobachter sei. Daher sei ihr der Einsatz von „Videmo 360" im Rahmen von strafrechtlichen Ermittlungen auch ohne ausdrückliche Rechtsvorschrift erlaubt. Diese Bewertung wird von uns nicht geteilt. Nach umfangreicher Prüfung sind wir zu dem Ergebnis gelangt, dass die Verarbeitung von Abbildungen menschlicher

Gesichter zu biometrischen Gesichtsmodellen vielmehr einen erheblichen datenschutzrechtlichen Verstoß darstellt.

Dabei handelt es sich nämlich nicht um ein bloßes Hilfsmittel zur Sichtung des umfangreichen Materials, sondern um ein Instrument, das weitere Nutzungs- und Verknüpfungsmöglichkeiten von personenbezogenen Daten erlaubt, die ein gewöhnliches Lichtbild nicht vermag. Es werden maschinenlesbare Modelle von menschlichen Gesichtern in einer umfangreichen Datenbank festgehalten. Die größtenteils davon betroffenen Personen haben keinen Anlass dafür gesetzt. Deren Gesichter wurden durch „Videmo 360" nur verarbeitet, weil sie sich zufälligerweise an einem bestimmten Ort und Zeit aufgehalten haben (z.B. an einem S-Bahnsteig) und/oder weil eine andere Privatperson die Entscheidung getroffen hatte, ein Video hochzuladen.

Der Einsatz von „Videmo 360" greift wesentlich intensiver in das Grundrecht auf informationelle Selbstbestimmung ein, als die optische Nutzung von Bild- und Videomaterial es vermag. Es bedarf für deren Einsatz daher zunächst einer Rechtsvorschrift, die sowohl für die Polizei als Handelnde als auch für die Betroffenen Voraussetzungen und Ausmaß erkennbar regelt. An einer derartigen Rechtsgrundlage fehlt es jedoch im geltenden Recht. Der HmbBfDI hat der Polizei Hamburg im Juli 2018 zunächst das Ergebnis der datenschutzrechtlichen Prüfung mitgeteilt. Da aufgrund dieser Prüfung keine Abhilfe durch die Polizei erfolgte, wurde der Einsatz von „Videmo 360" im September 2018 von uns gegenüber der Behörde für Inneres und Sport offiziell beanstandet. Da die Behörde für Inneres und Sport trotz Beanstandung an dem Einsatz von „Videmo 360" ausdrücklich festhielt und sogar den weitergehenden Einsatz dieses Instruments auf künftige

öffentliche Ereignisse in Aussicht gestellt hat, wurde nun die Löschung der erstellten Templatereferenzdatenbank von uns angeordnet. Dies betrifft nur die durch den Einsatz der Software berechneten Gesichtsmerkmale, nicht aber die Gesamtheit der von der Polizei erhobenen Bild- und Videodateien. Der Senator der Behörde für Inneres und Sport kann hiergegen Klage vor dem Verwaltungsgericht Hamburg erheben. Die Klage hat aufschiebende Wirkung, so dass die Anordnung nicht vollziehbar wird.

2. Facebook und der Datenskandal rund um Cambrigde Analytica – Bußgeldverfahren wegen der Erhebung der Daten ohne Rechtsgrund

Facebook gewährte jahrelang App-Entwicklern tiefe Einblicke in die Daten seiner Nutzer – unserer Auffassung nach ohne Rechtsgrund. Dennoch musste das Bußgeldverfahren eingestellt werden.

Anfang 2018 überrollte der Skandal rund um Facebook und die Datenanalysefirma Cambridge Analytica nicht nur die politische Bühne in den USA und Großbritannien, sondern auch die Medienlandschaft weltweit. Aus zahlreichen Medienberichten wurde bekannt, dass Cambridge Analytica sich über eine App unrechtmäßig personenbezogene Daten von Millionen Facebook-Nutzern beschafft hat, um Wähler mit zielgerichteten Botschaften zu politischen Zwecken zu manipulieren.

Aufgrund dieser Medienberichte und der Annahme, dass auch deutsche Nutzer betroffen sein könnten, nahmen wir im März 2018 Ermittlungen zur Klärung des Sachverhalts auf und konfrontierten die Facebook Ireland Ltd. zunächst

mit einem umfassenden Fragekatalog, v. a. zu der Schnittstelle (sog. API), die bis April 2014 bzw. übergangsweise bis (mindestens) Ende April 2015 den App-Entwicklern offenbar umfassende Zugriffsmöglichkeiten zu Nutzerdaten auf Facebook gewährte. Der Anknüpfungspunkt der Ermittlungen war vorliegend nicht ausschließlich die App „thisisyourdigitallife", deren Entwickler die Daten später an Cambridge Analytica weitergab, sondern generell die technische und rechtliche Ausgestaltung der Schnittstelle für die App-Entwickler und nicht zuletzt die Frage, wie Facebook Daten seiner Nutzer vor Missbrauch durch Dritte schützt.

Die Facebook Ireland Ltd. schätzte in ihrer Antwort die Zahl der potentiell Betroffenen in Deutschland auf ca. 310.000 Personen. Die Einlassung zur Ausgestaltung der Schnittstelle sowie zur Rechtsgrundlage, die sie vor allem auf Einwilligung und berechtigte Interessen stützte, vermochte uns jedoch nicht zu überzeugen.

Infolge der Beantwortung der Fragen und wegen der drohenden Verjährung – die Verjährungsfrist beträgt gem. § 31 Abs. 2 Nr. 1 OwiG für Geldbußen mit Höchstmaß von über fünfzehntausend Euro drei Jahre, es konnte also nur noch der Zeitraum von wenigen Tagen geahndet werden – eröffneten wir ein Bußgeldverfahren gegen die Facebook Ireland Ltd. als verantwortliche Stelle für die Datenverarbeitung außerhalb Nordamerikas. Die verfahrensgegenständliche Login-Funktion in der Plattform Graph API V1 war bis zum 30.04.2014 bzw. übergangsweise (mindestens) bis zum 30.04.2015 für bereits bestehende Apps verfügbar. Diese Facebook-Login-Funktion ermöglichte den App-Entwicklern, Einwilligung von Nutzern einzuholen, um Zugang zu bestimmten Kategorien von Nutzer-Daten zu erhalten. Darüber hinaus hatten die App-Entwickler die Zugriffsmöglichkeit auf bestimmte Datenkategorien, die die App-Nutzer mit ihren Facebook-Freunden auf Facebook geteilt hatten. Auf diesem

Wege konnten die App-Entwickler neben den Daten der App-Nutzer selbst auch Daten deren Facebook-Freunde erhalten, sofern diese im Rahmen ihrer voreinstellten Privatsphäreneinstellungen diesen Zugriff nicht ausdrücklich ausgeschlossen hatten (sog. „Opt-out"). Die so erhobenen Daten konnte der Entwickler der App „thisisyourdigitallife" zwar vertragswidrig, jedoch ohne technische Hürden an Cambridge Analytica weiterverkaufen.

Das Bußgeldverfahren musste nach Anhörung der Facebook Ireland Ltd. aus rechtlichen und tatsächlichen Gründen nach § 170 Abs. 2 Satz 1 StPO i.V. m. § 46 Abs. 1 OWiG in Anbetracht des drohenden Prozessrisikos eingestellt werden. Zum einen war die ganz überwiegende Zahl der Fälle zum Zeitpunkt der Verfahrenseröffnung in April 2018 bereits verjährt und der Tatbestand der Übermittlung personenbezogener Daten gem. § 43 Abs. 2 Nr. 1 BDSG a.F. für den Zeitraum vom 20.05.2015 bis zum 30.05.2015 hätte nicht gerichtsfest bewiesen werden können. Zum anderen stellte der Nachweis des Vorsatzes ein weiteres tatsächliches Problem dar: Die hier noch zu betrachtende Übergangszeit für bestehende Apps war von der Irischen Datenschutzbehörde (Irish Data Protection Commission, kurz IDPC) aufsichtsrechtlich überprüft worden (Audit Report der IDPC: *https://www.dataprotection.ie/docs/Facebook-Ireland-Audit-Report-December-2011/1187.htm*). Somit waren die Absicht oder zumindest die Fahrlässigkeit bezüglich der unbefugten Übermittlung schwer nachweisbar. Erschwerend im Hinblick auf die Zuständigkeitsfragen kam das Urteil des Europäisches Gerichtshofs hinzu (EuGH), das nach der Verfahrenseröffnung im Juni (Urteil vom 05.06.2018 – C121/16) ergangen war. Demnach hätte der HmbBfDI nach den dort aufgestellten Grundsätzen zwar die Kompetenz gemäß BDSG a.F. sowie OWiG vorzugehen, unklar war jedoch, ob das Vorgehen gegen die in Irland ansässige Facebook Ireland Ltd. der gerichtlichen Überprüfung hätte Stand halten können, oder die Facebook GmbH in Hamburg

der richtige Adressat gewesen wäre, so dass eine Einstellung nicht zuletzt aufgrund der unklaren Zuständigkeitslage geboten erschien.

Doch auch nach der Einstellung des Bußgeldverfahrens in Deutschland wird der Datenschutzskandal weiter aufgeklärt. So hatte die britische Datenschutzaufsicht Information Commissioner´s Office (kurz ICO) aufgrund der örtlichen Zuständigkeit für die Firma Cambridge Analytica und ihre mutmaßlichen Verwicklungen in das Brexit-Referendum ein Bußgeldverfahren eingeleitet (*https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf*) und umfassende technische Analysen der Datenströme vorgenommen, bei der dutzende Ermittler eingesetzt worden sind. Die Ergebnisse sind auf der Homepage der ICO nachlesbar (*https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf*). Die ICO hat ein Bußgeld in Höhe von 500.000 £ verhängt, gegen die Facebook Rechtsmittel eingelegt hat. Das Verfahren und weitere Untersuchungen dauern noch an.

3. Dating-Portale – Umgang mit Auskunftsersuchen

Auskünfte ergehen durch die verantwortlichen Unternehmen mittlerweile schneller und bequemer.

Bereits im Vorjahr sind durch den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit vier Bußgeldverfahren wegen der verspäteten Erteilung von Auskunftsersuchen gegen prominente Anbieter von Dating-Portalen eingeleitet worden. Im Zuge der erlassenen Sanktionen wurden die Prozesse in den Unternehmen umgestellt, so dass

im Jahr 2018 bisher nur ein Bußgeldverfahren wegen einer verspäteten Auskunftserteilung sowie ein Verfahren wegen der Missachtung des Werbewiderspruchs eingeleitet werden musste.

Darüber hinaus erfolgen weitere Optimierungsprozesse innerhalb der Unternehmen mit Blick auf eine Vereinfachung der Geltendmachung von Auskunftsersuchen. Diese Vorgabe ergibt sich nicht zuletzt aus Art. 12 Abs. 1 S. 1 DSGVO, nach dem ein Unternehmen geeignete Maßnahmen zu treffen hat, um betroffenen Personen alle Mitteilungen nach Art. 15 DSGVO, die sich auf die Verarbeitung ihrer personenbezogenen Daten beziehen, in präziser, transparenter, verständlicher und vor allem leicht zugänglicher Form zu übermitteln. Die Anbieter von Dating-Plattformen sollten dabei entsprechend Erwägungsgrund 64 alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Fall von Online-Kennungen.

