TÄTIGKEITSBERICHT DATENSCHUTZ 2016/17

Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Hamburg

26. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2016 / 2017

Herausgegeben vom
Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C)
20095 Hamburg

Tel. 040-428 54 40 40
Fax 040-428 54 40 00
mailbox@datenschutz.hamburg.de

Auflage: 700 Exemplare
Layout: Kameko Design, Inga Below
Foto Titelseite: Martin Schemm
Druck: print 74

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

Vorgelegt im Februar 2018
Prof. Dr. Johannes Caspar
(Redaktionsschluss: 31. Dezember 2017)

INHALTSVERZEICHNIS

Vorwort – Tätigkeitsbericht in neuem Gewand

Der Datenschutz befindet sich in diesen Tagen in einer Bewährungsprobe. Mit Blick auf die ab dem 25. Mai 2018 in ganz Europa geltende Datenschutzgrundverordnung gilt es, zahlreiche Stellschrauben neu zu justieren. Viele rechtliche Neuerungen sind hierbei umzusetzen, und die Datenschutzaufsichtsbehörden müssen sich für die anstehenden Aufgaben neu aufstellen. Insofern richtete sich der Blick auch im Verlauf des Berichtszeitraums 2016/2017 eher nach vorne als zurück.

Eine im Zusammenhang mit der Datenschutzgrundverordnung ebenfalls zu erwähnende Neuerung betrifft die Verpflichtung jeder Aufsichtsbehörde, jährlich einen Bericht über die eigene Tätigkeit zu erstellen, so dass sich künftig die Berichtszeit von zwei Jahren auf eines verkürzt. Für den Bereich des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit soll in Zukunft der Berichtszeitraum mit Abschluss eines Kalenderjahres zum 31.12. enden, so dass der Berichtszeitraum nicht mit dem Inkrafttreten der Datenschutzgrundverordnung am 25. Mai 2018 beginnt, sondern mit Beginn eines jeweiligen Kalenderjahres.

Vor diesem Hintergrund haben wir – gewissermaßen im Vorgriff – das Konzept des gegenwärtigen Tätigkeitsberichts grundlegend verändert. Dazu gehört es, den Text zu straffen

und die einzelnen Abschnitte stärker auf den Schwerpunkt der behördlichen Tätigkeiten hin zu zentrieren. Es liegt in der Konsequenz dieses neuen Konzepts, dass der Bericht, der für den Zeitraum 2014/2015 ca. 300 Seiten umfasste, auf nunmehr etwa die Hälfte gekürzt wird. Diese inhaltliche Beschränkung trägt im Übrigen auch den nach wie vor äußerst angespannten personellen Ressourcen Rechnung.

In seiner neuen Gestalt werden im Tätigkeitsbericht die wesentlichen Punkte nicht mehr thematisch nach Sachbereichen gegliedert, sondern nach output-orientierten Kriterien, die die Arbeit der Behörde (Prüfungen, Berichte, rechtsverbindliche Anordnungen und Bußgelder, Beratungen und Datenschutzkommunikation sowie Informationen zur Behörde) quantitativ sowie qualitativ beschreiben. Dies soll den Bericht besser lesbar, verständlicher und insgesamt transparenter machen.

Für den Berichtszeitraum wird im Folgenden unter diesen vereinheitlichenden Parametern eine Leistungsbilanz der Behörde in den letzten beiden Jahren für den Bereich des Datenschutzes in Hamburg gezogen und damit gleichzeitig die Öffentlichkeit über die wesentlichen Entwicklungen auf dem Gebiet des Datenschutzes für den Zuständigkeitsbereich des HmbBfDI sensibilisiert und umfassend informiert.

Prof. Dr. Johannes Caspar
Februar 2018

EINLEITUNG I.

I. EINLEITUNG

Tiefgreifende Neuordnung der rechtlichen Grundlagen erfasst gesamte Struktur aufsichtsbehördlichen Handelns

Gesetzgeberisch ist das geltende Datenschutzrecht auf europäischer Ebene grundlegend umgearbeitet worden: da ist zunächst die EU-Datenschutzgrundverordnung (DSGVO) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG zu nennen, die künftig als Vollregelung unmittelbar in allen Mitgliedstaaten anwendbar ist. Sie wird die EU datenschutzrechtlich vereinheitlichen und dazu führen, dass der Datenschutz künftig ein Markenkern der Rechtskultur Europas wird. Daneben verpflichtet die JI-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung die Mitgliedstaaten zur Umsetzung und dem Erlass eigener Regelungen zum Datenschutz für den Bereich der Strafverfolgung und der Gefahrenabwehr.

Mit der Veränderung der europäischen Tektonik des Datenschutzrechts verschieben sich auch die Fundamente des innerstaatlichen Datenschutzrechts über das Bundesdatenschutzgesetz bis hin zu den Landesdatenschutzgesetzen und datenschutzrechtlichen Fachgesetzen, die einer Anpassung an die neuen Regelungen bedürfen. Dieser Umsetzungsanpassungsbedarf im nationalen Recht ist noch nicht abgeschlossen. Ihn gilt es seitens der Datenschutzaufsichtsbehörden kritisch und achtsam zu begleiten.

Eine wesentliche Veränderung hat die Bürgerschaft der Freien und Hansestadt Hamburg bereits zum 1.1.2017 quasi im Vorgriff auf die Änderungen der Datenschutzgrundverordnung vorweggenommen: In Art. 60 a der Verfassung der Freien und

Hansestadt Hamburg hat die Aufgabe des Datenschutzes und der Informationsfreiheit und damit auch das Amt des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit auf Ebene der Landesverfassung eine eigene verfassungsbasierte Rechtsstellung erlangt. Hiermit wird eine völlige Unabhängigkeit hergestellt, wie sie Art. 52 der Datenschutzgrundverordnung verlangt und wie sie künftig für die Aufgabenerfüllung, nicht zuletzt für die rechtlich verbindliche Durchsetzung von Maßnahmen gegenüber öffentlichen Stellen, erforderlich ist. Insofern ist die Auflösung der zuvor noch bestehenden beschränkten Dienstaufsicht über den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit durch den Senat und die Herauslösung des Amts als Dienststelle der Justizbehörde konsequent und beispielgebend. Eine weitere wichtige Neuerung bringt die eigene Zuständigkeit des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, seinen Haushalt in einem Einzelplan eigenständig aufzustellen und diesen gegenüber der Bürgerschaft zu vertreten.

Nach wie vor im Gesetzgebungsverfahren auf europäischer Ebene befindet sich der Entwurf der E-Privacy-Verordnung des Europäischen Parlaments und des Rats über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG. Hier geht es um den Schutz der Privatsphäre für die Nutzer elektronischer Kommunikationsdienste und die Absicherung gleicher Wettbewerbsbedingungen für alle Marktteilnehmer. Die Verarbeitung elektronischer Kommunikationsdaten, bislang weitgehend auf die Nutzung von Onlinediensten bezogen, wird künftig durch Regelungen zum Tracking in der Offlinewelt ergänzt werden. Kommission und EU-Parlament haben hierzu bereits ihre Entwürfe vorgelegt. Derzeit diskutiert der Rat darüber. Es ist jedoch eher unwahrscheinlich, dass ein zeitgleiches Inkrafttreten der E-Privacy-Verordnung mit der Datenschutzgrundverordnung im Mai des nächsten Jahres erfolgen kann.

Nicht alle derzeit diskutierten Regelungsvorschläge haben bereits den Weg in das Gesetzgebungsverfahren genommen. Eine wichtige Diskussion der letzten beiden Jahre betrifft die Forderung nach Schaffung einer künftigen Digitalen Grundrechtecharta auf Ebene der Europäischen Union (digitalcharta.eu). Diese geht zurück auf eine Initiative einer Gruppe von Bürgerinnen und Bürgern aus ganz unterschiedlichen gesellschaftlichen Bereichen, die unterstützt von der Zeit-Stiftung nach Antworten auf die drängenden Fragen einer normativen Rahmenordnung zum Schutz vor möglichen negativen Auswirkungen einer umfassenden Digitalisierung suchen. Die Initiatoren eint das Bewusstsein, dass die Entwicklung von Staat und Gesellschaft nicht einer technikgetriebenen Ökonomisierung der Privatsphäre vorbehalten werden darf. Vielmehr ist eine inhaltliche Neuausrichtung der Grundrechteordnung notwendig. Diese Herausforderung gilt es anzunehmen, soll auch in Zeiten eines disruptiven technologischen und gesellschaftlichen Wandels eine selbstbestimmte menschengerechte Zukunft möglich sein. Die Diskussion um die Ausrichtung einer digitalen Grundrechteordnung verläuft dabei als ein iterativer Prozess, in dem die Öffentlichkeit einbezogen ist und die Beteiligung von möglichst vielen Menschen angestrebt wird. Gefordert ist die Gestaltungskraft und Verantwortung aller. Kommentare und Vorschläge sollen Verbesserungen und Ergänzungen der Entwurfsfassung der Charta ermöglichen, so dass sich der Entwurf dynamisch weiterentwickeln kann.

Die EU-Datenschutzgrundverordnung stand bei den legislativen Neuerungen in Deutschland in den letzten beiden Jahren im Vordergrund. Hier lag die Priorität auf der Schaffung rechtssicherer Strukturen der zum Teil sehr unbestimmten, unterkomplexen und tatbestandlich offenen Regelungen. Dazu hat die Artikel 29-Datenschutzgruppe der EU, die aus den Datenschutzbehörden aller EU-Mitgliedstaaten besteht, verschiedene Leitlinien erarbeitet und veröffentlicht (*https://www.datenschutz-hamburg.de/datenschutz-fuer-firmen-und-behoerden/*

das-neue-datenschutzrecht/working-papers-art-29.html). Ergänzend dazu hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Reihe von sogenannten Kurzpapieren veröffentlicht, die ebenfalls zur Auslegung der neuen Vorschriften dienen und für die verantwortlichen Stellen Orientierung und Hilfestellung leisten (*https://www.datenschutz-hamburg.de/news/detail/article/kurzpapiere-der-dsk-zur-dsgvo.html*).

Die Datenschutzgrundverordnung wird mit ihren 99 Artikeln die Datenschutzlandschaft in Europa tiefgreifend verändern. Sie enthält eine fortschrittliche Weiterentwicklung der Datenschutzrechte Betroffener, die an bewährte Traditionen anknüpft und künftig stärker auf Information, Transparenz und Beteiligung von Betroffenen bei der Verarbeitung ihrer Daten setzt. Der Bereich technisch-organisatorischer Maßnahmen wird durch die Prinzipien des Privacy by Design, Privacy by Default und die Datenportabilität gestärkt.

Die DSGVO ist ein Meilenstein für einen einheitlichen und starken Datenschutz in der EU. Dabei geht es nicht nur um interne Regelungen eines Binnenmarktes von einer halben Milliarde Menschen. Die Regelungen haben darüber hinaus Auswirkungen auf alle Unternehmen, die von außen kommend Waren und Dienstleistungen auf diesem Markt anbieten wollen. Darüber hinaus beeinflussen sie über die Anforderungen zur internationalen Datenübermittlung positiv die Angemessenheit des Datenschutzniveaus in den Drittstaaten. Das gilt sowohl gegenüber dem privaten Sektor als auch gegenüber staatlichen Regelungen der Datenverarbeitung zur Gewährleistung der inneren Sicherheit. Hier werden rechtsstaatliche Mindeststandards für den Schutz der Rechte Betroffener gefordert, die künftig den Maßstab für die Zulässigkeit von internationalen Datenstransfers darstellen.