Vor diesem Hintergrund werden Auskunftsersuchen betroffener Personen zukünftig verstärkt in elektronischer Form durch einen leitenden und schnell verständlichen Prozess realisiert werden. Art. 12 Abs. 3 DSGVO weist zudem explizit auf eine Auskunftserteilung in elektronischer Form hin, von der der Betroffene nach seinem Willen allerdings abrücken und eine andere Form der Auskunft ausdrücklich verlangen kann. Ob das verantwortliche Unternehmen dem abweichenden Begehren der betroffenen Person zwangsläufig nachkommen muss, lässt sich der DSGVO nicht zweifelsfrei entnehmen. Eine explizite Regelung dazu findet sich jedenfalls nicht. Im Hinblick auf Konstellationen, in denen betroffene Personen zugewiesene Chiffrenummern oder hinterlegte E-Mail Adressen vergessen oder schlichtweg nicht mehr in Benutzung haben, muss dessen ungeachtet eine Auskunftserteilung in anderer Form als auf elektronischem Weg und nach entsprechender

Prüfung der Identität gleichwohl einzufordern sein (*https://datenschutz-hamburg.de/assets/pdf/DSK_Kurzpapier_Nr_6_Auskunftsrecht.pdf*).

4. Data-Breach-Verdachtsmeldung durch Asklepios: Anweisung wegen unzureichender Informationsbereitstellung

Lässt sich der Verdacht einer Verletzung des Schutzes personenbezogener Daten im Nachgang einer Verdachtsmeldung nach Art. 33 DSGVO nicht erhärten, muss die verantwortliche Stelle dennoch alle von der Aufsichtsbehörde zu dem Vorfall angeforderten Informationen bereitstellen.

Eine Hamburger Klinik hat unsere Behörde im August über den Verdacht einer unberechtigten Einsichtnahme in die Patientenakte einer Klinikmitarbeiterin durch andere Beschäftigte der Klinik informiert. Die daraufhin von uns erbetene Übersendung der bisherigen Ergebnisse der internen Untersuchung erfolgte nicht. Stattdessen erhielten wir lediglich die kurze Rückmeldung, dass sich der tatsächliche Hergang nicht abschließend habe aufklären lassen und widersprüchliche, teils nicht ausreichend belegbare Aussagen den Verdacht der möglichen Datenschutzverletzung nicht erhärtet hätten. Unsere diesbezügliche Aufforderung zur Konkretisierung der maßgeblichen ermittelten Tatsachen blieb erneut unbeantwortet. Dementsprechend sahen wir uns dazu gezwungen, die Klinikgesellschaft im Rahmen unser Untersuchungsbefugnisse nach Art. 58 Abs. 1 lit. a) DSGVO anzuweisen, uns die für die Erfüllung unserer Aufgaben erforderlichen Informationen bereitzustellen, und die sofortige Vollziehung der Anweisung anzuordnen. Erst auf diese förmliche und für die verantwortliche Stelle gebührenpflichtige Maßnahme hin erfolgte nun eine ausführliche Beantwortung unserer Fragen, die uns eine weitere Prüfung des Vorgangs ermöglicht.

Der Fall zeigt, wie wichtig die den Aufsichtsbehörden durch die DSGVO eingeräumten Untersuchungsbefugnisse sind, um die Aufgaben der Überwachung und Durchsetzung des Datenschutzes wahrnehmen zu können. Zugleich sollte er den verantwortlichen Stellen vor Augen führen, dass auch die Entscheidung, Hinweisen auf eine Verletzung des Schutzes personenbezogener Daten nicht weiter nachzugehen und eigene Ermittlungen einzustellen, dokumentiert und auf Nachfrage gegenüber der Aufsichtsbehörde begründet werden muss.

5. Kein Datenschutz wider Betroffenenrechte: Anordnung der elektronischen Bereitstellung einer Datenkopie

Ein elektronisch gestellter Antrag auf Zusendung einer Datenkopie im Sinne von Art. 15 Abs. 3 Satz 1 DSGVO wird nicht dadurch erfüllt, dass dem Betroffenen die persönliche Aushändigung einer Datenkopie gegen Vorlage des Personalausweises beim mehrere Stunden entfernten Verantwortlichen angeboten wird.

Wir sind im Berichtszeitraum von einem Betroffenen um Unterstützung bei der Durchsetzung seines Auskunftsrechts nach Art. 15 DSGVO gebeten worden. Der in Südniedersachsen wohnhafte Betroffene hatte von der Muttergesellschaft eines Klinikkonzerns mit Sitz in Hamburg per E-Mail eine schriftliche und kostenfreie Auskunft über die zu seiner Person gespeicherten Daten gemäß Art. 15 DSGVO und Zusendung der Auskunft in Form einer vollständigen Kopie der personenbezogenen Daten angefordert. Nach Prüfung des Antrages teilte die Verantwortliche mit, eine Kopie der vorhandenen Daten könne der Betroffene nur gegen Vorlage seines Personalausweises bei der verantwortlichen Stelle in Hamburg

erhalten, da es sich bei den Daten um besonders geschützte Gesundheitsdaten handele, die weder elektronisch noch per Post übermittelt werden dürften. Gegenüber unserer Behörde erklärte die Verantwortliche, dass dieses Vorgehen zwar nicht standard- oder routinemäßig sei, im Falle des Betroffenen aber unbedingt ausgeschlossen werden müsse, dass eine Lücke bei der Übermittlung der Daten oder der Identitätsfeststellung gegen den Konzern verwendet werden könne. Der Postversand möge sicher sein, aber wenn die Gesundheitsdaten auf dem Postwege abhanden kämen, läge eine Datenpanne vor. Des Weiteren bestünde beim Postversand das Problem der Identitätsfeststellung. Denn wer tatsächlicher Absender der bei ihr eingegangenen E-Mail mit dem Antrag auf Auskunft nach Art. 15 DSGVO sei, könne nicht zweifelsfrei festgestellt werden.

Diese Begründung hat uns nicht überzeugt. Art. 12 Abs. 1 DSGVO fordert, dass Auskünfte in „leicht zugänglicher Form“ erteilt werden sollen; Art. 15 Abs. 3 Satz 3 DSGVO besagt, dass bei einem elektronisch gestellten Antrag die begehrten Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen sind. Diesen Anforderungen war mit dem Angebot einer persönlichen Übergabe der Datenkopie gegen Vorlage des Personalausweises bei mehrstündigem Anreiseaufwand nicht genügt. Ebenso konnten die von der Verantwortlichen angemeldeten Zweifel an der Identität des Betroffenen die Weigerung einer Übermittlung in elektronischem Format nicht begründen. Bei der Ermittlung der an die Identitätsprüfung gestellten Anforderungen ist vielmehr der Verhältnismäßigkeitsgrundsatz zu beachten und muss eine Aushöhlung der Betroffenenrechte durch übersteigerte Anforderungen an die Identitätsfeststellung vermieden werden.

Wir haben daher die Verantwortliche angewiesen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen und mit Blick

auf die bereits deutlich überschrittene Frist des Art. 15 Abs. 3 Satz 1 DSGVO die sofortige Vollziehbarkeit angeordnet. Die Verantwortliche ist der Anordnung dadurch nachgekommen, dass sie dem Betroffenen die Daten auf einer Datenaustauschplattform passwortgeschützt zum Abruf bereitgestellt hat. Das Passwort wurde dem Betroffenen in einem verabredeten Telefontermin mitgeteilt.

V. BERATUNGEN UND DATENSCHUTZ-KOMMUNIKATION

1. Digital First

1.1 Zum Gesamtprojekt Digital First

Zu den Aufgaben der verantwortlichen Stellen gehört auch, die datenschutzrechtlichen Fragen frühzeitig aufzubereiten. Hier sollten die Fragen zum Datenschutz künftig stärker auf der konkreten Projektebene einbezogen werden. Auch sollten sichere Authentisierungsmittel für das Servicekonto anwendungsgerecht eingebunden werden.

Wie bereits im letzten TB beschrieben (26. TB, V 2.2), hat das Projekt Digital First im Herbst 2017 entschieden, den Aufbau der neuen Plattform „Online-Service-Infrastruktur (OSI)" zunächst mit wenigen schnell realisierbaren Projekten zu verbinden. Dazu wurden von der Senatskanzlei in Abstimmung mit den Behörden die Verfahren Asbestmeldungen sowie Bewohner- und Besucherparken als Prototypen bestimmt. Nach der Jahresplanung sollten noch in 2018 sieben Pilotprojekte folgen und ab 2019 sollte in der Phase der „Fabrikation" eine zweistellige Anzahl von Verfahren mit hoher Taktfrequenz mit neuen digitalisierten Modulen produktiv gehen.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) begleitet die Diskussionen im Rahmen der „Steuerungsgruppe Digital First". Hier lassen sich insbesondere abstrakte und grundsätzliche Fragestellungen ansprechen. Der Anspruch, dem Datenschutz einen großen Stellenwert einzuräumen, so wie es in der Senatsdrucksache 2016/03060 verankert ist, erfordert jedoch gerade auch, dass datenschutzrechtliche Themen stärker in der realen Projektarbeit konkretisiert werden. Dazu gehört zum einen, dass die Verantwortlichen auf der Projektebene für die einzelnen Vorhaben gemäß der Beteiligungsrichtlinie frühzeitig über das Vorhaben informieren. Zum anderen gehört es zu

den Aufgaben der jeweils verantwortlichen Stelle, dass sie die Aufbereitung der datenschutzrechtlichen Fragestellung, insbesondere die Fragen der erforderlichen Rechtsgrundlage, eine Zuordnung der verfolgten Ziele zu den vier Leitlinien von Digital First und eine Bewertung der Risiken für die Rechte der Betroffene frühzeitig verschriftlichen und im Zuge der Projektarbeit schrittweise vertiefen. Eine solche Aufbereitung gehört weder zu den Aufgaben des HmbBfDI noch ist diese bei der hohen Zahl der geplanten Projekte leistbar. Wir haben immer wieder deutlich gemacht, dass wir auf der Grundlage einer solchen Aufbereitung gerne für Beratungen zur Verfügung stehen, um einer datenschutzgerechten Digitalisierung in Hamburg den Weg zu ebnen.

Das Servicekonto soll der zentrale Zugang zu allen Anwendungen für elektronische Dienstleistungen der FHH werden, in dem sich die Bürgerinnen und Bürger aber auch Organisationen Benutzerkonten anlegen können. Die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten im Servicekonto ist das Onlinezugangsgesetz (OZG). Bereits aus den Pilotprojekten, zu dem auch die Digitalisierung der Feststellung der Schwerbehinderteneigenschaft gehört, wird deutlich, dass zahlreiche Online-Dienstleistungen im Zuge von Digital First bereitgestellt werden sollen, bei denen sensible personenbezogene Daten, wie z.B. Gesundheits- oder Sozialdaten übertragen und verarbeitet werden. Für solche Verfahren ist neben der Gewährleistung der Vertraulichkeit insbesondere während der Übertragung auch eine sichere Authentisierung beim Anmeldevorgang im Servicekonto erforderlich. Die Anforderungen sind mit der EU eIDAS-Verordnung vorgegeben, in der verschiedene Vertrauensniveaus definiert sind. Mit der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) TR 03107 sind diese Anforderungen konkretisiert. Insbesondere für einen Zugang zur Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO wird ein hohes

Vertrauensniveau gefordert. Für ein solches Vertrauensniveau ist eine Zwei-Faktor-Authentisierung erforderlich. Nach der TR 03107 können neben der eID-Funktion des neuen Personalausweises auch Hardwaretoken als Authentisierungsmittel auf hohem Vertrauensniveau genutzt werden. Zur smsTAN wird in dieser technischen Richtlinie ausgeführt: „Für neue Verfahren mit Schutzbedarf hoch / substantiell sollte smsTAN nicht mehr eingeführt werden." Das weit verbreitete Authentisierungsmittel Benutzerkennung und Passwort erreicht ebenfalls nur das Vertrauensniveau „normal".

Die meisten Hamburgerinnen und Hamburger haben mittlerweile den neuen Personalausweis, der für die Nutzung der eID-Funktion als zweiter Faktor bei der Authentisierung ausgelegt ist. Er sollte für Online-Dienstleitungen, bei denen sensible Daten verarbeitet werden, als Authentisierungsmittel im Servicekonto eingesetzt werden.

1.2 Prototyp Digital First: Bewohner- und Besucherparken

Das Bewohner- und Besucherparken ist grundsätzlich als eine der ersten Fachanwendungen zur Umsetzung des Projekts Digital First geeignet. Zur Umsetzung haben wir verschiedene Hinweise im Rahmen der bestehenden Rechtslage gegeben. Der weitere Aufbau der digitalen Infrastruktur wird weiterhin eine sorgfältige Prüfung erfordern.

Mit dem Prototypen Bewohner- und Besucherparken verfolgt die Hansestadt inhaltlich das Ziel, das bestehende Online-Angebot zu aktualisieren und den Zielen von Digital First anzupassen. Bewohner sollen letztlich die Möglichkeit erhalten, alle mit dem Bewohnerparken verbundenen Anliegen elektronisch zu betreiben. Als erste Stufe ist die Beantragung vorgesehen, bei der die Bewohner die Wahlmöglichkeit haben sollen, ob

sie den Bewohnerparkausweis zuhause ausdrucken und wie bisher sichtbar im KFZ hinterlegen wollen (print@home) oder ob sie die vollautomatisierte Lösung verfolgen wollen, bei der auch die Verkehrsüberwachung vor Ort erstmals vollautomatisiert über einen Abruf aus den beim LBV verwalteten Bewohnerparkausweisen erfolgen soll. Für Besucher sollen die Bewohner innerhalb eines Monats eine bestimmte Anzahl von Besucherparkausweisen beantragen können, für die die Angabe des Besucherkennzeichens gefordert wird. Nach Erstellung und Versendung des Besucherausweises wird das Kennzeichen sofort gelöscht, so dass eine Profilbildung von Besuchern und Gästen ausgeschlossen ist.

Der Landesbetrieb Verkehr (LBV) hat uns als fachverantwortlicher Verarbeiter dafür sein Fachkonzept vorgestellt. Die dafür notwendige Infrastruktur der New Platform war nicht Gegenstand des Konzepts, da mit dem Projekt Digitale Stadt eine modulare Einführung der New Platform vereinbart worden war und Einvernehmen bestand, dass die Art der in dieser Anwendung zu verarbeitenden Daten keine Datenschutzfolgenabschätzung und dementsprechend auch keine vorherige Konsultation nach Artt. 35 f. DSGVO erforderlich machten.

Das Verfahren war neben den spezifischen straßenverkehrsrechtlichen Vorschriften an den vorhandenen bundesrechtlichen Vorgaben sowie den Anforderungen der ab 25.05.2018 anzuwendenden DSGVO zu messen. Es begegnet zum derzeitigen Zeitpunkt im Wesentlichen keinen datenschutzrechtlichen Bedenken.

Die Verarbeitungsbefugnis für das Bewohnerparken ergibt sich aus der Wahrnehmung einer gesetzlich übertragenen Aufgabe. Die Verarbeitungsbefugnis für das Besucherparken ist gesetzlich nicht ausdrücklich geregelt, kann aber als spezifische, ermessensgebundene Ausgestaltung einer Ausnahmegenehmigung von der ansonsten bestehenden Gebühren-

pflicht gewertet werden. Die Genehmigung muss dem erteilt werden, den es angeht. Dafür stellt das Kennzeichen als auf den Halter rückführbares Datum den geringstmöglichen Erhebungsumfang dar; zudem ist es zur Überprüfung der erteilten Ausnahme vor Ort erforderlich, aber auch ausreichend. Die Erhebung des KFZ-Kennzeichens beim Besuchten stellt eine Dritterhebung dar, die nach §§ 5, 6 HmbDSG zulässig ist, da sie offensichtlich im Interesse des Betroffenen erfolgt und davon ausgegangen werden kann, dass er bei Kenntnis eingewilligt hätte.

Die Anwendung konnte nach dem Onlinezugangsgesetz (OZG) beurteilt werden. Es sieht u.a. vor, dass Bund und Länder bei der Ausführung von Bundesgesetzen ab spätestens 2022 Verwaltungsleistungen auch elektronisch anzubieten haben. Insoweit besteht seit dessen Geltung die gesetzliche Möglichkeit, Verwaltungsleistungen auch komplett medienbruchfrei elektronisch zu erbringen. Eine Einwilligung in die bisher als Zusatzangebot zur persönlichen Vorsprache angebotene elektronische Antragstellung kann daher entfallen. Spezifische Anforderungen nach dem OZG wie die Einwilligung in die Nutzung bereits vorhandener Daten sind dabei umzusetzen. Der Workflow sollte obligatorisch alle nach dem OZG und der DSGVO erforderlichen Einwilligungen unterstützen und offen sein für weitere bereichsspezifische Anforderungen. Dazu gehört u.a. die Einwilligung in die automatisierte Entscheidungsfindung nach Art. 22 Abs. 2 lit. c DSGVO, da diese Form der automatisierten Einzelentscheidung im Bereich des Bewohnerparkens bisher gesetzlich nicht vorgesehen ist.

Darüber hinaus haben wir neben Hinweisen auf die allgemeinen Anforderungen nach DSGVO empfohlen, die angegebenen Speicherfristen insbesondere bei den auf Einwilligung beruhenden Verfahrensteilen auf das unbedingt erforderliche Maß zu begrenzen und die Erforderlichkeit im Einzelnen nochmals zu überprüfen. Außerdem sollte die Aufgabenwahrneh-

mung der beteiligten Stellen nach der funktionalen Aufgabenzuordnung betrachtet und im Rechte- und Rollenkonzept umgesetzt werden.

Zu Redaktionsschluss hat der LBV angekündigt, die Möglichkeit zur weiteren Erläuterung in Anspruch nehmen zu wollen.

2. Strategie Intelligente Transportsysteme (ITS)

Die Mitarbeit in den Strategie-Gremien wurde fortgesetzt. Einzelne Projekte wurden datenschutzrechtlich beraten. Weiterhin zeigt sich eine große Bandbreite datenschutzrechtlicher Fragestellungen.

Wir haben die ITS-Strategie des Senats und deren datenschutzrechtliche Implikationen bereits ausführlich im 26. TB behandelt (V.2.3). Im Berichtszeitraum haben wir im Rahmen unserer Kapazitäten weiter an der Gremienarbeit teilgenommen und dort u. a. über den Fortschritt der internationalen datenschutzrechtlichen Diskussion berichtet. Weiter haben wir an der Fortschreibung der ITS-Strategie im Fortschrittbericht mitgewirkt und darin die angemessene Betonung des Themas als alle Bereiche betreffendes Querschnittsthema erreicht.

Zum Schwerpunktthema „Automatisiertes und vernetztes Fahren" (vgl. 26. TB, V.2.3) hat es erste Gespräche und Beratungen gegeben. Dabei konnte letztlich eine weitere Sensibilisierung hinsichtlich der Erforderlichkeit hinreichender Rechtsgrundlagen auch für den Testbetrieb mit Echtdaten aus dem realen Straßenverkehr erreicht werden.

2.1 Fortschrittsbericht des Senats

An der Abstimmung des Fortschrittsberichts waren wir beteiligt. Wir haben den Fortschrittsbericht nicht als Medi-

um zur datenschutzrechtlichen Kommentierung einzelner Projekte verstanden, sondern schwerpunktmäßig nochmals um die Berücksichtigung der nachfolgenden grundsätzlichen Fragestellungen geworben:

- Für Erprobungen im Rahmen des sog. Testfelds Hamburg (Testung mit Echtdaten) bedarf es einer gesetzlichen Grundlage, die die Verarbeitung personenbezogener Daten von Verkehrsteilnehmern im allgemeinen Verkehrsraum zu Testzwecken ausdrücklich erlaubt.

- Die Erprobung des autonomen Fahrens bedarf neben der Zulassung der eingesetzten Busse nach StVZO einer Änderung des StVG und einer weitergehenden Befassung damit zusammenhängenden Datenschutzfragen auf europäischer Ebene. Die Art.-29-Gruppe hatte sich im Rahmen ihrer Befassung mit C-ITS im Jahr 2017 ausdrücklich nur zu den sog. Stunde-1-Anwendungen geäußert und sich eine erneute Befassung bei fortgeschrittenem automatisiertem und autonomem Fahren vorbehalten.

- Die Beteiligung des HmbBfDI im Rahmen von Lenkungskreis und Arbeitskreis kann nur eine allgemeine Beratung hinsichtlich grundsätzlicher datenschutzrechtlicher Anforderungen beinhalten. Die Beurteilung der konkreten Projekte bis hin zur Freigabe von Verarbeitungstätigkeiten obliegt den insoweit Projektverantwortlichen; auf Anfrage leisten wir projektbezogene Beratung im Rahmen unserer Kapazitäten.

2.2 Schwerpunkt „Automatisiertes und vernetztes Fahren“

Das automatisierte und vernetzte Fahren wirft noch viele datenschutzrechtliche Fragen auf. Bei der angestrebten Testung unter Realbedingungen sollten insbesondere die Fragen der erforderlichen Rechtsgrundlagen rechtzeitig, nötigenfalls landesrechtlich, gelöst werden.

Seit langem sind in der Öffentlichkeit wie auch auf EU-Ebene die Stichworte automatisiertes und vernetztes Fahren (engl.: C-ITS) sowie autonomes Fahren im Gespräch. Die dafür unter Spezialisten gebräuchlichen Einstufungen des Automationsgrades sind allgemein weniger geläufig. Der Oberbegriff Automatisiertes und vernetztes Fahren gliedert sich in insgesamt sechs Automationsstufen.

Davon sind die Stufen 0 und 1 (kein eingreifendes Fahrzeugsystem/herkömmliches Fahren und Fahren mit zugelassenen Assistenzsystemen) bereits eingeführt.

In der Stufe 2/Teilautomatisiertes Fahren übernimmt das technische System in spezifischen, geregelten Anwendungsfällen die Längs- oder Querführung des Fahrzeugs, der Fahrer muss das System aber noch dauerhaft überwachen. In der Stufe 3/Hochautomatisiertes Fahren erkennt das System seine Grenzen und fordert den Fahrer dann zur Übernahme des Systems auf. In der Stufe 4/Vollautomatisiertes Fahren ist in spezifischen definierten Anwendungsfällen kein Fahrer mehr erforderlich. In der Stufe 5/Autonomes Fahren ist vom Start bis zum Ziel kein Fahrer mehr erforderlich, und zwar vollumfänglich bei allen Straßentypen, Geschwindigkeitsbereichen und Umfeldbedingungen.