Besonderes Augenmerk legt die Neuregelung auf den einheitli-

chen Rechtsvollzug. Es ist klar, dass allein die Vereinheitlichung des Rechts wenig bewirkt, wenn das Recht in jedem Mitgliedstaat anders angewendet wird und sich Räume für Unternehmen bieten, am Ort der laxen Auslegungspraxis selbst bei schweren Datenschutzverstößen nichts befürchten zu müssen. Immer wieder haben sich in der Vergangenheit unterschiedliche Einschätzungen zur Rechtmäßigkeit der Datenverarbeitung durch die europäischen Datenschutzbehörden ergeben (vgl. etwa zur automatisierten Gesichtserkennung bei Facebook, 24. TB, S. 195). Mechanismen, diese verschiedenen Positionen zu einer gemeinsamen Bewertung aller europäischen Aufsichtsbehörden zusammenzuführen, gab es bislang nicht. Sie werden durch die DSGVO jedoch geschaffen. Insoweit trägt die Datenschutzgrundverordnung durch ein komplexes aufsichtsbehördliches Verfahren dazu bei, einheitliche Entscheidungen im Rechtsvollzug in der Europäischen Union zu erlangen.

Die Datenschutzgrundverordnung stellt künftig sicher, dass für jedes Unternehmen in der EU eine sogenannte federführende Aufsichtsbehörde mit Sitz an der Hauptniederlassung des jeweiligen Unternehmens zuständig ist (sog. One-Stop-Shop). Diese Regelung ermöglicht es Unternehmen, am Ort ihrer europäischen Zentrale ausschließlich mit einer einzigen Behörde statt mit 28 Behörden zu kommunizieren. Damit es nicht zu einem Unterlaufen von Datenschutzstandards kommt, wenn sich ein Unternehmen am Ort der vermeintlich schwächsten Aufsichtsbehörde ansiedelt, sieht die Datenschutzgrundverordnung eine zentrale Europäische Stelle vor, die künftig in streitigen Fragen die Befugnis hat, verbindliche Entscheidungen zu treffen: Darüber wird künftig durch ein neues Gemeinschaftsorgan, der Europäische Datenschutzausschuss wachen, der - und das ist ein Novum im Recht der Gemeinschaft - durch Behörden der Mitgliedstaaten konstituiert wird. Ein europäischer Datenschutzausschuss, der sich aus den Datenschutzbeauftragten aller Mitgliedstaaten rekrutiert, wacht künftig als höchstes Gremium des Datenschutzes auf europäischer Ebene darüber,

dass die Entscheidungen der federführenden Aufsichtsbehörden mit den Vorgaben der EU-Datenschutzgrundverordnung vereinbar sind. Für die Betroffenen ist es dann auch weiterhin möglich, sich mit Beschwerden an ihre nationalen Aufsichtsbehörden zu wenden, die diese dann in Kooperation mit den federführenden Behörden bearbeiten.

Deutschland wird wie bisher in der Art. 29-EU-Datenschutzgruppe durch zwei Vertreter, die Beauftragte bzw. den Beauftragten für Datenschutz und Informationsfreiheit des Bundes sowie eine Vertreterin bzw. einen Vertreter aus den Ländern repräsentiert werden. Die Ländervertretung wird künftig durch den Bundesrat bestimmt. Die Vertretung der Bundesländer in der Art. 29-EU-Datenschutzgruppe, dem bisherigen Zusammenschluss der Aufsichtsbehörden der Mitgliedstaaten, hat seit 2015 der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit inne (näher zur Tätigkeit unter V. 5).

Neben dieser neuen Architektonik aufsichtsbehördlichen Handelns werden künftig auch die Eingriffskompetenzen der Aufsichtsbehörden wesentlich geschärft. So erhalten diese künftig die Befugnis, Bußgelder in Höhe von bis zu 20 Millionen Euro oder, falls dieser Betrag höher ist, 4 % des jährlichen weltweiten Umsatzes eines Unternehmens zu verhängen. Gleichzeitig sind die Aufsichtsbehörden gegenüber öffentlichen Stellen wie regierungsmittelbaren Behörden oder der mittelbaren Staatsverwaltung befugt, rechtsverbindliche Anordnungen zu treffen, was deutlich über das bisher lediglich formale Instrument der Beanstandung bzw. der Rüge hinausgeht.

Der Katalog in Art. 57 Abs.1 lit a bis lit v sieht in Zukunft zahlreiche neue Aufgaben für die Aufsichtsbehörden vor, die bei der künftigen Behördenausstattung zu berücksichtigen sind. Hierzu zählen u.a. die Aufklärung und Sensibilisierung der Öffentlichkeit insbesondere über Risiken, die mit der Verarbeitung von Daten verbunden sind, die Ausarbeitung von

Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln sowie von Verhaltensregelungen und die Überwachung entsprechender Akkreditierungsverfahren.

Zur Ermittlung des Mehraufwands im Zuge der Umgestaltung der aufsichtsbehördlichen Tätigkeit haben die Aufsichtsbehörden der Länder den renommierten Datenschutzexperten Prof. Dr. Alexander Roßnagel von der Universität Kassel mit der Erstellung eines Gutachtens beauftragt. In seiner umfassenden Ausarbeitung hat dieser die künftigen Funktionen und die Bedeutung der Aufsichtsbehörden näher unter den Aspekten der Datenschutzprüfungen und -anordnungen, Kooperation in der Europäischen Union, Datenschutzkommunikation, Verfahrensmanagement, Justiziariat, Beschwerde- und Sanktionsstelle analysiert. Hinsichtlich der durchschnittlichen zusätzlichen Arbeitsbelastung anhand der Anforderungen der DSGVO wurde ein Mehrbedarf von jeweils 24 bis 33 Stellen für eine Behörde wie den HmbBfDI ermittelt (*http://suche.transparenz.hamburg.de/dataset/gutachten-zum-zusaetzlichen-arbeitsaufwand-fuer-die-aufsichtsbehoerden-der-laender-durch-d-2017*). Die angemessene Ausstattung mit personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ist eine Verpflichtung, die der europäische Gesetzgeber den Mitgliedsstaaten gemäß DSGVO auferlegt.

PRÜFUNGEN II.

1. Polizeiliche Datenverarbeitung auf dem Prüfstand

Auch in Zeiten der Gefährdung öffentlicher Sicherheit ist die polizeiliche Datenhaltung an Recht und Gesetz gebunden. Die hierzu durchgeführten datenschutzrechtlichen Prüfungen ergaben zahlreiche Defizite.

1.1 Einleitung

Im Berichtszeitraum 2016/2017 hat der HmbBfDI die polizeiliche Datenverarbeitung mehrmals auf den Prüfstand gestellt. Dabei ging es nicht nur um die Verarbeitung von personenbezogenen Daten in landeseigenen Dateien der Polizei Hamburg, die auf Grundlage des Polizeidatenverarbeitungsgesetzes (PolDVG) geführt werden. Betroffen waren auch Verbunddateien, also Dateien des polizeilichen Informationssystem (INPOL), die das Bundeskriminalamt (BKA) als Zentralstelle für den elektronischen Datenverbund zwischen Bund und Ländern gem. § 11 Abs. 1 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) führt und in die auch die Polizei Hamburg Daten liefert. Aus § 13 Abs.1 BKAG ergibt sich eine Pflicht der Landeskriminalämter, dem BKA erforderliche Informationen zur Erfüllung seiner Aufgaben als Zentralstelle zu übermitteln. Zur Erfüllung dieser Pflicht haben die Landeskriminalämter im automatisierten Verfahren Daten in das polizeiliche Informationssystem einzugeben.

Die datenschutzrechtliche Verantwortung für Speicherungen in landeseigenen Dateien liegt gem. § 10 Abs. 1 HmbDSG bei der Polizei Hamburg. Für die im polizeilichen Informationssystem gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten, trägt die Behörde, die die Daten eingegeben hat (§ 12 Abs. 2 BKAG), somit also die Polizei Hamburg, die Verantwortung. Die Datenschutzkontrolle der landeseigenen Dateien obliegt gem. § 23 HmbDSG

dem HmbBfDI. Die Datenschutzkontrolle der Verbunddateien obliegt nach § 24 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) zwar primär der Bundesbeauftragten für den Datenschutz (BfDI). Allerdings können die von den Ländern in das polizeiliche Informationssystem eingegebenen Datensätze auch von den jeweiligen Landesbeauftragten für den Datenschutz im Zusammenhang mit der Wahrnehmung ihrer Prüfungsaufgaben in den Ländern kontrolliert werden, soweit die Länder die datenschutzrechtliche Verantwortung für die im polizeilichen Informationssystem gespeicherten Daten haben. Dies folgt aus § 12 Abs. 3 BKAG.

In diesem Sinne hat der HmbBfDI die Verarbeitung von personenbezogenen Daten in der landeseigenen Datei „CRIME Gruppen- und Szenegewalt" und im polizeilichen Auskunftssystem POLAS geprüft, wobei letztere im Zusammenhang mit der Datenverarbeitung während des Akkreditierungsverfahrens für den G-20 Gipfel im Berichtszeitraum noch nicht abgeschlossen ist, aber bereits zum diesem Zeitpunkt erste Ergebnisse vorgetragen werden können (mehr hierzu unter II. 2).

Bei den Verbunddateien wurde die Datei „Gewalttäter Sport" sowie die Rechtsextremismusdatei (RED) geprüft. Dabei haben die Prüfungen zahlreiche schwere datenschutzrechtliche Mängel offenbart.

1.2 CRIME Gruppen und Szenegewalt

In der landeseigenen Datei „CRIME Gruppen- und Szenegewalt" wurde neben den materiell-rechtlichen Speichervoraussetzungen in den Personenrollen Beschuldigte, Verdächtige und Kontakt- und Begleitpersonen auch die Einhaltung der Lösch-, Prüf- und Speicherfristen geprüft.

Mit Stichtag 21.01.2016 waren 4.358 Personen in der Datei in den Rollen Beschuldigte, Verdächtige, Kontakt- und Begleitpersonen, Störer sowie Störer-Waffen gespeichert.

Davon wurden im Laufe der Prüfung rund 4.000 Personen gelöscht. Mit Stichtag 03.05.2016 waren in der Datei nur noch 564 Personen eingetragen.