Auch die ITS-Strategie der FHH beinhaltete von Anfang an das Handlungsfeld „Intelligente Fahrzeuge“. Bereits Anfang 2017 hat es seitens des Handlungsfeldes erste Überlegungen für ein Zielbild automatisiertes und vernetztes Fahren gegeben, die jedoch längere Zeit nicht weiter verfolgt wurden. Ende 2017 war uns seitens des Projektmanagement Office ITS mitgeteilt worden, dass man schwerpunktmäßig das Thema automatisiertes und vernetztes Fahren verfolgen wolle und dazu Beratungsbedarf sehe. Die danach zunächst angedachte Struktur einer eigenen Arbeitsgruppe, die die anstehenden Datenschutzfragen in dem angedachten Großprojekt

identifizieren und den vorgesetzten Stellen gegenüber benennen sollte, ist offenbar nicht weiter verfolgt worden.

2.2.1 Projekt Teststrecke Automatisiertes und Vernetztes Fahren (TavF)

Das Projekt TavF umfasst eine ca. 9 km lange nutzeroffene und herstellerunabhängige Teststrecke in der Innenstadt, die im Laufe der kommenden zwei Jahre durch den Landesbetrieb Straßen, Brücken, Gewässer (LSBG) mit der notwendigen Infrastruktur ausgestattet werden soll, um damit nach und nach die verschiedenen Stufen des automatisierten Fahrens unterstützen zu können. Letztlich soll darüber das autonome Fahren erprobt werden können. Die jeweiligen Projektpartner als Nutzer sind selbst für die rechts- und datenschutzkonforme Ausstattung ihrer Fahrzeuge und Technik verantwortlich.

Als erste Stufe wurde uns im November 2018 vom LSBG die Ausstattung verschiedener Ampeln mit Zusatzgeräten, sog. Roadside Units, vorgestellt, mit denen per W-LAN zunächst ausschließlich unidirektional die Ampelphasen rot/gelb/grün einschließlich der jeweiligen Fahrtrichtungen gesendet werden sollen. Es bestand Einigkeit, dass im Stadium dieser sog. Infrastructure2Vehicle-Kommunikation (I2V) noch keine personenbezogenen Daten verarbeitet werden und damit datenschutzrechtliche Belange noch nicht betroffen sind. Spätestens bei späteren Ausbaustufen, wenn die grundsätzlich mit der Technik auch schon jetzt mögliche Vehicle2Infrastructure-Kommunikation umgesetzt werden soll, durch die Daten vorbeifahrender KFZ von der Infrastruktur in Echtzeit erhoben und z.B. für die flexible Steuerung von Ampeln weiterverarbeitet werden sollen oder später auch für die technische Beeinflussung des Fahrverhaltens der Verkehrsteilnehmer genutzt werden sollen, sind auch seitens des LSBG Datenschutzbelange zu berücksichtigen.

Ergänzend haben wir darauf hingewiesen, dass teilnehmende Fahrzeuge, die untereinander kommunizieren (sog. V2V-Kommunikation) oder auch personenbeziehbare Daten anderer Verkehrsteilnehmer im öffentlich zugänglichen Straßenraum erheben und zu unmittelbaren Fahrzeugreaktionen verarbeiten, nur dann datenschutzgerecht eingesetzt werden können, wenn diese Verarbeitung gesetzlich erlaubt ist (vgl. dazu auch schon 26.TB 2.3.e) einschließlich der besonderen Anforderungen, die nach Art. 22 DSGVO an automatisierte Einzelentscheidungen gestellt werden. Da nicht absehbar ist, dass eine rechtzeitige Regelung vor Aufnahme durch den zuständigen Bundes- oder den europäischen Normgeber erfolgen wird, haben wir empfohlen, eine landesrechtliche ITS- Regelung zu Testzwecken zu prüfen. Dabei haben wir wiederholt die datenschutzrechtliche Problematik der Testung mit Echtdaten im realen Straßenverkehr angesprochen, die nun allgemein offenbar massiv unter dem Stichwort „Reallabore" als Strategie des Bundesministeriums für Wirtschaft und Energie verfolgt werden soll. Hierzu ist nun seitens der Behörde für Wirtschaft und Innovation Beratungsbedarf angemeldet worden.

2.2.2 Projekt Hamburg Electric Autonomous Transportation (HEAT)

Auch für den Bereich des öffentlichen Nahverkehrs ist der Einsatz von automatisierten und vernetzten Fahrzeugen in der Planung. Die Hamburger Hochbahn AG hat uns dazu mit den beteiligten Projektpartnern bereits im März 2018 Überlegungen vorgestellt, nach denen das automatisierte und vernetzte Fahren in den gemäß § 63a StVG geregelten Stufen in einem Bus vom automatisierten Fahren mit Fahrerbegleitung und ohne Fahrgäste bis hin zum autonomen Fahren mit Fahrgästen zwischen Juli 2018 und Anfang 2020 auf einer ca. 3,6 km langen Strecke in der Hafencity umgesetzt werden sollte.

Wir haben seinerzeit darauf hingewiesen, dass die Regelungen im StVG für das autonome Fahren noch nicht ausreichten, dass die nach der Richtlinie 2010/40/EU (sog. ITS-Richtlinie) erforderliche Delegierte Verordnung zur Festlegung der technischen Anforderungen an automatisiertes und vernetztes Fahren noch ausstehe und die Datenschutzbeauftragten der Art.-29-Gruppe in ihrer Stellungnahme zu C-ITS schon für die sog. Stufe I-Anwendungen eine bereichsspezifische gesetzliche Regelung gefordert hätten (vgl. hierzu auch schon 26. TB, V 2.3b). Dies gilt somit erst recht für die fortgeschrittenen Verfahren des automatisierten bis autonomen Fahrens (Stufen 3 – 5).

Unabhängig von der Frage der Testung mit Echtdaten werden insbesondere auch die verschiedenen technischen Komponenten, die personenbezogene oder personenbeziehbare Daten in die automatisierten Reaktionen einbeziehen sollen, einer eingehenden Betrachtung hinsichtlich Zulässigkeit, Datensparsamkeit und Sicherheit unterzogen werden müssen. Wir sehen auch die Notwendigkeit, die technischen Anwendungen angesichts der damit durchaus verbundenen Gefahren für Leib und Leben einer grundsätzlich gesetzlich näher zu regelnden Vorabkontrolle zu unterwerfen und auch die passiv betroffenen Verkehrsteilnehmer hinreichend über die Datenverarbeitung im öffentlichen Raum zu informieren (Artt. 13ff DSGVO).
Im November 2018 haben wir auf den Sachstand zum Erlass der Delegierten Rechtsverordnung nach der ITS-Richtlinie einschließlich der dazu vom Europäischen Datenschutzausschuss abgegebenen Stellungnahme hinweisen können. Bis Redaktionsschluss lag das angekündigte Datenschutzkonzept noch nicht vor.
Wir werden das Projekt im Rahmen unserer Kapazitäten weiter begleiten.

2.3 Projekt Vehicle Data Driven Business (vddb)

Trotz des Ziels, führend in intelligenten Verkehrsanwendungen zu sein, sollte sich die Stadt bei Einbindung in allgemeine Verkehrsforschungs- und Big-Data-Projekte vor unnötigen Verantwortlichkeiten hüten.

Das Projekt vddb ist Ausfluss des im Jahre 2016 zwischen der VW AG und der Freien und Hansestadt Hamburg (FHH) geschlossenen Memorandums of Understanding, mit dem die Parteien eine Zusammenarbeit in den Bereichen Urbane Mobilitätskonzepte und Intermodalität, Verkehrssteuerung und -management, Autonomes Fahren und Parken, Innovative Fahrzeugkonzepte und Alternative Technologien sowie Luftreinhaltung vereinbart hatten.

Ausgehend von der Situation, dass immer mehr Fahrzeuge mit moderner Sensorik und Connectivity Devices ausgestattet sind, besteht die Möglichkeit zur Sammlung großer Datenmengen, aus denen Mehrwerte für verschiedene Anwender generiert werden können. Im Fokus sollten zunächst mögliche Bedarfe der FHH stehen. Mit dem Projekt sollten der Bedarf an Mehrwerten, die dafür erforderlichen personenbezogenen, personenbeziehbaren Daten und sonstigen Informationen sowie die dafür erforderliche technische Umsetzung eruiert und ausgewertet werden. Die dafür verarbeiteten Daten aus den KFZ, mitgeführten Devices und erforderlichenfalls eigens installierten Zusatzgeräten sollten Informationen zunächst insbesondere zu den Kategorien Wetter, Reibwerte und Glätte, freie Parkplätze, ausgefallene Straßenlaternen, Verkehrszeichen, Fahrbahnzustand und -markierungen sowie Fotos zur Plausibilisierung liefern können. Nach der ursprünglichen Planung kam der FHH dabei der Part zu, geeignete Fahrzeugflotten zu stellen und städtische Informationsbedarfe zu ermitteln. Die eigentliche Datenerhebung und weitere Verarbeitung bis hin zur Informationsgewinnung mittels Aggregierung

sollte durch die VW AG erfolgen. Im weiteren Verlauf wurde von der Einbindung stadteigener Fahrzeuge abgesehen und seitens der VW AG stattdessen der Einsatz von Taxiflotten favorisiert.

Zu den uns vom Landesbetrieb Straßen, Brücken, Gewässer (LSBG) vorgelegten Vertragsunterlagen haben wir im Wesentlichen empfohlen, von einer vertraglich vereinbarten gemeinsamen Verantwortung gemäß Art. 26 DSGVO Abstand zu nehmen, was insbesondere eine Mithaftung nach Art. 82 DSGVO bedeuten würde, zumal sich die VW AG die Ausgestaltung des Verfahrens und die Verwertung aller erhobenen Daten vorbehalten hat. In diesem Fall wäre die personenbezogene Datenverarbeitung allein von der VW AG zu verantworten und unterläge der Aufsicht der Landesbeauftragten für den Datenschutz Niedersachsen.

Vorsorglich haben wir gleichwohl auch darauf hingewiesen, dass im vorgelegten Datenschutzkonzept nicht alle betroffenen Personengruppen berücksichtigt waren. Dies galt allgemein für die Fahrzeughalter und die sonstigen Verkehrsteilnehmer sowie insbesondere, soweit mit der einzusetzenden Technik auch Tonaufnahmen des Innenraums entstehen sollten, für die Fahrzeuginsassen.
Des Weiteren wäre in jedem Einzelfall zu prüfen, ob die angestrebte Pseudonymisierung und Aggregierung der Daten je nach Anzahl der beteiligten KFZ, dem Umfang des Testfelds und der Gestaltung des Zeitfensters und des Zeitraums tatsächlich gewährleistet werden können.
Schließlich waren die vorgelegten Einwilligungserklärungen in verschiedenen Punkten überarbeitungsbedürftig.

Zu Redaktionsschluss wurde uns mitgeteilt, dass man unserer Empfehlung gefolgt sei und vorgeschlagen habe, aus der gemeinsamen Verantwortung auszusteigen, und sich dieser Vorschlag seitens der VW AG in der Prüfung befinde.

3. Werbung unter Geltung der DSGVO

Auch im Bereich Werbung ist die Anzahl der Beschwerden, Eingaben und Beratungsanfragen im Berichtszeitraum exponentiell angestiegen. Zum einen war die Verunsicherung im Umgang mit der neuen Rechtslage spürbar, zum anderen hat die mediale Berichterstattung im Zuge des Wirksamwerdens der DSGVO das Bewusstsein für datenschutzrechtliche Fragen geschärft.

So haben sich Bürgerinnen und Bürger über werbliche Ansprachen von Unternehmen beschwert, die sie entweder postalisch oder elektronisch erhalten haben. Dabei ist die Verwendung von Adressdaten für werbliche Zwecke in vielen Fällen auch ohne Einwilligung möglich.