Im Ergebnis

- enthielt die Datei Szeneangehörige, für die eine Zuständigkeit der zugriffsberechtigten Stellen schon seit längerem nicht mehr bestand, so dass es an der Erforderlichkeit der Speicherung bei den datenführenden Dienststellen fehlte. Dies betraf etwa Personen aus den Bereichen Punker, Skinheads, Rocker und russische Aussiedler. Der Verbleib eines großen Teils der Papierakten hierzu war bislang nicht zu klären.
- bei einem nicht unerheblichen Teil der Verdächtigen und Beschuldigten konnte die Erforderlichkeit der Speicherung nicht positiv festgestellt werden.
- in der Datei waren zahlreiche Kontakt- und Begleitpersonen gespeichert, obwohl die gesetzlich festgelegte Speicherdauer von drei Jahren (vgl. § 16 Abs. 3 S. 2 Gesetz über die Datenverarbeitung der Polizei, PolDVG) überschritten war. Eine Löschroutine für diesen Personenkreis – trotz maximaler Speicherfrist – war technisch nicht hinterlegt und wurde auch nicht manuell ausgeführt.
- schließlich waren auch personenbezogene Daten einer minderjährigen Person gespeichert, die nach Maßgabe der zugrundeliegenden Errichtungsanordnung aufgrund ihres Alters gar nicht in die Datei hätte aufgenommen werden dürfen.

Dies hat der HmbBfDI formell gegenüber dem Senator der Behörde für Inneres und Sport beanstandet. Die Beanstandung hat letztlich dazu geführt, dass die CRIME-Datei „Gruppen und Szenegewalt" in ihrer ursprünglichen Form nicht mehr fortgeführt wird. Daten aus dieser Datei, die für die Aufgabenerfüllung der Polizei weiterhin erforderlich sind, wurden hingegen in die neu errichtete CRIME-Datei „Türstehergewalt" und CRIME-Datei Sportgewalt überführt.

1.3 Verbunddatei „Gewalttäter Sport“

Im Nachgang zu dieser Prüfung hat der HmbBfDI eine ausgewählte Stichprobe von Personen, die in der Verbunddatei „Gewalttäter Sport“ gespeichert sind, geprüft. Hintergrund und Anlass für die Prüfung war die zuvor veranlasste Prüfung der landeseigenen CRIME-Datei „Gruppen- und Szenegewalt“ beim Landeskriminalamt Hamburg (LKA). Bei dieser Prüfung stellte der HmbBfDI fest, dass ein Teil der Stichprobe aus dem Bereich Sportgewalt auch in der Verbunddatei „Gewalttäter Sport“ beim Bundeskriminalamt (BKA) gespeichert war. Im Rahmen dieses Kontrollbesuches hatte uns die Polizei Hamburg mitgeteilt, dass sie beabsichtige, eine landeseigene „Sportgewalt“ Datei zu erstellen. Es stellte sich daher die Frage, ob eine landeseigene Sportgewalt-Datei neben der Verbunddatei geführt werden darf. Möglicherweise könnte es sich hierbei um eine unzulässige Doppelspeicherung handeln. Mit einer aus der CRIME-Datei „Gruppen- und Szenegewalt“ gezogenen Stichprobe von 23 Personen sollte diese Frage überprüft werden.

Die Frage der unzulässigen Doppelspeicherung konnte im Ergebnis verneint werden, da beide Dateien über unterschiedliche Speichervoraussetzungen verfügen und unterschiedlichen Zwecken dienen. Während es sich bei der CRIME-Datei um eine Fallbearbeitungsdatei handelt, dient die Verbunddatei der Information länderübergreifend. Im letzteren Fall handelt sich um eine Datei, die rein präventiven Zwecken der konkreten Gefahrenabwehr durch Information der Einsatzkräfte vor Ort dient. Gegen eine unzulässige Doppelspeicherung spricht weiterhin, dass beide Dateien über unterschiedliche Zugangsberechtigungskonzepte – wobei das der CRIME-Datei sehr eng gefasst ist – verfügen.

Unabhängig hiervon wurde bei der auf insgesamt 53 gespeicherte Personen erweiterten Stichprobe auch die Speicherdauer genauer geprüft. Zwar werden die Daten aus der

Verbunddatei systemseitig automatisch nach Ablauf der maximalen fünfjährigen Speicherdauer gelöscht; gleichwohl kann eine Löschung auch schon vor Ablauf dieser Frist notwendig sein z.B. bei der Einstellung von Ermittlungsverfahren. Eine systematische Prüfung und sich hieraus eventuell ergebende Löschung solcher vorzeitig zu löschenden Daten findet jedoch nicht statt; dies wird von uns weiterverfolgt werden.

1.4 Verbunddatei „Rechtsextremismus“

Als weitere Verbunddatei hat der HmbBfDI die vom Bundesverfassungsgericht geforderte und zwischenzeitlich gesetzlich verankerte Prüfung der Rechtsextremismusdatei (RED) in Abständen von zwei Jahren gem. § 11 Abs. 2 REDG beim LKA 7 (Staatsschutz) abgeschlossen.

Im Gegensatz zu der Prüfung der Antiterrordatei (vgl. 25. TB. IV. 1.4) hat sich die Protokollierung zwischenzeitlich auf ein Maß reduziert, das eine datenschutzrechtliche Kontrolle zulässt. Aus den Protokollen hat sich allerdings keine Auffälligkeit in der Nutzung der RED gezeigt. Problematisch hingegen waren die Speicherungen selbst. Zwar konnte das LKA 7 bei allen noch in der RED gespeicherten Personen detailliert darlegen, welche Erkenntnisse zu den überprüften Personen vorlagen, die eine Speicherung in der RED begründen. Allerdings stellte der HmbBfDI wiederholt fest, dass die Ausgänge des Strafverfahrens nicht oder nicht zeitnah in die RED eingepflegt wurden. Dies betrifft insbesondere Fälle, in denen eine Aufnahme in die RED erfolgte, weil die Betroffenen als Täter oder Teilnehmer einer rechtsextremistischen Gewalttat Beschuldigte sind (§ 2 Abs. 1 Nr. 1 b REDG). Sobald diese Voraussetzung nicht mehr vorliegt, müssen diese Personen aus der RED gelöscht werden.

2. Datenverarbeitung im Zusammenhang des G20-Gipfels

Die polizeiliche Arbeit beim G20-Gipfel hat auch in datenschutzrechtlicher Hinsicht zahlreiche Probleme und Fragestellungen aufgeworfen.

Die datenschutzrechtliche Aufarbeitung beim G20-Gipfel im Juli 2017 hat für einen sehr hohen Prüfungsaufwand gesorgt und erheblich Ressourcen beim HmbBfDI gebunden.
Der nachträgliche Entzug der Akkreditierung von Journalisten bildete dabei ebenso einen Schwerpunkt wie die grundlegende Datenverarbeitung bei Polizei und Verfassungsschutz, die die Grundlage für die Erteilung sowie für den Entzug der Akkreditierung bildete.

2.1 Einleitung

Sämtliche Personen (u.a. Journalisten, Sicherheitspersonal, Rettungssanitäter, Service-Mitarbeiter, etc.), die am 07. und 08.07.2017 eine Berechtigung zum Zugang zu der Sicherheitszone 1 haben wollten, wurden aufgrund einer zuvor erteilten Einwilligung durch das Bundespresseamt/Presse- und Informationsamt der Bundesregierung (BPA) unter Hinzuziehung des Bundeskriminalamtes (BKA) einer Überprüfung zu Zwecken des Personenschutzes gemäß § 5 Bundeskriminalamtsgesetz (BKAG) unterzogen. Zusätzlich zu der Akkreditierung konnten Journalisten für sogenannte geführte Pressetermine innerhalb der Sicherheitszone 1 (sog. Pools) gesonderte Poolcards beantragen.
Für die Akkreditierung von Journalisten war das BPA federführend zuständig, für die Akkreditierung der Service-Mitarbeiter das BKA. Das BKA führte für eigene Bedarfe und für das BPA Personenüberprüfungen zum Zwecke des Personenschutzes unter Beteiligung weiterer Sicherheitsbehörden durch.

Diese Personenüberprüfung beinhaltete neben einer Abfrage in polizeilichen Dateien des BKA eine gesonderte Abfrage bei der Polizei Hamburg u.a. in dem Vorgangsverwaltungssystem ComVor-Index und dem polizeilichen Auskunftssystem POLAS sowie Abfragen beim Bundesamt für Verfassungsschutz (BfV) im Nachrichtendienstlichen Informationssystem (NADIS WN), dem Datenverbundsystem, an dem die Verfassungsschutzbehörden des Bundes und der Länder beteiligt sind. Stellte sich im Akkreditierungsverfahren heraus, dass Informationen in NADIS WN nicht vom BfV, sondern von einem anderen Bundesland eingemeldet waren, wurde der Nachrichtengeber im Verfassungsschutzverbund im Einzelauskunftsverfahren über NADIS WN beteiligt. So auch das Landesamt für Verfassungsschutz Hamburg (LfV Hamburg).

In diesem Zusammenhang hat das BKA ab dem 22. Mai 2017 der Polizei Hamburg über 21.000 Personendaten übermittelt. Die Polizei Hamburg hat diese Personendaten per Massendatenverfahren mit dem Datensatz aus POLAS sowie rückwirkend für das letzte Jahr mit dem Datensatz aus ComVor-Index automatisiert abgeglichen. Dabei wurden bei ca. 850 Personen Treffer in den beiden Dateien erzielt. Die Daten dieser Personen hat das LKA Hamburg, ohne die Rechtmäßigkeit der Speicherungen zu prüfen, an das BKA übersandt.

Beim LfV Hamburg hingegen wurden insgesamt zu 55 Personen Datensätze abgefragt. Dabei handelte es sich um Personen, zu denen das LfV Hamburg Erkenntnisse in NADIS WN gespeichert hatte. Das LfV Hamburg sollte bei diesen Personen beurteilen, ob Erkenntnisse im Sinne eines vom BKA vergebenen Kriterienkatalogs vorlagen. Als relevante Erkenntnisse („Kriterien“) sollten nur solche herangezogenen werden, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass die zu akkreditierende Person beispielsweise „einer gewaltbereiten Bewegung angehört oder eine solche nachdrücklich unterstützt“ oder aber „sonstige Sicherheitsbeden-

ken bestehen“. Bei insgesamt 30 Personen übermittelte das LfV Hamburg keine Daten an das BfV. In insgesamt 25 Fällen lagen dem LfV Erkenntnisse im Sinne des Kriterienkatalogs vor, die dem BfV schließlich übermittelt wurden.

Die Entscheidung, die Akkreditierung zu erteilen, oblag allein dem BKA. Die Polizei Hamburg und das LfV Hamburg waren bei der Entscheidung lediglich mitwirkende Behörden.
Trotz vorliegender Sicherheitsbedenken entschieden das BKA und BPA offensichtlich, allen Personen eine Akkreditierung zu erteilen. Dabei wurde bei den Journalisten eine Abwägung zwischen dem Rechtsgut der Pressefreiheit und der zu gewährleistenden Sicherheit der Gipfelteilnehmer vorgenommen, die zugunsten der Pressefreiheit ausfiel.

Aufgrund der räumlichen Gegebenheiten vor Ort und der Dynamik des Gipfelgeschehens (angekündigter Action Day am 07.07.2017 zur Störung des Gipfelverlaufs) wurde die Sicherheitslage neu beurteilt. Aus Sicht des BKA konnte offenbar nicht mehr sichergestellt werden, dass die trotz nunmehr bestehender Sicherheitsbedenken akkreditierten Journalisten von Pool-Terminen mit Schutzpersonen ausgeschlossen werden konnten. Dies galt insbesondere für Termine in den Delegationshotels, in denen eine elektronische Überprüfung der Akkreditierung nicht möglich war. Aufgrund der Vielzahl der Pool-Termine über den gesamten Gipfelverlauf war die Situation aus Sicht des BKA nicht kontrollierbar und ein störungsfreier Verlauf der Medientermine nicht mehr zu gewährleisten. Daraufhin entschieden das BPA und BKA, denjenigen Personen die Akkreditierung und die Poolcards zu entziehen, zu denen sicherheitsrelevante Erkenntnisse vorlagen.

Zur Umsetzung dieser Entscheidung hat das BKA verschiedene Listen erstellt mit Namen von Journalisten und Service-Mitarbeitern, zu denen bereits im Vorfeld des G20-Gipfels (erhebliche) Sicherheitsbedenken bestanden haben. Dabei

handelte es sich um zwei Listen mit jeweils 82 Personen, die sich lediglich dadurch unterschieden, dass auf der einen Liste Name, Vorname und Geburtsdatum der Personen gelistet war, denen nachträglich die Akkreditierung entzogen werden sollte. Die zweite Liste enthielt zusätzliche Informationen wie z.B. auch das Datum des Vermerks sowie der Entscheidung, das Votum zur Personenüberprüfung und den Hinweis, ob Erkenntnisse des BfV vorliegen. Die Personen auf beiden Listen waren allerdings identisch. Beide Listen wurden der Polizei Hamburg übermittelt. Zusätzlich wurde eine dritte Liste übermittelt. Dabei handelte es sich um eine Gefährderliste mit 35 Personeneinträgen, wobei drei Personen doppelt aufgelistet waren. Diese Liste enthielt neben Namen, Vornamen, Geburtsdatum und Geburtsort auch Personengebundene Hinweise (PHW) wie z.B. politische motivierte Kriminalität Links (PMK-links). Eine Liste mit ausschließlich Journalisten, wie zunächst in der Presse berichtet, wurde nach Informationsstand des HmbBfDI jedoch nicht übermittelt.

Auch wenn die Bundesregierung sowie das BKA im Nachgang zum G20-Gipfel sich dahingehend äußerten, dass auch das LKA selbst entsprechende Listen erstellt habe, konnte sich der HmbBfDI anhand des vorgelegten E-Mail-Verkehrs durch die Polizei Hamburg vergewissern, dass sämtliche Listen vom BKA übersandt wurden. Auch die Polizei Hamburg bestätigte diese Aussage, wonach sie eigenständig keine Liste angefertigt habe.

Anhand dieser Listen erfolgte schließlich am 07.07.2017 und zum Teil am 08.07.2017 eine Kontrolle auch durch Mitarbeiterinnen und Mitarbeiter von Polizeieinheiten verschiedener Bundesländer unter anderem an den Zugangspunkten zur Sicherheitszone 2. Hierbei kam es zu der Situation, dass die kontrollierenden Polizeibeamten derart offen mit den Listen umgingen, dass dritte Personen leicht in der Lage waren, sich Einblick in die Listen zu verschafften und diese auch filmen konnten.

Aufgrund der Listen vom BKA wurde schließlich neun Journalisten die Akkreditierung entzogen.

Der HmbBfDI hat im Nachgang versucht nachzuvollziehen, wie diese Listen an die kontrollierenden Polizeibeamten gelangten, konnte dies aber nicht mehr lückenlos rekonstruieren. Die Aufklärung gestaltete sich – auch aufgrund der divergierenden Aussagen des LKA Hamburg und dem BKA – schwierig. Fest steht allerdings, dass sich erst am Abend des 07.07.2017 herausstellte, dass die Listen nur zur internen Verwendung im BKA und der BAO Hanse (Besondere Aufbauorganisation Hanse des BKA) bestimmt waren.

2.2 Umgang mit den Listen nach Entzug von Akkreditierungen während des G20-Gipfels am 07. und 08.07.2017 in Hamburg

Der Kontrollumfang des HmbBfDI umfasste zunächst die Prüfung, wer die datenschutzrechtliche Verantwortung für den Umgang mit den Listen der Personen, denen die Akkreditierung entzogen werden sollte, im Rahmen der Vorortkontrolle zu tragen hatte.

Die Untersuchung hat ergeben, dass die beteiligten Behörden im Umgang mit den Listen offenbar am 7. Juli nicht in der Lage waren, ein geordnetes Verfahren und damit auch die erforderlichen organisatorischen Maßnahmen zum Datenschutz einzuhalten. So lässt sich nur unscharf rekonstruieren, welche Listen zu welcher Zeit von welcher Stelle erstellt wurden. Erschwert wird die Analyse des Geschehens dadurch, dass Teile des Sachverhalts offenbar von der Polizei Hamburg und dem BKA in der Nachbetrachtung unterschiedlich gesehen und bewertet wurden.

Das sicherheitsbehördliche Handeln bei der Kontrolle des Zugangs hatte sich im Verlauf des G20-Gipfels offenbar verselbständigt. Für die Überwachung und den Schutz der Messe

als zentralen Austragungsort der Gipfelgespräche wurde eine Reaktionskette in Gang gebracht, bei der ein planvolles Zusammenwirken der zum Schutz des Gipfels eingesetzten Ordnungskräfte zwischen BKA und Polizei Hamburg nicht mehr gelang. Statt klarer Absprachen und der Verfolgung eines gemeinsamen Konzepts ist es hier zu einem eher sporadischen, durch einzelne Beamte ausgelösten, weitgehend improvisierten Kontrollszenario gekommen.

Das Außerachtlassen der Sorgfaltsanforderungen des Datenschutzes im Zuge der Kontrollsituation vor Ort durch anwesende Polizeikräfte liegt im gesetzlich verankerten Verantwortungsbereich der Polizei Hamburg. Das Kursieren entsprechender Sperrlisten und deren Handhabung, die einen Einblick unbefugter Dritter ermöglichte, hatte für die kontrollierten Personen eine subjektiv deutlich stigmatisierende und wohl auch einschüchternde Wirkung. So sahen sich die auf eine Zulassung zum Ort der Berichterstattung angewiesenen Journalisten in einer Situation, dass Sperrlisten mehr oder weniger offen kursierten, bei denen der einzelne Betroffene nicht wissen konnte, ob sich der eigene Name darauf befindet und ob er mit einer Einsichtnahme durch dritte Personen, insbesondere andere Kollegen rechnen musste.

Der HmbBfDI kommt in seiner Prüfung zu dem Ergebnis, dass gegen § 8 Hamburgisches Datenschutzgesetz (HmbDSG) verstoßen wurde, da keine organisatorischen Maßnahmen ergriffen wurden, um die Kenntnisnahme durch die Journalisten zu verhindern, indem die Listen vor Ort so gehalten wurden, dass dritte Personen bzw. die Kontrollierten Einblick nehmen und diese filmen konnten und hierbei die auf der Liste enthaltenen personenbezogenen Daten zur Kenntnis genommen haben.

2.3 Prüfung der Datenübermittlung vom LKA zum BKA

Der HmbBfDI prüft darüber hinaus derzeit bei einer ausgewählten Stichprobe der ca. 850 Treffer, zu denen die Polizei

Hamburg Erkenntnisse an das BKA übermittelt hat, ob die Voraussetzungen für die Speicherung in POLAS vorliegen. Diese Datei dient der Gefahrenabwehr, einschließlich der vorbeugenden Bekämpfung von Straftaten, und der Aufklärung von Straftaten. Voraussetzung für die Speicherung gem. § 16 Abs. 2 S. 3 PolDVG und der Errichtungsanordnung der Datei ist u.a. das Vorliegen eines strafrechtlichen Ermittlungsverfahrens und einer Negativprognose. Die Polizei muss hinreichend darlegen, dass eine Speicherung aufgrund der Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen sowie der Besorgnis der Begehung weiterer Straftaten erforderlich ist. Ebenso wichtig ist der Ausgang des Strafverfahrens, denn die Nutzung von Strafverfolgungsdaten für Gefahrenabwehrzwecke muss beendet werden, wenn der durch das Ermittlungsverfahren gerechtfertigte Verdacht entfällt (vgl. § 16 Abs. 2 S. 4 PolDVG). Diese Voraussetzungen müssen kumulativ vorliegen. Liegt eine der Voraussetzungen nicht vor, so ist die Speicherung rechtswidrig.

Der HmbBfDI hat bisher zwei Vorortprüfungen wahrgenommen und die Datensätze zu 13 Personen geprüft, wobei zu 10 Personen Einträge nicht nur in ComVor Index, sondern in POLAS bzw. in INPOL gespeichert sind. Ein weiterer Teil der Stichprobe wird derzeit im schriftlichen Verfahren geprüft.

Hierbei konnte der HmbBfDI bereits feststellen, dass

- bei einem nicht unwesentlichem Teil der geprüften, in POLAS bzw. INPOL gespeicherten, Fälle die erforderliche Negativprognose nicht oder nicht ausreichend vorlag bzw. nicht ausreichend dokumentiert wurde – zum Teil fanden sich floskelartige Negativprognosen wieder („es ist nicht auszuschließen, dass der Betroffene zukünftig wieder in Erscheinung treten wird“);
- der Ausgang des Strafverfahrens bei mehreren Einträgen nicht berücksichtigt wurde, wobei zu diesem Zeitpunkt unklar ist, ob dies auf organisatorische Mängel zurückzuführen ist oder aber darauf, dass die nach § 482 Absatz 2

Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieben ist.

2.4 Prüfung der Datenübermittlung vom LfV zum BfV

Auch beim LfV Hamburg hat der HmbBfDI die Datenübermittlung zu den bereits genannten 25 Personen an das BfV zwecks Akkreditierung überprüft. Die Prüfung wurde zwischenzeitlich abgeschlossen. Schwerwiegende Datenschutzverstöße konnte der HmbBfDI nur in einem Fall feststellen. Hierbei handelte es sich um einen Medienvertreter, bei dem die Voraussetzungen für die Speicherung nach dem Hamburgischen Verfassungsschutzgesetz (HmbVerfSchG) nicht vorlagen. Dies hat das LfV Hamburg bereits gegenüber dem Betroffenen eingeräumt. Der HmbBfDI hat sich im Nachgang die Belegstücke, die dem LfV Hamburg zu der Speicherung vorlagen, geprüft und dabei festgestellt, dass keine verfassungsfeindlichen Bestrebungen gemäß § 4 HmbVerfSchG vorlagen, die eine Speicherung des Medienvertreters rechtfertigen.

2.5 Fazit

Insgesamt haben die Geschehnisse um den Entzug der Akkreditierung sowie die Prüfungen zu den polizeilichen Dateien (siehe dazu II 1) gezeigt, dass die Datenhaltung bei der Polizei Hamburg defizitär ist und häufig den rechtlichen Anforderungen nicht gerecht wird. Ähnliche Prüfungen, die von Bundes- sowie Landesdatenschutzbeauftragten in ihrem Zuständigkeitsbereich durchgeführt wurden (vgl. u.a. Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Kühlungsborn, den 10. November 2016 „Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf - Konsequenzen für polizeiliche Datenverarbeitung notwendig“ *https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/92DSK_FalldateiRauschgift.html*), sowie der Bericht eines betroffenen Journalisten zum Entzug der Akkreditierung haben bestätigt, dass es sich hierbei um ein

übergreifendes bundesweites Defizit handelt, das auf strukturelle Fehler zurückzuführen sein dürfte. Insoweit ist eine bundesweite kontinuierliche Überprüfung durch die zuständigen Datenschutzbehörden alternativlos.