Postalische Werbeansprachen an eigene Kundinnen sind etwa zulässig, solange diese von ihrem Widerspruchsrecht keinen Gebrauch gemacht haben. Ein solcher Werbewiderspruch kann voraussetzungslos geltend gemacht werden. Auf das Widerspruchsrecht ist in verständlicher Form sowie getrennt vom werblichen Inhalt der Ansprache hinzuweisen. Erfolgt ein Werbewiderspruch, führt dies zu einem Verarbeitungsverbot für Zwecke der Direktwerbung. Um diesem gesetzlichen Verarbeitungsverbot zu entsprechen, führen Unternehmen Sperrdateien (auch ‚Blacklist'), die es ermöglichen, bei künftigen Werbekampagnen einen Abgleich durchzuführen. Insofern besteht hier in der Regel eine Aufbewahrungspflicht des Unternehmens.

Mit dieser Aufbewahrungspflicht kollidieren gelegentlich Löschungsersuchen betroffener Personen, die sowohl einen Löschungsanspruch, als auch einen Werbewiderspruch geltend machen. Hier mussten wir teilweise Überzeugungsarbeit leisten. Ohne Zweifel stehen sich die Ansprüche gegenüber und müssen zu einem Ausgleich gebracht werden. Unterneh-

men ist zu empfehlen, diese Speicherung transparent darzulegen und gleichzeitig zu verdeutlichen, dass die Sperrdatei zu keinem anderen Zweck verarbeitet wird.

Immer wieder kommt es allerdings vor, dass Werbewidersprüche keinen Eingang in diese Sperrdateien finden und es infolgedessen zu einer datenschutzwidrigen werblichen Ansprache kommt. Als Sanktion haben wir in einer Vielzahl der Fälle Verwarnungen nach Art. 58 Abs. 2 lit. b) DSGVO ausgesprochen. Eine Verwarnung kommt regelmäßig bei einfachen Verletzungen der DSGVO in Betracht, welche zu keiner erheblichen Gefährdung des informationellen Selbstbestimmungsrechts geführt haben. Sofern wir in Zukunft Wiederholungsfälle oder einen systematischen Fehlumgang mit Webewidersprüchen feststellen, werden aber auch Bußgeldverfahren angestrengt werden.

Anders als postalische Direktwerbung steht die elektronische Bewerbung grundsätzlich unter einem Einwilligungsvorbehalt der betroffenen Person. Dies gilt sowohl bei werblichen Ansprachen gegenüber Verbraucherinnen und Verbrauchern, als auch bei Unternehmenswerbung. Lediglich bei Bestandskunden kann eine Ausnahme dieses Einwilligungsvorbehaltes greifen.

Diese Einwilligung muss durch den Verantwortlichen auch nachweisbar sein. Hierbei bietet sich regelmäßig das Double-Opt-In-Verfahren an. Unzureichend für den Nachweis der Einwilligung ist dabei die bloße Angabe eines ‚Timestamps', der Registrierungsdatums und IP-Adresse beinhaltet. Der Nachweis der Einwilligung erfordert vielmehr die Protokollierung des gesamten Registrierungsverfahrens sowie des Inhalts der Einwilligung.

Auch bei telefonischen Bewerbungen gilt ein Einwilligungsvorbehalt gegenüber Verbraucherinnen und Verbrauchern. Sonstige Marktteilnehmer können aufgrund einer mutmaß-

lichen Einwilligung telefonisch beworben werden. Werbliche Ansprachen per Telefax sind unabhängig davon, ob diese gegenüber Verbraucherinnen und Verbrauchern oder sonstigen Marktteilnehmern erfolgen, nur mit einer ausdrücklich erklärten Einwilligung zulässig.

Bei Missachtungen von Werbewidersprüchen, rechtsgrundloser E-Mail-Werbung oder anderen unbefugten Verarbeitungsvorgängen stehen wir auch weiterhin als Beschwerdestelle zur Verfügung. Gegen unbefugte Telefonwerbung (sog. „Cold Calls“) ist die Bundesnetzagentur zuständige Beschwerdestelle.

4. Meldung von Data Breaches

Werden personenbezogene Daten aufgrund einer Datenpanne Dritten bekannt, ist der Vorfall unter Umständen bei uns und gegebenenfalls auch bei den Betroffenen zu melden. Wir haben dazu ein ausführliches Hinweispapier veröffentlicht.

Ob Softwarefehler, Hackerangriff oder Aktendiebstahl – wenn personenbezogene Daten unbeabsichtigt gelöscht oder Dritten bekannt werden, ist das gegebenenfalls ein meldepflichtiger Vorgang. Art. 33 DSGVO verlangt eine Mitteilung binnen 72 Stunden im „Falle einer Verletzung des Schutzes personenbezogener Daten“, „es sei denn, dass die Verletzung (...) voraussichtlich nicht zu einem Risiko führt“. Seit dem 25. Mai 2018 erreichen uns täglich Meldungen nach Art. 33 DSGVO. Dies geschieht vor allem über unser Onlineformular (*https://datenschutz-hamburg.de/meldung-databreach*). In Beratungsanfragen zeigt sich eine nach wie vor hohe Unsicherheit bei Verantwortlichen, in welchen Fällen wir zu informieren sind. Darum haben wir ein ausführliches Informationspapier erstellt, das auch beispielhafte Fallgruppen darstellt (*https://datenschutz-hamburg.de/assets/pdf/2018.11.15_Data%20Breach_Vermerk_extern.pdf*).

Die deutsche Formulierung „Verletzung des Schutzes“ darf danach nicht so missverstanden werden, dass jede Datenschutzverletzung (also jeder Verstoß gegen die DSGVO) zu melden ist. Die englischsprachige Formulierung „Data Breach“ ist dahingehend deutlicher, dass es sich um einen Sicherheitsbruch handeln muss, bei dem Daten unrechtmäßig Dritten offenbart werden oder infolge eines Sicherheitsbruchs gelöscht oder zeitweise unzugänglich gemacht werden. Mögliche Beispiele sind Hacking und Datendiebstahl, Fehler in Datenbanken oder Webservern, verlorengegangene USB-Sticks oder der Einbruch in Serverräume, die mit dem Verlust oder der Zerstörung von Hardware oder dem Auslesen von Datenträgern einhergehen. Auch unbeabsichtigte Falschübermittlungen fallen darunter wie etwa die fehlerhafte Etikettierung von Briefen oder die Versendung einer Massen-E-Mail unter Verwendung des cc- statt des bcc-Adressfelds. Ein Großteil der bei uns eingehenden Meldungen bezieht sich auf solche Fehlversendungen. Handelt es sich hingegen um eine zielgerichtete Übermittlung an einen unberechtigten Empfänger, handelt es sich nicht um einen Data Breach, sondern um eine schlichte rechtswidrige Verarbeitung. Ein Data Breach liegt nicht vor, wenn ein Zugriff Dritter auf die Daten sicher ausgeschlossen werden kann, weil dies etwa durch Logfiles belegt ist oder weil gestohlene Hardware wirksam verschlüsselt ist.

Die Meldepflicht bei uns besteht nur, wenn die Verletzung zu einem Risiko für die Betroffenen führt. Das Risiko bemisst sich aus der Korrelation zwischen der Schwere des möglichen Schadens und dessen Eintrittswahrscheinlichkeit. Kriterien für die Bemessung des Risikos sind unter anderem die Sensibilität und der Umfang der Daten und das Missbrauchsrisiko für die Betroffenen.

Große praktische Probleme resultieren aus der Anforderung, die Meldung binnen spätestens 72 Stunden vorzunehmen.

Die Frist beginnt ab Kenntnis von den erheblichen Tatsachen durch die verantwortliche Stelle. Dabei genügt es grundsätzlich, dass irgendjemand im Unternehmen oder der verantwortlichen Behörde Kenntnis erlangt. Die Meldepflicht tritt noch nicht ein, wenn zunächst nur vage Hinweise vorliegen. Dann hat der Verantwortliche jedoch so schnell wie möglich weitere Ermittlungen anzustellen und sich mit uns in Verbindung zu setzen, sobald sich ein angemessener Grad an Sicherheit herauskristallisiert. Sind dann noch nicht alle vom Gesetz geforderten Inhalte der Meldung bekannt, ist dies kein Hinderungsgrund für eine rechtzeitige Information. In dem Fall hat die Meldung schrittweise zu erfolgen, sodass die fehlenden Angaben später nachgereicht werden.

Besteht nicht nur ein einfaches, sondern ein hohes Risiko, sind zudem neben der Aufsichtsbehörde auch die Betroffenen zu informieren. Unsere Erfahrung zeigt, dass sich viele Unternehmen aus Angst vor Reputationsverlust zieren, sich an die Betroffenen zu wenden. Dabei ist es für den Einzelnen oftmals essentiell zu erfahren, dass er beispielsweise bei Diebstahl von Zahlungsinformationen seine Kontobewegungen im Auge behalten sollte oder im Fall von abgerufenen E-Mail-Adressen auf Phishing-E-Mails in seinem Posteingang achten sowie seine Passwörter ändern sollte. Erfahren Betroffene erst im Nachhinein durch den Missbrauch ihrer Daten vom Data Breach, ist der Reputationsverlust deutlich höher als bei professionellem, transparentem Verhalten. Zudem sollten im Zweifel die Betroffenen informiert werden, um ein Bußgeldrisiko auszuschließen.

5. Datenschutz in Arzt- und Zahnarztpraxen

Die hohe Zahl der Beratungsanfragen von Ärzten und Patienten zeigt Unsicherheiten bei der Umsetzung der DSGVO im Hinblick auf die Komplexität der maßgeblichen Regelungen. Für den Tätigkeitsbericht haben wir die fünf meistgestellten Fragen zum Datenschutz in Arzt- und Zahnarztpraxen ermittelt.

1. Wie sind die Informationspflichten nach Art. 13 und 14 DSGVO in der Arztpraxis umzusetzen?

Jeder Arzt, jede Berufsausübungsgemeinschaft (BAG) und jedes Medizinische Versorgungszentrum (MVZ) hat als Verantwortlicher den Patienten die in Art. 13 und 14 DSGVO genannten Informationen über die Verarbeitung ihrer Daten bereitzustellen.

Die Information der Patienten kann durch gut sicht- und lesbare Aushänge an verschiedenen, besonders frequentierten Orten der Praxis erfolgen (Rezeption, Wartezimmer o. ä.). Zusätzlich sollten die Informationen als Handzettel ausgelegt und bei der Erstaufnahme eines Patienten auf die Informationen und die Mitnahmemöglichkeit hingewiesen werden.

Patienten müssen die Datenschutzinformation nicht unterschreiben. Allerdings sollte auf eine belastbare Art und Weise dokumentiert werden, dass eine Information erfolgt ist.

2. Wann muss im Rahmen der ärztlichen Behandlung von Patienten eine Einwilligungserklärung eingeholt werden?

Die Erhebung, Speicherung und Nutzung von Gesundheitsdaten durch einen behandelnden Arzt, eine BAG oder ein MVZ

ist im Rahmen des Behandlungsvertrages und dem zur Behandlung erforderlichen Umfang ohne Einwilligungserklärung der Patientin/des Patienten von Gesetzes wegen zulässig (vgl. Art. 9 Abs. 2 lit. h letzte Alternative DSGVO).

Auch die Übermittlung von Patientendaten zwischen mehrere Ärztinnen und/oder Ärzten, die gleichzeitig oder nacheinander dieselbe Patientin/denselben Patienten untersuchen oder behandeln, kann – analog der Regelungen zur Schweigepflicht – ohne Einwilligung erfolgen, sofern Anhaltspunkte dafür vorliegen, dass das Einverständnis der Patientin/des Patienten anzunehmen ist und § 73 Abs. 1b SGB V nicht entgegensteht. Andernfalls ist die Übermittlung zwischen den behandelnden Ärzten nur auf der Grundlage einer Einwilligung zulässig.

Dies gilt auch für die Datenübermittlung zwischen behandelndem Arzt und beauftragtem Laborarzt. Nach unserer Auffassung handelt es sich bei der Erteilung von Laboraufträgen an einen Laborarzt nicht um ein Auftragsverarbeitungsverhältnis zwischen behandelndem Arzt und Laborarzt. Es bedarf daher keines Auftragsverarbeitungsvertrages nach Art. 28 DSGVO. Allerdings sind die Patienten entsprechend Art. 13 Abs. 1 lit. e DSGVO darüber zu informieren, an welchen Laborarzt Patientendaten übermittelt werden. Dentallabore sind demgegenüber im Verhältnis zu dem beauftragenden Zahnarzt als Auftragsverarbeiter einzustufen, weshalb zwischen beiden ein Auftragsverarbeitungsvertrag abgeschlossen werden muss.

Die Abrechnung über die Kassenärztliche Vereinigung Hamburg (KVH) bzw. über die Kassenzahnärztliche Vereinigung Hamburg (KZV HH) ist gesetzlich im SGB V geregelt und bedarf daher keiner Einwilligung. Demgegenüber setzt die Datenübermittlung an eine privatärztliche Abrechnungsstelle ebenso wie die dortige Verarbeitung der übermittelten Da-

ten eine wirksame Einwilligungserklärung der Patientin/des Patienten voraus, sofern die Abrechnungsstelle nicht lediglich als Auftragsverarbeiter tätig wird. Dasselbe gilt für eine etwaige Bonitätsüberprüfung von Privatpatienten über Auskunfteien wie die Schufa, für die zusätzlich eine Schweigepflichtentbindungserklärung eingeholt werden muss.

Will eine Arztpraxis zusätzliche Dienste wie z.B. einen Newsletter oder Recall-Service anbieten, ist die diesbezügliche Verarbeitung von Patientendaten aufgrund des nicht durch den Behandlungsvertrag gedeckten Zwecks nur mit Einwilligung der Patientin/des Patienten zulässig.

3. Darf die ärztliche Behandlung verweigert werden, wenn der Patient den Erhalt der Datenschutzinformationen nicht quittiert und/oder nicht in die Verarbeitung personenbezogener Daten einwilligt?

Nein, eine Behandlungsverweigerung wegen Nichtquittierung der Datenschutzinformationen oder Ablehnung einer Einwilligungserklärung kann weder auf die Informationspflicht nach Art. 13 DSGVO und die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO, noch auf das Verarbeitungsverbot des Art. 9 Abs.1 DSGVO gestützt werden.

4. Ist die Übermittlung von Patientendaten (Befunden, Arztbriefen u. ä.) per E-Mail oder per Fax zulässig?

Angesichts der Sicherheitsanforderungen an die Verarbeitung von Gesundheitsdaten gilt sowohl bei der elektronischen Speicherung als auch bei der elektronischen Übermittlung von Gesundheitsdaten grundsätzlich eine Verschlüsselungspflicht. Das heißt, dass ein Versand von Patientendaten mittels einfacher (lediglich transport-, nicht aber Ende-zu-

Ende-verschlüsselter) E-Mail regelmäßig keinen zulässigen Übermittlungsweg darstellt. Das gilt auch dann, wenn die Patientin/der Patient sich ausdrücklich mit dem Versand per einfacher E-Mail einverstanden erklärt hat, da die Verpflichtung zur Gewährleistung eines angemessenen Schutzniveaus nicht durch eine Vereinbarung zwischen Praxis und Patient abbedungen werden kann. Eine Übermittlung von Gesundheitsdaten wie Diagnosen, Krankheitsverläufen, Arzt- und Befundberichten, radiologischen Bildern oder Symptombeschreibungen per einfacher E-Mail ist daher nur dann vertretbar, wenn die „Umstände der Verarbeitung" (vgl. Art. 32 DSGVO) den Verschlüsselungsverzicht rechtfertigen. Dies kann zum Beispiel bei medizinischen Notfällen aufgrund der Dringlichkeit oder bei wechselndem Auslandsaufenthalt des Patienten mangels Erreichbarkeitsalternativen der Fall sein. Einfache Terminanfragen und -absagen, die neben dem Patientennamen und dem Kalenderdatum des angefragten/abgesagten Termins keine Gesundheitsdaten enthalten, dürfen aufgrund ihrer vergleichsweise geringen Sensibilität generell unverschlüsselt übermittelt werden.

Da im Regelfall bereits eine Umstellung des Telefonnetzes auf eine IP-basierte Datenübermittlung (All-IP) stattgefunden hat, bestehen gegenüber einer Faxübermittlung die gleichen Sicherheitsbedenken wie bei dem Versand von Gesundheitsdaten mittels einfacher E-Mail. Ist ein Faxversand ausnahmsweise zulässig, muss in organisatorischer Hinsicht sichergestellt werden, dass im Rahmen der Abgangskontrolle Adressat und Faxnummer (insbesondere die Aktualität gespeicherter Nummern) kontrolliert werden und die Übersendung beim Adressaten telefonisch angekündigt wird, so dass auch dort nur Berechtigte von den Daten Kenntnis nehmen können. Eine telefonische Ankündigung ist dann nicht erforderlich, wenn sich der Absender beim Empfänger vergewissert hat, dass aufgrund des Standorts des Empfängerfaxgeräts kein Unbefugter Kenntnis von dem Fax nehmen kann.

5. Wann muss eine Arztpraxis einen Datenschutzbeauftragten benennen?

Zu dieser Frage hat die DSK am 26. April 2018 einen Beschluss gefasst (vgl. *https://www.datenschutzkonferenz-online.de/media/dskb/20180426_dskb_dsb_bestellpflicht.pdf*), auf den insgesamt verwiesen wird.

6. Vertretung der Bundesländer in der Art. 29-Gruppe und im EDSA

Auch über den Wechsel von der Art. 29-Gruppe zum Europäischen Datenschutzausschuss haben wir dieses Gremium tatkräftig unterstützt.

Wie bereits im letzten Tätigkeitsbericht (26. TB, V 5) berichtet, haben wir den Auftrag der DSK erhalten und auch im Jahr 2018 wahrgenommen, die Länder in der Artikel 29-Gruppe zu vertreten. Dieses unter der Datenschutz-Richtlinie bestehende Gremium wurde mit Geltung der DSGVO ab 25. Mai 2018 durch den Europäischen Datenschutzausschuss (EDSA bzw. EDPB, European Data Protection Board) abgelöst. Das EDSA ist mit erheblich erweiterten Kompetenzen und Ressourcen ausgestattet, ist in die Zusammenarbeit zwischen den Aufsichtsbehörden in vielen Fällen einzubinden und fasst für die Aufsichtsbehörden verbindliche Beschlüsse, wie in Kapitel VII der DSGVO festgelegt.

Die DSK hat sich im Vorweg dieser Überleitung dafür eingesetzt, dass die Benennung oder jedenfalls das Vorschlagsrecht des Ländervertreters als Stellvertreters der bzw. des Bundesbeauftragten weiterhin ihr obliegt, konnte sich damit aber nicht durchsetzen. Vielmehr hat sich der Gesetzgeber im neuen Bundesdatenschutzgesetz für eine Wahl durch den Bundesrat entschieden, ohne dass die DSK als fachliches Gre-

mium zu beteiligen oder zu hören wäre. Dies ist aus fachlicher Sicht bedauerlich und rückt die Wahl verstärkt in den Bereich politischer Kriterien.

Besonders misslich ist dabei, dass der Bundesrat dem Vorschlag der DSK für die Nominierung des Ländervertreters offenbar nicht gefolgt ist und daher das Gremium bis heute keinen gewählten Ländervertreter hat.

Gleichwohl hat die DSK uns gebeten, die Bundesbeauftragte als gemeinsame Vertreterin im EDSA zu unterstützen und bei den Sitzungen zu begleiten. Dieser Bitte sind wir nachgekommen und haben in den fünf Sitzungen des EDSA im Jahr 2018 die Kommunikation zwischen den Ländern und dem EDSA aufrechterhalten, um die Länderinteressen dort so gut es geht zu wahren. Da die Länder neben dem Bund auf Arbeitsebene des EDSA (Expert Groups) mit großem Engagement und Arbeitseinsatz beteiligt sind, ist eine solche Vertretung wichtig, um die dort erzielten Ergebnisse zu sichern. In dieser Einschätzung sind wir uns mit der Bundesdatenschutzbeauftragten einig, und die Abstimmung der von deutscher Seite im EDSA eingenommenen Positionierung verläuft regelmäßig kooperativ. Eine enge und vertrauensvolle Abstimmung zwischen gemeinsamem Vertreter und Stellvertreter im EDSA wird daher immer wieder gefordert sein.

7. Presse- und Öffentlichkeitsarbeit

Die Pressearbeit beim HmbBfDI hat sich 2018 deutlich intensiviert; hinsichtlich der Anzahl an Anfragen kam es im Vergleich zum Vorjahr zu einer Steigerung von ca. 42%. Hierfür waren vor allem Anfragen zur seit Mai 2018 europaweit geltenden DSGVO, zum Facebook-Datenskandal rund um Cambridge Analytica sowie zur Gesichtserkennungssoftware Videmo 360 ausschlaggebend.

Im Berichtsjahr 2018 hat sich die bereits in den Vorjahren recht hohe Anzahl an Anfragen der Presse und der Medien noch deutlich erhöht. Die seit Mai 2018 geltende DSGVO hat hieran einen maßgeblichen Anteil, da zum einen zahlreiche inhaltliche Fragen zur neuen rechtlichen Regelung eingingen, zum anderen aber auch immer wieder abgefragt wurde, welche Auswirkungen die DSGVO auf die Arbeit der Aufsichtsbehörde hat. Hierbei ging es insbesondere um den deutlichen Anstieg der Beschwerden und die damit verbundene Arbeitsbelastung auf Seiten des HmbBfDI. Des Weiteren stand auch die Frage des Umsetzungsgrades der DSGVO durch Unternehmen und Verantwortliche im Fokus.

Neben diesem thematischen Hauptschwerpunkt spielten aber auch erneut die großen US-amerikanischen Internetkonzerne eine zentrale Rolle. Hier sind vor allem der Facebook-Datenskandal rund um Cambridge Analytica sowie der Data Breach bei Google+ zu nennen. Gerade der zuerst genannte Fall hat zu einem deutlichen Peak bei den Anfragen des Monats März geführt (siehe Abb. 1). Wie schon in den Vorjahren sind zu diesen Themen auch zahlreiche Anfragen ausländischer Medien beim HmbBfDI eingegangen.

Des Weiteren gab es auch im Bereich der „Hamburgensien" einige Schwerpunkte, die gehäufte Presseanfragen verur-

sachten. Hier sind insbesondere zu nennen: die rechtliche Auseinandersetzung um die im Zusammenhang mit den Ermittlungen zum G20-Gipfel eingesetzte Gesichtserkennungssoftware „Videmo 360" sowie das von der Hamburger AfD-Fraktion eröffnete sogenannte „Neutralitätsportal".