Die politische Forderung nach einem Aufweichen des Trennungsgebots zwischen Nachrichtendiensten und Polizei sowie einer Herabsetzung der Speichervoraussetzung (Abschaffung der Negativprognose), um die Datenhaltung der Sicherheitsbehörden künftig zu erleichtern, ist zurückzuweisen. Dies ist weder mit rechtstaatlichen Grundsätzen noch mit den Grundrechten der betroffenen Bürgerinnen und Bürger vereinbar. Auch und gerade in Zeiten erhöhter Bedrohung der inneren Sicherheit sind Polizei und Nachrichtendienste an rechtstaatliche Vorgaben und die Gesetze gebunden. Dies auch unter schwierigen Bedingungen einzuhalten, ist Wesenskern des Rechtsstaats.

Nach alledem wird die Polizei Hamburg große Anstrengungen unternehmen müssen, in Zukunft die Datenhaltung datenschutzrechtlich zu optimieren. Dies wurde durch die Polizei bereits öffentlich angekündigt. Laut Pressemitteilung der Polizei Hamburg vom 19.10.2017 geht es um etwa 160 000 Einzelpersonen und ein Gesamtvolumen von 900 000 Datensätzen in der Datei POLAS. Der Datenbestand solle so bereinigt werden, dass er den „datenschutzrechtlichen Anforderungen gerecht wird und andererseits die Ermittlungen der Polizei im Hinblick auf Kapitaldelikte, Abwehr terroristischer Gefahren und Umgang mit Sexualstraftätern nicht gefährdet“ (siehe hierzu *https://www.abendblatt.de/hamburg/article212286177/Nach-G20-Akkreditierungsentzug-Pruefprozess-von-Daten.html*).

Die Bereitschaft zur Überprüfung des Datenbestandes ist nachhaltig zu begrüßen und muss nun zügig und konsequent umgesetzt werden. Der HmbBfDI wird dieses Vorhaben wei-

terhin konstruktiv begleiten und über den Fortgang dieser Entwicklung berichten.

3. Feuerwehr: Schutz von Funkdaten erst nach dem 2. Vorfall

Im Zuge der Einsatzalarmierung werden Notfalldaten der Feuerwehr unverschlüsselt übertragen und können mitgeschnitten werden. Erst nachdem solche illegalen Funkmitschnitte im Internet veröffentlicht wurden, kündigt die Feuerwehr eine technische Teil-Lösung für 2018 an.

Im September 2016 haben wir die Information erhalten, dass die Feuerwehr Hamburg personenbezogene Daten, die Bürgerinnen und Bürger betreffen und die bei der Alarmierung von Rettungswagen, Notarztwagen usw. dorthin übertragen werden, per Funk unverschlüsselt an diese Empfänger übermittelt. Soweit Bürgerinnen und Bürger Hilfe benötigen, umfasst der Inhalt dieser Alarmierungen auch konkrete Informationen über z.B. die betroffenen Hilfebedürftigen; neben dem Einsatzort werden hierbei auch beispielsweise Namen und erste (Verdachts-)Diagnosen übermittelt. Diese Funkübertragungen wurden von Unbefugten abgehört, die diese sensiblen personenbezogenen Daten 2016 und nochmals im Frühjahr 2017 im Internet allgemein zugänglich veröffentlichten. Unter der Angabe der Straße und der Hausnummer, dem Alter der Person konnte man dort zum Beispiel die Information lesen „drohende Geburt (=> 5 Monate/20 Wochen)“.

Der Hintergrund: Die Feuerwehr Hamburg arbeitet seit den frühen neunziger Jahren mit einem Digitalen Alarmierungssystem, in das auch die Freiwilligen Feuerwehren und die Rettungsdienste eingebunden sind. In den 2000er Jahren wurde dieses System überarbeitet, so dass seitdem auch die Voraussetzungen dafür bestehen, eine 128-Bit-Verschlüsselung

einführen zu können. Die Feuerwehr hat die dafür erforderliche Neubeschaffung von verschlüsselungsfähigen digitalen Meldeempfängern jedoch nicht getätigt. Auch eine Umstellung der Einsatzalarmierung auf TETRA-BOS-Digitalfunk, den Standard für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, wurde zwar frühzeitig angedacht, unterblieb aber, obwohl die Feuerwehr Hamburg seit 2014 das BOS-Digitalfunknetz vollumfänglich nutzt.

Im Zuge des ersten illegalen Abhörvorfalles und der Veröffentlichung der Notfalldaten im Internet hat die Feuerwehr als erste Maßnahme den übertragenen Datensatz gekürzt. Bei der Einsatzalarmierung werden aktuell die Alarmart, der Einsatzort und die Kurzbezeichnung der alarmierten Ressource übertragen. Trotz dieser Kürzung sind auch diese weiterhin unverschlüsselt übertragenen Daten personenbezogen und enthalten sensible Inhalte.

Bereits im September 2016 haben wir der Feuerwehr unter Verweis auf § 8 Abs. 2 Hamburgisches Datenschutzgesetz (HmbDSG) die gesetzliche Forderung aufgezeigt, dass jede Daten verarbeitende Stelle diejenigen technischen Maßnahmen ergreifen muss, die gewährleisten, dass u.a. nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Vertraulichkeit). Eine Übertragung personenbezogener Daten setzt als Maßnahme voraus, dass ein dem jeweiligen Stand der Technik entsprechendes Verschlüsselungsverfahren eingesetzt wird. Ohne eine solche Verschlüsselung ist nicht sichergestellt, dass nur Befugte Kenntnis von den übertragenen Daten erlangen können.

Trotz dieser gravierenden Gefährdung, die nicht zuletzt der zweite Vorfall im Mai 2017 eines unbefugten Abhörens und einer unzulässigen Veröffentlichung der Daten im Internet belegt, sah die von der Feuerwehr zunächst vorgestellte Planung vor, dass die Realisierung einer Verschlüsselung nicht vor

2019 möglich sei, bei dem von der Feuerwehr favorisierten technischen Ansatz der Nutzung von TETRA-BOS-Digitalfunk nicht vor 2020.

Dem HmbBfDI ist bewusst, dass eine hinreichend präzise Alarmierung der Einsatzkräfte für das Wohlergehen oder sogar Überleben von Bürgerinnen und Bürgern äußerst wichtig ist. Das bedeutet aber nicht, dass dadurch gesetzlich erforderliche Maßnahmen zum Schutz des informationellen Selbstbestimmungsrechts beliebig mit ungewissem zeitlichen Horizont in die Zukunft geschoben werden können. Wir haben daher intensiv darauf gedrängt, dass angesichts des real stattfindenden unbefugten Abhörens und der Veröffentlichung sensibler personenbezogener Notfalldaten deutlich schneller eine hinreichend sichere Verschlüsselung der Daten gewährleistet werden muss. Die Feuerwehr hat uns zwischenzeitlich über das Ergebnis von Gesprächen mit den Softwareherstellern informiert; hiernach solle eine Lösung nunmehr im 2. Quartal 2018 technisch realisiert sein. Dazu sollen modernere Digitale Meldeempfänger genutzt werden, die im Zuge der Ersatzbeschaffung bei der Feuerwehr bereits vorhanden sind. Dies sind jedoch nur ca. 300 Geräte. Wir halten es für unabdingbar, dass alle mit der Erstversorgung befassten Einheiten und Personen bis Mitte 2018 mit den erforderlichen modernen Digitalen Meldeempfängern ausgestattet werden. Die Details und Einschränkungen der geplanten Zwischenlösung der Feuerwehr liegen uns jedoch bis zum Redaktionsschluss nicht vor.

4. HERAKLES reloaded – Langer Weg der Kasse.Hamburg zu einem sicheren Verfahren

6600 Beschäftigte konnten ohne Anlass in den über 2 Millionen Kontenstammdatensätzen des Buchhaltungsprogramms der FHH frei suchen. Mittlerweile wurden die Zugriffsberechtigungen auf das erforderliche Maß beschränkt und die Anlässe der Suche werden festgehalten. Aber noch sind nicht alle Mängel beseitigt.

Unsere Prüfung des IT-Verfahrens HERAKLES hatte 2015 ergeben, dass die Zugriffsregelungen nicht den Anforderungen des § 8 Abs. 2 Hamburgisches Datenschutzgesetz (HmbDSG) entsprechen (vgl. 25. TB, VIII 2.2). In einer Pressemitteilung der zuständigen Finanzbehörde zu unserem 25. TB, in dem wir die Zahl der Zugriffsberechtigten auf ca. 5000 geschätzt hatten, wurde lediglich eine Zahl von „rund 1700“ eingeräumt, die dann aber deutlich nach oben korrigiert werden musste (vgl. auch Bericht im Hamburger Abendblatt vom 27./28.02.2016 „Behörde wehrt sich: Datenschützer ignoriert Realität“). Wir hatten mehrfach nachhaken müssen, um endlich verlässliche Zahlen zu erhalten. Tatsächlich konnten 6600 Beschäftigte der Behörden und Ämter im Februar 2016 eine freie Suche nach Personen („Geschäftspartnern“) durchführen und sich zu einem Datensatz Name, Vorname, Anschrift, Geschäftspartnernummer und - soweit gespeichert – Kontoverbindungen anzeigen lassen. Damit waren wir mit unserer ursprünglichen Angabe nicht unwesentlich unter der faktischen Zahl der Zugriffsberechtigten zurückgeblieben.

Fast drei Jahre nach den ersten Eingaben von Beschäftigten der FHH, die uns über diesen Missstand berichtet hatten, konnten wir mit der Finanzbehörde wichtige technische Maßnahmen vereinbaren, um die erheblichen Mängel zu reduzieren:

- Für den überwiegenden Teil der Nutzer wurde die Suche so verändert, dass sie über den Formularserver erfolgt und nun immer die Dokumentenart und der Zahlungsgrund eingegeben werden müssen und protokolliert werden. Die freie Suche hat sich für einen großen Teil der Nutzer als nicht erforderlich herausgestellt und wurde für die Anwender in den Behörden und Bezirken gesperrt.
- Die Zahl der Personen, die über die Möglichkeit der freien Suche verfügen, konnte so von 6600 auf 455 im Oktober 2017 reduziert werden. Unsere Nachfrage bei Behörden, die eine augenscheinlich überdurchschnittliche Zahl von Zugriffsberechtigten aufwiesen, hat im November 2017 dazu geführt, dass nach internen Überprüfungen weitere Zugriffsberechtigungen gelöscht wurden, weil für die Aufgabenstellung eine freie Suche nicht erforderlich ist.
- Wir haben der Kasse.Hamburg wiederholt deutlich gemacht, dass auch Suchanfragen bei der freien Suche protokolliert werden müssen, damit der Grund für die Nutzung nachvollziehbar ist. Anders lässt sich die Revisionsfähigkeit nach § 8 Abs. 2 Nr. 5 HmbDSG nicht gewährleisten. Im November 2017 haben wir von der Kasse.Hamburg die Nachricht erhalten, dass die Protokollierung der freien Suche in den Behörden und bei der Kasse Hamburg voraussichtlich im ersten Quartal 2018 realisiert werden soll.

Seit nunmehr drei Jahren setzen wir uns intensiv dafür ein, dass im IT-Verfahren Herakles die Anforderungen des Datenschutzes eingehalten werden. Fortschritte konnten wir zwar erreichen. Dennoch ist unter dem Strich zu beklagen, dass es deutlich zu lange gedauert hat, bis die Kasse.Hamburg den Weg zu mehr Datenschutz eingeschlagen hat. Dem Stellenwert des Datenschutzes muss in der Praxis eine höhere Bedeutung zukommen. Dies gilt nicht zuletzt vor dem Hintergrund des Inkrafttretens der EU-DSGVO ab Ende 2018. Die Aufwertung technisch-organisatorischer Maßnahmen und der Befugnisse der Datenschutzaufsichtsbehörden sollte hierzu hinreichenden Anlass bieten.

5. Kinder und Jugendliche besser schützen mit sicherem E-Mail-Verkehr

Im Oktober 2017 haben wir die E-Mail-Kommunikation mit externen Stellen durch den Allgemeinen Sozialen Dienst (ASD) des Fachamtes Jugend- und Familienhilfe im Bezirksamt Wandsbek geprüft. Hierbei mussten wir feststellen, dass in ausnahmslos allen kontrollierten Fällen nicht hinreichend verschlüsselte E-Mails auch und gerade mit sensiblen personenbezogenen Sozialdaten von Kindern und Jugendlichen versendet wurden.

Die geprüften Akten betrafen Fälle der Heimerziehung und sonstiger betreuter Wohnformen (§ 34 SGB VIII) und der Inobhutnahme von Kindern und Jugendlichen (§ 42 SGB VIII). Ausschließlicher Prüfungsgegenstand war die Frage, ob das Fachamt Jugend- und Familienhilfe mit Stellen außerhalb der FHH per E-Mail personenbezogene Sozialdaten kommuniziert und inwieweit hierbei die erforderlichen technischen Maßnahmen zur Gewährleistung des Datenschutzes eingehalten werden. In ausnahmslos jeder geprüften Akte wurden E-Mails gefunden, die von Mitarbeiterinnen und Mitarbeitern des ASD an Stellen außerhalb der FHH geschickt wurden und personenbezogene Sozialdaten auch und gerade der betroffenen Kinder und Jugendlichen enthielten.

Nach § 78a SGB X ist jede datenverarbeitende Sozialleistungsstelle verpflichtet, diejenigen technischen Maßnahmen zu treffen, die erforderlich sind, um den Datenschutz sicherzustellen. Eine Maßnahme zur Gewährleistung, dass Sozialdaten bei der elektronischen Übertragung nicht unbefugt gelesen werden können, ist die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Bei Sozialdaten ist grundsätzlich von einem mindestens hohen Schutzbedarf auszugehen, da insbesondere ein Bruch der

Vertraulichkeit und ein damit einhergehendes Bekanntwerden der Informationen für die Betroffenen eine breite Ansehens- oder Vertrauensbeeinträchtigung bedeuten würde und somit erhebliche Auswirkungen auf ihre gesellschaftliche Stellung nach sich ziehen dürfte. Dies gilt gleichermaßen auch für Gesundheitsdaten, die das Datenschutzrecht per se bereits als besondere Arten personenbezogener Daten qualifiziert (§ 67 Abs. 12 SGB X) und die zum Teil Inhalt der Kommunikation auch des Jugendamtes sind. Im vorliegenden Zusammenhang wird der Schutzbedarf zusätzlich dadurch erhöht, dass es sich bei den Betroffenen um Kinder und Jugendliche handelt, bei denen u.a. eine Heimerziehung oder Inobhutnahme im Raume steht; diese Maßnahmen ihrerseits fußen wiederum auf besonders sensiblen Informationen zu den Betroffenen.

Zum Schutz derart sensibler Informationen ist die Verwendung einer sogenannten Ende-zu-Ende-Verschlüsselung erforderlich. Für die E-Mail-Kommunikation der Dienststellen der FHH untereinander existiert mit RMS eine Verschlüsselungsmöglichkeit, die auch eine einem hohen Schutzbedarf entsprechende Ende-zu-Ende-Verschlüsselung gewährleistet. Für die E-Mail-Kommunikation an Stellen außerhalb der FHH existiert ein derartiges Verschlüsselungsverfahren bisher nicht. Implementiert ist derzeit lediglich eine Transportverschlüsselung.

Entgegen den gesetzlichen Anforderungen an eine datenschutzkonforme elektronische Übertragung von Sozialdaten waren die überprüften E-Mails nicht hinreichend verschlüsselt; eine Ende-zu-Ende-Verschlüsslung wurde nicht vorgenommen. Während der Prüfung wurde darüber hinaus bestätigt, dass derartige Inhalte vermutlich in nahezu allen Akten gefunden werden können. Die FHH bietet die Möglichkeit an, dass sich Behörden bzw. einzelne Mitarbeiterinnen und Mitarbeiter De-Mail-Konten einrichten, über die verschlüsselte E-Mails versendet werden können. Die Nutzung einer De-Mail

würde zumindest zu einem erhöhten Schutz der übertragenen Sozialdaten führen. In den vorliegenden Fällen wurde jedoch keine De-Mail versendet.

Für uns ist es unstreitig, dass die Mitarbeiterinnen und Mitarbeiter speziell in den Fachämtern Jugend- und Familienhilfe auf eine schnelle Kommunikationsmöglichkeit angewiesen sind. Immer wieder kommt es zu Krisensituationen, in denen staatliche Hilfe sehr schnell gewährt werden muss. Ein langwieriger Briefwechsel bei einer dringend erforderlichen Inobhutnahme steht nicht nur den zeitlichen Abläufen, sondern vor allem dem jeweiligen Kindeswohl diametral entgegen. Für uns steht somit fest, dass den Fachämtern Jugend- und Familienhilfe die Möglichkeit der schnellen E-Mail-Kommunikation zwingend zur Verfügung stehen muss, diese somit nicht untersagt werden kann. Ein Untersagen würde vielmehr zur gesteigerten Gefährdung der Kinder und Jugendlichen führen. Dies muss ausgeschlossen werden.

Gleichzeitig gilt es aber auch zu verhindern, dass die Grundrechte auf informationelle Selbstbestimmung der Kinder und Jugendlichen auf Integrität und Vertraulichkeit informationstechnischer Systeme durch nicht hinreichende technische und organisatorische Maßnahmen bei der elektronischen Kommunikation verletzt werden. Wir haben die Behörde für Arbeit, Soziales, Familie und Integration daher gebeten, hierzu Stellung zu nehmen und entsprechende Maßnahmen zu ergreifen.

6. Übersendung vollständiger Kontonummern in unverschlüsselten E-Mails

IBAN-Kennungen dürfen aufgrund ihrer hohen Missbrauchsgefahr nicht auf einem unsicheren Übertragungsweg verschickt werden.

Es wandten sich mehrere Kunden von Versandhändlern und Reiseveranstaltern an uns, die Rechnungen und Bestellbestätigungen per E-Mail erhalten hatten. Diese Nachrichten ihrer Gläubiger enthielten unter anderem die vollständige Bankverbindung der Petenten. Es handelte sich um unverschlüsselte E-Mails, bei denen regelmäßig nicht ausgeschlossen werden kann, dass unbefugte Dritte sie mitlesen. Dabei ist die Kombination aus der Identität des Kontoinhabers, seiner IBAN und seiner BIC dem hohen Missbrauchsrisiko ausgesetzt, dass Kriminelle unberechtigte Abbuchungen vornehmen. Zudem besteht die Gefahr, dass die Daten für Identitätsbetrug im Versandhandel genutzt werden. Deshalb sollten diese Daten nicht in die falschen Hände geraten. Der Gesetzgeber hat die besondere Schutzbedürftigkeit dieser personenbezogenen Daten anerkannt, indem er in § 42a S. 1 Nr. 4 BDSG eine Meldepflicht für den Fall etabliert hat, dass personenbezogene Daten zu Bankkonten Dritten unrechtmäßig zur Kenntnis gelangen.

Als rechtmäßige Alternative können die Dokumente, die Bankverbindungen der Kunden enthalten, postalisch oder mit verschlüsselter E-Mail verschickt werden. Wenn dennoch der unverschlüsselte elektronische Versand erfolgen soll, ist die enthaltene IBAN zu maskieren. Dazu werden in der Regel die letzten Ziffern der Kennung durch X-Zeichen ersetzt. Die jeweiligen Unternehmen haben auf unsere Intervention hin ihre Verfahren dahingehend angepasst.

Die Maskierung der IBAN kann auch in Vorankündigungen (sogenannten Pre-Notifications) einer SEPA-Abbuchung erfolgen, sofern die Kontonummer dort überhaupt aufgeführt werden soll. Zwar sind Gläubiger verpflichtet, Schuldner im Vorfeld über eine Lastschrift zu informieren; zum notwendigen Mindestinhalt der Ankündigung gehört jedoch nicht die Benennung des konkreten Bankkontos, von dem abgebucht wird.

7. Google-Suchergebnisse – Insolvenzbekanntmachungen

Wir haben durchgesetzt, dass die Google LLC mehrere Internetangebote, auf denen personenbezogene Daten aus Insolvenzverfahren unzulässig veröffentlicht wurden, generell nicht mehr als Suchergebnisse verlinkt.

Nach der Insolvenzordnung sind personenbezogene Daten in Insolvenzverfahren durch die Amtsgerichte über eine länderübergreifende Veröffentlichung im Internet bekannt zu machen (www.insolvenzbekanntmachungen.de). Dort wird eine Indexierung durch Suchmaschinen verhindert. Eine Suche ist nur auf dem amtlichen Portal selbst möglich, wobei der Name allein als Suchkriterium nur während einer Dauer von zwei Wochen nach der Veröffentlichung verwendet werden kann.

Seit einiger Zeit werden die amtlich veröffentlichten Daten regelmäßig und systematisch von Dritten ausgelesen und auf eigenen Internetangeboten so veröffentlicht, dass Suchmaschinen sie namensbezogen auffinden. Die hohe Aufmerksamkeit bei Insolvenzdaten wird so für kommerzielle Zwecke genutzt, und die Nutzer dieser Internetangebote werden auf fragwürdige und sicherheitsgefährdende Werbeangebote weitergeleitet. Die Betreiber konnten bisher nicht ermittelt

werden. Die Auffindbarkeit von Informationen über Insolvenzverfahren bei bloßer Namenssuche stellt – zumindest bei Verbrauchern, freiberuflich Tätigen und Kleingewerbetreibenden – einen erheblichen Eingriff in deren Recht auf informationelle Selbstbestimmung dar und kann auch existenzielle Bereiche wie Miet- oder Arbeitsverhältnisse betreffen.