Neben den oben genannten Hauptthemen richteten sich die Presseanfragen aber auch auf weitere Bereiche des Datenschutzes. Dazu gehörte beispielsweise der große Komplex Videoüberwachung mit Unterthemen wie Bodycams oder der geplanten Überwachung der Diesel-Fahrverbote. Auch zukunftsorientierte Aspekte wie Künstliche Intelligenz und Autonomes Fahren wurden seitens der Medien abgefragt. Kurzfristig erlangte gar die Frage des Datenschutzes bei Namen auf Klingelschildern eine gewisse mediale Aufmerksamkeit.

Im Berichtszeitraum 2018 haben den HmbBfDI insgesamt 368 Presseanfragen erreicht, das sind ca. 42% mehr als im Vorjahr 2017 (259). Im Durchschnitt wurden rund 30 Anfragen pro Monat bearbeitet.

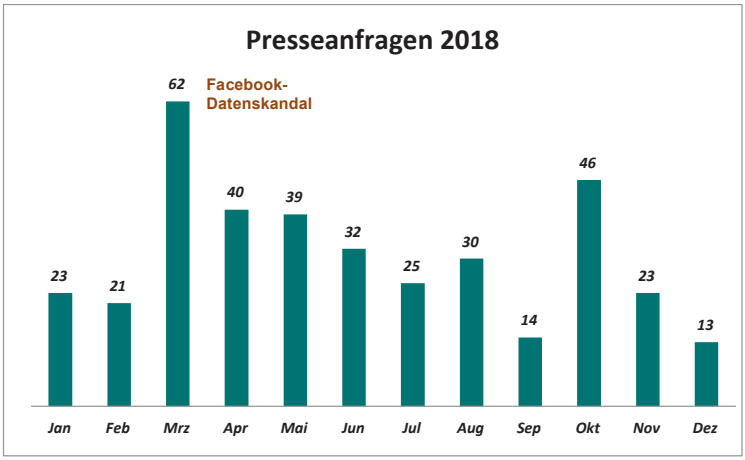


Abb. 1: Presseanfragen 2018 pro Monat mit Kennzeichnung „besonderer Ereignisse"

Wie Abb. 1 verdeutlicht, sticht der Monat März 2018 mit dem Anfragen-Peak zum Facebook-Datenskandal deutlich hervor. Insgesamt lässt sich bezüglich der Presseanfragen zu den beiden Internet-Konzernen Facebook und Google sagen, dass die Anfragen hierzu ca. 42% der Gesamtzahl ausmachten. Damit hat sich das Interesse hieran im Vergleich zum Vorjahr wieder deutlich erhöht (2017: 27% der Gesamtzahl). Von den beiden Konzernen liegt Facebook (34%) deutlich vor Google (8%).

Was die Herkunft der anfragenden Medien anbelangt, so bilden überregionale Medien wie schon im vorangegangenen Berichtszeitraum den Schwerpunkt. Anfragen ausländischer Medien sind im Jahr 2018 aufgrund der Geschehnisse um Facebook bzw. Cambridge Analytica sowie Google+ deutlich angestiegen, wie die nachstehende Tabelle zeigt:

Presseanfragen…	2017	2018
regionaler Medien:	72	68
überregionaler Medien:	174	273
ausländischer Medien:	13	45
Gesamt:	259	368

Tabelle1: Presseanfragen beim HmbBfDI 2017 und 2018

Neben den Tätigkeitsberichten des vergangenen Berichtszeitraums gab es im Jahr 2018 keine weiteren Veröffentlichungen im Printbereich. Das Internet-Angebot des HmbBfDI wurde in einem Relaunch umfassend erneuert und bietet unter anderem zahlreiche Informationen, Kurzpapiere und Handreichungen zur EU-Datenschutzgrundverordnung. Im Berichtszeitraum hat der HmbBfDI 10 Pressemitteilungen veröffentlicht.

Zudem haben der Hamburgische Datenschutzbeauftragte sowie einige Mitarbeiterinnen und Mitarbeiter der Be-

hörde erneut Vorträge und Präsentationen zu Aspekten der DSGVO sowie verschiedenen Themen des Datenschutzes durchgeführt und sich an Gesprächsrunden oder Podiumsdiskussionen beteiligt.

INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT VI.

1. Statistische Informationen (Zahlen und Fakten)

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder haben sich in ihrer Konferenz (DSK) am 08. November 2018 darauf geeinigt, dass die teilnehmenden Aufsichtsbehörden der Berichtspflicht aus Art. 59 DSGVO zukünftig in einheitlicherer Form nachgekommen werden. Obwohl die Übereinkunft erst ab dem Berichtszeitraum 2019 gilt und die Umsetzung freiwillig ist, wird im Folgenden, soweit es möglich ist, bereits für das Jahr 2018 darauf Bezug genommen.

1.1 Beratungen der Bürgerinnen und Bürger (Eingaben-Statistik / Beschwerden und Beratungen)

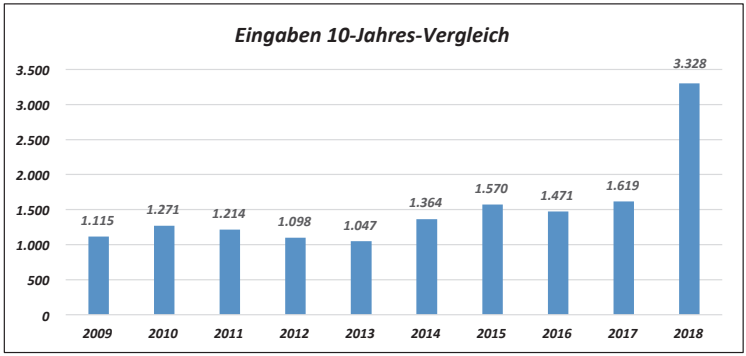
Bis zum 24. Mai 2018 wurden alle datenschutzrechtlichen Beschwerden von Bürgerinnen und Bürgern, alle Anzeigen von Datenschutzverletzungen und Beratungsanfragen in Einzelfällen - angelehnt an das Petitionsrecht - als Eingaben bezeichnet. Im Rahmen der DSGVO müssen die verschiedenen Sachverhalte aber differenzierter dargestellt werden, was die Vergleichbarkeit, gerade für das Jahr 2018, in dem fast fünf Monate noch altes Recht galt, schwierig macht. Um eine Vergleichbarkeit mit der neuen Systematik zu erreichen, hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) die Eingaben daher schon ab 01. Januar 2018 nach den Vorgaben der DSGVO erfasst und zwischen „datenschutzrechtlichen Beschwerden von Betroffenen“, „Beratungen betroffener Personen“ und „Sonstige Eingänge datenschutzrechtlicher Art“ differenziert. Neben den informationsfreiheitsrechtlichen Eingängen, über die weiterhin separat im Tätigkeitsbericht Informationsfreiheit berichtet wird, werden zusätzlich noch „Beratungen von Parlamenten und Regierungen“ und „Auskunftsersuchen an den HmbBfDI als verantwortliche Stelle“ im Rahmen der sogenannten „Anlassbezogenen Sachbearbeitung“ statistisch erfasst.

Im Berichtszeitraum haben den HmbBfDI insgesamt 3.670 schriftliche Eingänge erreicht, davon 1.079 bis zum 24. Mai 2018 und 2.591 ab 25. Mai 2018), davon waren zum Zeitpunkt der Drucklegung dieses Berichts allerdings nur 3.377 (rund 92%) statistisch erfasst, so dass von einer tatsächlich höheren Zahl ausgegangen werden muss.

Von den statistisch erfassten Eingängen waren
- 1.898 datenschutzrechtliche Beschwerden (499 bis 24. Mai / 1.399 ab 25. Mai)
- 457 Beratungen Betroffener (129 bis 24. Mai / 328 ab 25. Mai) und
- 973 sonstige Eingänge datenschutzrechtlicher Art (381 bis 24. Mai / 592 ab 25. Mai).

Damit haben den HmbBfDI im Jahre 2018 mehr als 3.328 datenschutzrechtliche Eingaben erreicht, was im Vergleich zum Vorjahr (1.619 Eingaben) mehr als eine Verdoppelung ist. Oder auch, um die immense Steigerung der Fallzahlen vielleicht noch etwas pointierter darzustellen, das mehr als 52fache der 63 Eingaben, die den Hamburgischen Datenschutzbeauftragten in der ersten Jahreshälfte des Bestehens seiner Dienststelle erreicht haben und von denen der damalige Amtsinhaber sagte, dass ihn in den ersten Monaten seiner Tätigkeit verhältnismäßig viele Eingaben erreicht haben (1. TB, 4.2.1).

Auch der 10-Jahres-Vergleich macht die massive Steigerung der Eingabenzahlen im besonderen Maße deutlich, wobei auch hier wieder bei den Eingaben des Jahres 2015 die 400 Eingaben, die seinerzeit zu Google Street View eingegangen sind, keine Berücksichtigung finden, da dieses einmalige Phänomen das Bild verfälschen würde. Ob es sich auch bei den Eingaben 2018 um eine einmalige Spitze handelt oder ob sich die Zahl der Beschwerden und Beratungsanfragen auf diesem hohen Niveau einpendeln wird, wird im nächsten Tätigkeitsbericht an dieser Stelle beantwortet werden.



Neben den oben genannten Arten von Eingängen haben den HmbBfDI noch 19 Auskunftsersuchen nach Art. 15 DSGVO (bzw. § 18 HmbDSG vor dem 25. Mai 2018) erreicht, also Anfragen von Bürgerinnen und Bürgern nach den beim HmbBfDI zu ihrer Person gespeicherten Daten. Diese verhältnismäßig hohe Zahl (in den Vorjahren waren es nie mehr als 3 Anfragen pro Jahr) ist wahrscheinlich auf einen Irrtum bzw. eine missverständlich formulierte Datenschutzerklärung von verantwortlichen Stellen zurückzuführen, denn größtenteils sind die Anfragenden hier vorher nie in Erscheinung getreten (vgl. I.3).

Wie an dieser Stelle im letzten Tätigkeitsbericht des HmbBfDI prognostiziert wurde (vgl. 26. TB, VI. 1.1), ist es bei unserer Zuständigkeit für die Bearbeitung der Anträge auf Löschung aus den Suchergebnissen der Google-Suchmaschine, die zuvor von Google abgelehnt wurden, geblieben (vgl. III.5). Diese sind mit 231 Eingaben wieder auf einem hohen Niveau, bleiben jedoch unter dem Vorjahreswert (299). Ob sich die Werte in dieser Größenordnung einpendeln, bleibt abzuwarten.

Zusätzlich wurden 4.106 datenschutzrechtliche Beratungen für das Jahr 2018 statistisch erfasst. Diese Zahl beinhaltet nicht nur die bereits oben genannten „Beratungen Betroffener“ und die schriftlich eingegangenen Beratungsanfragen Nichtbetroffener oder verantwortlicher Stellen, die den

größten Teil der sonstigen Eingänge datenschutzrechtlicher Art ausmachen, sondern auch die verhältnismäßig häufigen Anfragen nach telefonischer Beratung und die gelegentlichen persönlichen Vorsprachen von Bürgerinnen und Bürgern bei HmbBfDI. Dies bedeutet, dass neben allen weiteren Aufgaben der Mitarbeiterinnen und Mitarbeiter des HmbBfDI durchschnittlich noch rund 19 Beratungen pro Arbeitstag durchgeführt wurden.