Auch vor dem Hintergrund dieser Problematik hat die Bund-Länder-Kommission für Informationstechnik in der Justiz die Justizverwaltungen der Länder gebeten, Vorschläge zur Anpassung der bundesweiten Regelungslage der öffentlichen Bekanntmachungen in Insolvenzverfahren zu entwickeln. Wir wirken dabei mit, um die datenschutzrechtliche Situation der Betroffenen zu verbessern.

Uns hat eine Vielzahl von Beschwerden in diesem Zusammenhang erreicht. Denn zunächst war Google nicht bereit, entsprechende Suchergebnisse aus dem Suchindex zu entfernen. Erst auf wiederholte Initiative und Androhung von aufsichtsbehördlichen Maßnahmen konnten wir Google dazu bewegen, eine Reihe dieser problematischen Angebote insgesamt zu sperren und das Problem damit deutlich zu entschärfen (*https://www.datenschutz-hamburg.de/news/detail/article/keine-google-links-mehr-zu-insolvenzdaten-auf-unzulaessigen-gewerblichen-internetangeboten.html*).

8. Prüflabor

Die Prüfung von Daten, die persönliche Geräte mit dem Internet austauschen, ist eine zunehmend wichtige Aufgabe für uns. Mittlerweile haben wir die komplexen technischen Voraussetzungen hierfür erfolgreich hergestellt.

Unser Alltag ist immer mehr durchdrungen mit Dienstleistungen und Geräten, die mit dem Internet verbunden sind. Über Smartphones, Fernsehgeräte, intelligente Lautsprecher, ver-

netzte Steckdosen und smartes Spielzeug holen wir uns beeindruckende und komfortable Möglichkeiten, unser Leben zu verbessern bis in unsere intimsten Bereiche. Leider sind die meisten dieser Dienste durch wenig Transparenz in Hinblick auf die Verarbeitung personenbezogener Daten gekennzeichnet und fordern dem Nutzer daher ein hohes Maß an nahezu blindem Vertrauen ab. Leichtfertig sollte man dieses jedoch nicht gewähren. Eine wachsende Zahl von zum Teil spektakulären Fällen, bei denen aufgedeckt wurde, welche Daten Apps, Roboterstaubsauger oder andere IoT-Geräte an den Hersteller übertragen, ohne dass den Nutzern dies bewusst ist oder sie darüber aufgeklärt werden, zeigt, dass Vorsicht angeraten ist.

Für eine Datenschutzaufsichtsbehörde stellt diese Situation eine große Herausforderung dar. Denn sie verfügt zwar über weitgehende gesetzliche Untersuchungsbefugnisse, die es ihr gestatten, Auskünfte bei verantwortlichen Stellen einzuholen und Prüfungen und Besichtigungen vorzunehmen. Diese Befugnisse können jedoch nur dort sinnvoll und effizient eingesetzt werden, wo ein ausreichender Konkretisierungsgrad vorliegt. Beschwerden Betroffener oder Hinweise aus der Presse können hier hilfreich sein. Allerdings verhindert es häufig gerade die mangelnde Transparenz der eingesetzten Technik, dass eine kritische Bewertung der stattfindenden Datenströme überhaupt stattfinden kann. Hier können Prüfwerkzeuge weiterhelfen, die mit relativ geringem und abschätzbarem Aufwand einen Einblick in das technische Geschehen erlauben und helfen, u.a. die folgenden Fragen zu beantworten:

- Mit welchen Servern werden Daten ausgetauscht?
- Erfolgt die Übertragung verschlüsselt?
- Welche Daten werden übertragen?
- Werden eindeutige Kennzeichen wie Werbe-IDs, Seriennummern oder Netzwerkadressen übertragen?

- Führen Widersprüche gegen bestimmte Datenübertragungen (z.B. zur Nutzungsmessung) tatsächlich zu entsprechend weniger Datenverkehr?
- Erfolgt umgekehrt eine bestimmte Übermittlung tatsächlich erst dann, wenn der Nutzer z.B. den Haken in dem entsprechenden Einwilligungsfeld gesetzt hat?

Erkenntnisse dieser Art sind in der Regel nicht alleine geeignet, eine datenschutzrechtliche Bewertung vorzunehmen. Sie können aber gerade die Hinweise liefern, die ein gezieltes Prüfen bzw. Einholen von Auskünften erst möglich macht. Zudem erleichtern es solche technischen Werkzeuge, die Plausibilität der eingeholten Auskünfte zu prüfen. Insgesamt können sie erheblich dazu beitragen, die Wahrnehmung unserer Behörde als ernstzunehmender Faktor bei den unserer Aufsicht unterliegenden Stellen zu fördern.

Aus diesem Befund heraus wurde aus dem Kreis einzelner Mitarbeiter der Behörde ein Werkzeug entwickelt, das die praktischen Anforderungen geeignet abdecken soll. Diese Entwicklung erfolgt allerdings nicht im Auftrag oder unter Beteiligung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, sondern als privates Projekt. Das Besondere dieser Lösung liegt darin, Software für eine spezifische Hardwareplattform (Raspberry Pi) bereitzustellen. Mit geringem finanziellen Aufwand entsteht so ein Prüfwerkzeug, das jederzeit einsatzbereit ist und aufgrund der geringen Abmessungen und Anforderungen der Hardware auch mobil eingesetzt werden kann – für Prüfungen im Zusammenhang mit Standortdaten ein wichtiger Aspekt.

Unsere ersten Erfahrungen mit dem Einsatz des Prüftools waren positiv. Es konnten in verschiedenen Fällen Datenströme aufgedeckt und nachvollzogen werden, die teilweise zu kritischen Nachfragen Anlass gaben. Diese bislang eher sporadischen Erfahrungen werden wir in Zukunft ausbauen.

Im Kreis der Datenschutzaufsichtsbehörden ist zudem vereinbart, die bislang sehr unterschiedlichen Erfahrungen, Ansätze und Wissensstände rund um Prüfungen von Apps und IoT-Geräten stärker auszutauschen und zu vereinheitlichen.

BERICHTE III.

1. Videoüberwachungsverbesserungsgesetz

Das Videoüberwachungsverbesserungsgesetz begegnet verfassungs- und europarechtlichen Bedenken.

Am 4.Mai 2017 trat das Videoüberwachungsverbesserungsgesetz in Kraft. § 6b Abs. 1 Bundesdatenschutzgesetz (BDSG) wurde folgender Satz angefügt:
„Bei der Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.“ Ferner wurde geregelt, dass dieser angefügte Satz für die Verarbeitung und Nutzung der erhobenen Videodaten entsprechend gilt.

Mit dieser Ergänzung des § 6b BDSG macht der Gesetzgeber eine Gewichtungsvorgabe für die Interessenabwägung zu Gunsten der Zulässigkeit einer Videoüberwachung. Die Neuregelung soll angesichts des Terroranschlags in Ansbach und des Amoklaufs in München im Jahr 2016 den Einsatz von Videoüberwachungstechnik durch private Stellen erleichtern und so zu einer präventiven Erhöhung der Sicherheit der Bevölkerung beitragen (vgl. BT-Drucksache 18/10941). Begründet wurde die Notwendigkeit der Neuregelung mit einer zu restriktiven Kontrollpraxis der Datenschutzaufsichtsbehörden. Als Beispiel wurde im Gesetzentwurf unsere rechtskräftige Anordnung aus dem Jahr 2010 gegenüber einem Unternehmen mit Sitz in Hamburg angeführt, das bundesweit Einkaufszentren betreibt (vgl. 23. TB, IV 1.2.). Es erscheint zumindest unüblich, dass ein Gesetzentwurf mit einem Einzel-

fall begründet wird. Dies gilt umso mehr, weil die dem Einzelfall zugrundeliegende Anordnung bestandskräftig geworden ist, ohne dass die verantwortliche Stelle von ihrem Recht Gebrauch gemacht hat, den Rechtsakt durch die Verwaltungsgerichtsbarkeit überprüfen zu lassen.

Auch materiell bestehen gegen das Gesetz erhebliche verfassungs- und europarechtliche Bedenken. Es ist nicht die Aufgabe privater Stellen, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen. Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen in der Regel aus Kostengründen kein Live-Monitoring durchführen und die Bilder der vielen Kameras durch ihr eigenes Personal nicht so auswerten, dass bei Gefahren direkt und schnell eingegriffen werden kann (vgl. 26. TB, V 4.). In der Praxis bleibt der Nutzen der Kameras daher auf eine Speicherung auf Vorrat für die spätere Strafverfolgung beschränkt. Die präventive Zielsetzung des Gesetzes wird insoweit nicht erreicht. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat diese und weitere Bedenken am 6. März 2017 im Rahmen einer öffentlichen Expertenanhörung des Innenausschusses des Bundestages vorgetragen (*https://www.bundestag.de/blob/495892/968dd6e4291bf978ad9c0d20840fe306/18-4-785-f-data.pdf*). Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hatte zuvor in ihrer Entschließung „Videoüberwachungsverbesserungsgesetz zurückziehen!“ vom 9. November 2016 (*https://www.datenschutz.de/entschliessung-der-92-konferenz-der-unabhaengigen-datenschutzbehoerden-des-bundes-und-der-laender-videoueberwachungsverbesserungsgesetz-zurueckziehen/*) ebenfalls massive Kritik an dem Gesetzesvorhaben geäußert. Leider haben diese Bedenken kein Gehör gefunden. Vielmehr wurde die Regelung wortgleich als § 4 in das Datenschutz-Anpassungs- und -Umset-

zungsgesetz EU übernommen. Wir haben erhebliche Zweifel daran, dass der deutsche Gesetzgeber auch zukünftig noch die Befugnis hat, die Videoüberwachung durch private Stellen selbst zu regeln. Eine entsprechende Öffnungsklausel enthält die ab 25. Mai 2018 unmittelbar anzuwendende Datenschutzgrundverordnung nicht.

2. Gesichtsanalyse und Emotional Decoding

Eine Unterarbeitsgruppe der Datenschutzkonferenz beschäftigt sich mit dem Einsatz von Gesichtsanalyseverfahren zu Werbezwecken.

Im Berichtszeitraum erhielten wir mehrere Presseanfragen zur Rechtmäßigkeit von optisch-elektronischen Verfahren, die in Supermärkten, Postfilialen und Wildparks zur Gesichtsanalyse eingesetzt werden. Diese Verfahren sollen nach Auskunft der Hersteller die Bestimmung des ungefähren Alters und des Geschlechts einer Person ermöglichen. Durch eine Analyse der Mimik können zusätzlich Rückschlüsse auf die Gefühlslage eines Menschen gezogen werden (Emotional Decoding). Auf Basis der ermittelten Informationen kann eine Werbemaßnahme (z.B. auf einem Monitor) in Echtzeit an die Zielgruppe angepasst und ihre Wirksamkeit anhand der Reaktion der analysierten Person gemessen werden. Für die betroffenen Personen ist der Einsatz dieser Verfahren in der Regel nicht erkennbar, da in den uns bekannten Fällen kein gesonderter Hinweis auf die Gesichtsanalyse erfolgte.

Die Datensouveränität des Einzelnen gebietet es, nicht nur die äußere Erscheinung der Person, sondern gerade auch die inneren Gemütszustände vor einer automatisierten maschinellen Erfassung zu schützen. Ob diese Verfahren aber überhaupt den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) unterliegen, ist fraglich. Jedenfalls die Hersteller dieser Ver-

fahren gehen davon aus, dass bei der Analyse keine personenbezogenen oder personenbeziehbaren Daten erhoben und verarbeitet werden und diese Verfahren daher nicht den Bestimmungen des BDSG unterliegen. Diese Bewertung halten wir für nicht überzeugend. Der Einsatz der Verfahren setzt unseres Erachtens die Erhebung und die zumindest kurzzeitige Speicherung personenbezogener oder personenbeziehbarer Daten voraus. Selbst wenn die Datenverarbeitung nur für kurze Zeit erfolgen sollte, dürften diese Verfahren somit nur mit einer Einwilligung der Betroffenen eingesetzt werden oder müssten durch eine Rechtsvorschrift erlaubt sein. Die Kürze der Verarbeitungsdauer mag im Rahmen einer Abwägung zu berücksichtigen sein, für die Frage, ob es sich überhaupt um eine Verarbeitung handelt, die einer Rechtfertigung bedarf, ist sie jedoch ohne Belang.

Die Datenschutzkonferenz des Bundes und der Länder hat daher die Unterarbeitsgruppe (UAG) „Biometrische Analyse" initiiert, in der wir mitwirken. Diese UAG hat den Auftrag, sich mit der Datenverarbeitung durch Sensorik und Videotechnik und deren datenschutzrechtlicher Einordnung zu befassen. Darüber hinaus soll eine Übersicht aktueller Verfahren und deren technischer Ausgestaltung im Kontext der biometrischen Analyse entstehen. Durch immer ausgefeiltere Algorithmen und rasche Entwicklungen, insbesondere im Bereich des maschinellen Lernens, wird biometrischen Erkennungsmethoden in den nächsten Jahren ein enormes Potential beigemessen. Als Berechtigungsnachweis werden diese Techniken einer breiten Nutzerbasis zugänglich gemacht, wie es aktuell schon namhafte Hersteller von Smartphones mit Fingerabdrucksensoren und Gesichtserkennung demonstrieren. Hierbei muss jedoch bedacht werden, dass solche Verfahren lediglich Wahrscheinlichkeiten der Ähnlichkeit liefern und fehlerbehaftet sind. Auch deshalb dürfen biometrische Erkennungssysteme im Kontext der Werbung nicht dazu missbraucht werden, Angebote nur einer bestimmten Zielgruppe zu gewähren oder

aber im umgekehrten Falle individuelle Preisstaffelungen einzuführen, die einzelnen Zielgruppen unterschiedliche Preise präsentiert, wie es heutzutage leider bereits in einigen Branchen aus anderer Datenbasis üblich ist.

Der Datenschutz darf den technischen Entwicklungen nicht hinterherschauen, sondern muss weiterhin eine konstruktive und begleitende Funktion innerhalb der Produktentwicklung und Innovation einnehmen. Die UAG Biometrische Analyse soll hierzu ihren Anteil leisten und Unklarheiten und Risiken aus der Sicht des Datenschutzes begegnen und aufarbeiten. Im nächsten Tätigkeitsbericht werden wir über die Ergebnisse berichten.

3. Übertragung von Aufsichtsbefugnissen auf den Bund im Bereich der Steuerverwaltung

In einem wenig transparenten Gesetzgebungsverfahren des Bundes wurden den Landesdatenschutzbeauftragten (LfDs) umfangreiche Zuständigkeiten für die Aufsicht über die Länderfinanzbehörden entzogen. Gegen unsere Empfehlung will die Finanzbehörde weitere Aufsichtsbefugnisse auf die Bundesebene verlagern.

Die neue EU-Datenschutz-Grundverordnung (DSGVO) und das Datenschutzanpassungsgesetz machten die Änderung zahlreicher Fachgesetze erforderlich. Im Zuge dessen hatte sich unsere Behörde ausführlich mit der Änderung des Bundesversorgungsgesetzes und verwandter sozialrechtlicher Regelungen befasst. Für die LfDs völlig überraschend und kurzfristig, wurde die 12-seitige Drucksache 18/12041 mit drei Artikelgesetzen aufgrund eines Änderungsantrags vom 16. Mai 2017 (Ausschussdrucksache 18(11)1031) zu einer 75-seitigen Drucksache mit 21 Artikeln aufgebläht, in der u. a. umfangreich und tiefgreifend die Abgabenordnung (AO)

geändert wurde (im Folgenden: AO-neu). Uns blieb keine Zeit, die zahlreichen Änderungen detailliert zur Kenntnis zu nehmen, geschweige denn, sie zu prüfen und zu bewerten, bevor sie am 2. Juni 2017 vom Bundestag in der Ausschussfassung (BT-Drs. 18/12611) angenommen wurden. Leider zu spät wurde deutlich, dass in § 32h Abs. 1 des AO-Entwurfs Zuständigkeiten für die Überwachung der Landessteuerbehörden, die zurzeit von den LfDs wahrgenommen werden, ab 25. Mai 2018 bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) liegen werden. Interventionen wären wegen des außerordentlich knappen Zeitablaufs aber wohl ohnehin zu spät gekommen.

Obwohl die Steuerverwaltung Hamburg an den Vorüberlegungen auf Arbeitsebene für die Finanzbehörde Hamburg an einer länderoffenen Arbeitsgruppe unter Federführung des Bundesfinanzministeriums (BMF) beteiligt war, wurden wir über die beabsichtigten Kompetenzänderungen nicht informiert. Allerdings ist inzwischen deutlich geworden, dass die Steuerverwaltung Hamburg der Auffassung war, nur so könne erreicht werden, dass die eingesetzten Datenverarbeitungsverfahren datenschutzrechtlich bundesweit einheitlich bewertet werden. Diese Einschätzung teilen wir nicht, und nicht zuletzt wäre für die Betroffenen – i. d. R. hamburgische Steuerzahler – eine datenschutzrechtliche Betreuung durch den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) vor Ort eindeutig „bürgernäher".

§ 32h Abs. 3 AO-neu soll es ermöglichen, dass durch Landesgesetz Aufsichtsbefugnisse auch für landesrechtlich geregelte Steuern, z. B. Kirchen- oder Hundesteuer, auf die BfDI übertragen werden können. Die Steuerverwaltung Hamburg trat mit Schreiben vom 6. September 2017 mit entsprechenden Überlegungen und einem Gesprächswunsch an uns heran. Die Finanzbehörde plante, die Aufgabenübertragung in dem Entwurf eines neuen Hamburgischen Datenschutzgesetzes zu

regeln. Wir teilten der Steuerverwaltung schriftlich mit, dass wir die Befürchtungen der Steuerverwaltung, dass es bei der Anwendung bundeseinheitlich eingesetzter Datenverarbeitungsverfahren, soweit sie auch bei Landessteuern eingesetzt werden, zu unterschiedlichen Bewertungen von Verfahren oder Datenschutzfolgeabschätzungen (DFA) durch nebeneinander bestehende Zuständigkeiten der BfDI und des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit kommen könnte, für eher theoretischer Natur hielten:
Dass wir ein Verfahren, das die BfDI bereits als datenschutzkonform bewertet hat, anders bewerten würden - und gar zum Anlass einer Anordnung gegen die Steuerverwaltung nehmen könnten - scheint nicht realistisch. Schon die einheitliche Rechtslage, die künftig gilt, gibt zu solchen Befürchtungen keinen Grund. Während nach jetziger, bis zum 24. Mai 2018 geltender Gesetzeslage die technisch-organisatorischen Maßnahmen landesrechtlich geregelt sind und unterschiedlich interpretiert werden können, gilt in Zukunft Art. 32 DSGVO unmittelbar. Sollte im Rahmen unserer Zuständigkeit ein bundesweit eingesetztes Verfahren eine Rolle spielen, das tatsächlich von der BfDI noch nicht datenschutzrechtlich geprüft wäre, würde der HmbBfDI zunächst Kontakt mit der BfDI aufnehmen. Entsprechend gilt dies auch für die DFA. Und schließlich wiesen wir noch auf die ungewisse Kostenregelung in § 32h Abs. 3 AO-neu hin, wonach Hamburg der BfDI für die Aufgabenübertragung die entsprechenden Kosten erstatten muss.

Auch im Übrigen halten wir die gesetzliche Regelung in § 32h Abs. 3 AO-neu für unklar, zumal die Begründung zu der Regelung offensichtlich fehlerhaft ist. Eine Regelung in Anlehnung an § 32h Abs. 3 AO-neu zu verfassen, die hinreichend bestimmt ist, scheint deshalb nicht einfach. Verfassungsrechtliche Fragen haben wir bisher ausgeklammert.
Die Finanzbehörde Hamburg ist nach unserem Erkenntnisstand zurzeit bundesweit die einzige Landesfinanzverwaltung, die von § 32h Abs. 3 AO-neu Gebrauch machen möchte.

Das deutet darauf hin, dass auch in anderen Ländern die Gefahr, dass es zu unterschiedlichen Bewertungen bundesweit eingesetzter Verfahren durch die Landes- und Bundesdatenschutzaufsicht kommen könnte, so nicht gesehen bzw. anders gewertet wird. Es erscheint daher durchaus sinnvoll, zunächst einmal die Entwicklung und die Diskussion in den anderen Bundesländern abzuwarten. Das gilt in besonderer Weise mit Blick auf die norddeutschen Bundesländer, die ihre Datenverarbeitungsverfahren gemeinsam im Data Center Steuern (DCS) bei Dataport betreiben und nach unserer Meinung einheitlich handeln sollten.

Auch die Tatsache, dass eine Verlagerung der Zuständigkeit auf die BfDI nach § 32h Abs. 3 AO-neu zur Folge hat, dass Hamburg dann für die Verwaltungskosten aufkommen muss, spricht klar gegen eine solche Regelung. Dies darf nicht dazu führen, dass entsprechende Kosten am Ende den Haushalt des HmbBfDI belasten.

4. Google-Suchergebnisse – „Recht auf Vergessenwerden“

Der HmbBfDI prüft in Deutschland Eingaben zu Fällen, in denen es die Google LLC abgelehnt hat, Suchergebnisse zu entfernen, die bei der Eingabe der Namen von Betroffenen in der Internetsuchmaschine des Unternehmens angezeigt werden.

Dieser Prüfungstätigkeit liegt das Urteil des Europäischen Gerichtshofes (EuGH) vom 13.05.2014 (C-131/12) zugrunde. Suchergebnissen zu den Namen von Personen haben – insbesondere unter Berücksichtigung von deren Profilbildung (vgl. EuGH, Urteil vom 13.05.2014, C-131/12, Rn. 37) – eine besondere Bedeutung. Die Internetsuchmaschine Google, für die der HmbBfDI in Deutschland zuständig ist, hat im Inland fortlaufend einen Marktanteil von mehr als 90 Prozent.

Entsprechend den datenschutzrechtlichen Vorgaben prüft