1.2 Stellungnahmen in Gesetzgebungsverfahren (Förmliche Begleitung bei Rechtsetzungsvorhaben)

Im Jahr 2018 wurde der Hamburgische Datenschutzbeauftragte in 30 Fällen von der jeweils federführenden Fachbehörde um eine datenschutzrechtliche Stellungnahme zu Rechtsetzungsvorhaben gebeten.

1.3 Bußgelder und Anweisungen (Abhilfemaßnahmen)

Mit Einführung der DSGVO haben sich die Sanktions- und Abhilfebefugnisse gewandelt. Die Möglichkeit des Bußgeldverfahrens aus dem Ordnungswidrigkeitsrecht ist geblieben, ebenso die Möglichkeit der Anordnung, die nach neuem Recht als Anweisung bezeichnet wird. Hinzugekommen sind Verwarnungen für den Fall, dass die Rechtswidrigkeit eines Verhaltens formell festgestellt werden soll, ohne dass die Verhängung eines Bußgelds geboten ist. Das Pendant zu Verwarnungen, die auf vergangenes Verhalten abzielen, sind Warnungen, mit denen die voraussichtliche Rechtswidrigkeit eines geplanten Verhaltens förmlich festgestellt wird.
Im Berichtszeitraum sind keine gerichtlichen Entscheidungen in Verfahren mit unserer Beteiligung ergangen.

1.3.1. Geldbußen

Die überwiegende Anzahl der im Berichtszeitraum verhängten Bußgelder bezieht sich auf die alte Rechtslage, weil die Verstöße vor dem 25.05.2018 begangen wurden. Bei der Bemessung der Bußgeldhöhe wurde deshalb noch der deutlich niedrigere Rahmen des BDSG alter Fassung herangezogen. In den zwei letzten Fällen fand der deutlich erhöhte Bußgeldrahmen nach der DSGVO Anwendung.

Bußgeldbescheide			
Sachverhalt	Verbotsvorschrift	Bußgeldhöhe in Euro	Status
Zusendung von Werbung via E-Mail trotz Widerspruchs	§ 43 Abs. 2 Nr. 5b BDSG a.F.	1.000,--	bestandskräftig
verspätete Auskunft	§ 43 Abs. 1 Nr. 8a BDSG a.F.	4.000,--	bestandskräftig
Zusendung von Werbung via E-Mail trotz Widerspruchs	§ 43 Abs. 2 Nr. 5b BDSG a.F.	3.000,--	Einspruch eingelegt
Videoüberwachung in einer Arztpraxis	§ 43 Abs. 2 Nr. 1 BDSG a.F.	5.000,--	bestandskräftig
Patientennamen im Cloud-Kalender	§ 43 Abs. 2 Nr. 1 BDSG a.F.	500,--	bestandskräftig
Fehlender Auftragsverarbeitungsvertrag	Artt. 83 Abs. 4 lit. a, 28 Abs. 3 DSGVO	5.000,--	Einspruchsfrist läuft
Verspätete Meldung eines Data Breaches und unterbliebene Information der Betroffenen	Artt. 83 Abs. 4 lit. a, 33 Abs. 1, 34 Abs. 1 DSGVO	20.000,--	Einspruchsfrist läuft

1.3.2 Verwarnungen

Seit Geltungsbeginn der DSGVO wurden zahlreiche Verwarnungen ausgesprochen. Es handelt sich um förmliche, feststellende Verwaltungsakte, die keine Geldbuße zum Gegenstand haben. Im Wiederholungsfall spielen vorangegangene Verwarnungen jedoch eine erhebliche Rolle bei der Frage, ob und in welcher Höhe ein Bußgeld verhängt wird.

Verwarnungen	
verspätete Auskunft	Art. 12 Abs. 3 DSGVO
unzureichende Auskunft	Art. 15 Abs. 1 DSGVO
verspätete Auskunft	Art. 12 Abs. 3 DSGVO
verspätete Auskunft	Art. 12 Abs. 3 DSGVO
verspätete Auskunft	Art. 12 Abs. 3 DSGVO
verspätete Auskunft	Art. 12 Abs. 3 DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
verspätete Auskunft	Art. 12 Abs. 3 DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Elektronische Bewerbung ohne Rechtsgrundlage	Art. 6 Abs. 1 Satz 1 DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Elektronische Bewerbung ohne Rechtsgrundlage	Art. 6 Abs. 1 Satz 1 DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Werbung trotz Werbewiderspruchs	Art. 21 Abs. 3, 6 Abs. 1 Satz 1 lit f) DSGVO
Verstoß gegen Datensicherheit	Art. 6 Abs. 1 i.V.m. Art 24, 25, 32 DSGVO
unvollständige Auskunft	Art. 15 Abs. 1 DSGVO
unrechtmäßige Speicherung	§ 15 TMG (alt), Art. 6 I f DSGVO
verspätete Auskunft	Art. 12 Abs. 3 DSGVO
rechtswidrige Videoüberwachung und Tonaufzeichnung	Art. 6 Abs. 1 lit f) und § 4 BDSG
Betrieb einer Dashcam	Art. 6 Abs. 1 lit f) und § 4 BDSG

1.3.3 Anweisungen und Anordnungen

Anweisungen sind Verwaltungsakte, mit denen wir ein Handeln, Dulden oder Unterlassen verbindlich verlangen können. Seit Geltungsbeginn der DSGVO ist es uns auch möglich, verbindliche Anweisungen gegenüber öffentlichen Stellen auszusprechen. Ergeht ein solcher Verwaltungsakt nicht auf Grundlage der DSGVO, sondern gemäß der Richtlinie (EU) 2016/680 gegen Polizei- der Justizmaßnahmen, spricht man von einer Anordnung.

Anweisungen und Anordnungen		
Sachverhalt	Zielrichtung der Anordnung	Rechtsgrundlage
Antrag auf Erhalt einer Kopie	Anweisung, den Anträgen des Betroffenen zu entsprechen	Art. 15 Abs. 3 Satz 1 DSGVO
Erstellung von Templates zur automatisierten Gesichtserkennung	Anordnung zur Löschung einer polizeilichen Datenbank	§ 6 HmbRI(EU)2016/680 UmsAAG i.V.m § 43 HmbJVollzDSG

1.4 Meldepflicht nach Art. 33 DSGVO

Die Verletzung des Schutzes personenbezogener Daten ist bei der Aufsichtsbehörde anzuzeigen, wenn ein Risiko für die Rechte und Freiheiten der Betroffenen besteht. Seit dem 25.05.2018 sind solche Meldungen in 210 Fällen eingegangen. Bei einem hohen Risiko sind auch die Betroffen zu informieren. Dies ist dabei in 74 Fällen geschehen. Die Anlässe für Data-Breach-Meldungen lassen sich wie folgt kategorisieren:

- Diebstahl: 16
- Falschversand: 65
- Hackerangriff: 35
- Softwarefehler: 8
- Fehlentsorgung: 3
- Verlust: 8
- Sonstiges: 57

1.5 Register nach § 38 Abs. 2 BDSG a.F.

Das Register nach § 38 Abs. 2 BDSG alter Fassung haben wir bis zum 24.05.2018 fortgeführt. Mit Wegfall der Rechtsgrundlage zur Speicherung der enthaltenen Daten haben wir es gelöscht.

2. Aufgabenverteilung (Stand: 1.1.2019)

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Straße 22, 20459 Hamburg
Tel.: 040/42854-4040
Fax: 040/42841-4000
E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.datenschutz-hamburg.de

Dienststellenleiter:	Prof. Dr. Johannes Caspar
Stellvertreter:	Ulrich Kühn
Vorzimmer:	Heidi Niemann

Presse- und Öffentlichkeitsarbeit, IT-Leitung, Internetangebot des HmbBfDI
Martin Schemm

Beauftragter für den Haushalt, Verwaltungs- und Personalleiter
Arne Gerhards

Haushaltsplanung und -bewirtschaftung, Berichtswesen
Robert Flechsig

Gebühren und Bußgelder, Beschaffung, Aus- und Fortbildung
Rolf Nentwig

Vorzimmer, Geschäftsstelle
Heidi Niemann

Registratur
Katharina Schmidt

Registratur
Ipek Sari

Technische Grundsatzfragen bei E-Government, technisch-organisatorische Beratung und Prüfung
Dr. Sebastian Wirth

Technisch-organisatorische Beratung und Prüfung
Jutta Nadler

Technische Grundsatzfragen bei Biometrie, Videoüberwachung, Prüflabor, technisch-organisatorische Beratung und Prüfung
Eike Mücke

Informationsfreiheit/Transparenz, Videoüberwachung, Auskunftsanspruch nach Presserecht
Dr. Christoph Schnabel

Informationsfreiheit/Transparenz, Videoüberwachung
Cornelia Goecke

Informationsfreiheit/Transparenz, Videoüberwachung
Barbara Görnandt

Verkehr, Wirtschaftsverwaltung, Bezirks- und Parlamentsangelegenheiten, Wahlen und Volksabstimmungen, Hochschulwesen, behördliche Datenschutzbeauftragte, Landwirtschaft, Kirchen
Eva-Verena Scheffler

Grundsatzfragen des HmbDSG, Gesundheitswesen, Forschung, Schule und Bildungswesen, Sozialwesen
Saskia Fritzsche

Grundsatzfragen BDSG und DSGVO, Grundsatzfragen Internationales, Auskunfteien, Inkasso
N.N.

Beschäftigtendatenschutz, Handel, Industrie, Versand- und Onlinehandel, Geodaten
Dr. Jens Ambrock

Finanz-, Steuer- und Rechnungswesen, Steuerberater und Wirtschaftsprüfer, Vereine/Parteien/Gewerkschaften/ Stiftungen
Heike Wolters

Werbung- und Adresshandel, Markt- und Meinungsforschung, Bauen und Wohnen, Wasserversorgung und Energiewirtschaft
Richard Heyer

Sicherheit und Justiz, Waffenrecht, private Sicherheitsdienste und Detekteien, Rechtsanwälte und Notare, Ausländerwesen
Anna-Lena Greve

Gewerbliche Dienstleistungen, Kreditwirtschaft, Versicherungswirtschaft
Oksan Karakus

Technische Grundsatzfragen bei Medien, Telemedien, Telekommunikation, Presse, Rundfunk, technisch-organisatorische Beratung und Prüfung
Ulrich Kühn

Juristische Grundsatzfragen bei Presse, Rundfunk, Google Suchergebnisse,
Telemedien insb. Google
Katja Weber

Technische Grundsatzfragen bei Apps, Internet of Things, technisch-organisatorische Beratung und Prüfung
Herr Schneider

Juristische Grundsatz- und Sachbearbeitung bei Google Suchergebnisse, Medien, Telemedien, E-Government, Elektronischer Rechtsverkehr
Herr Schröder

Juristische Grundsatz- und Sachbearbeitung bei Telemedien insb. soziale Netzwerke, Google Suchergebnisse, Medien, gewerbliche Dienstleistungen
Frau Jacobson

Statistik, Meldewesen, Pass- und Ausweiswesen, Personenstands- und Archivwesen, Kultur
Uta Kranold

Projekt „Prüfung von Smart Devices“
Roland Schilling

Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH
Foto Titelseite: Thomas Krenz
Druck: Beisner Druck GmbH & Co. KG

Herausgeber:
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Straße 22
20459 Hamburg
Tel.: 040/42854-4040 (Geschäftsstelle)
Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit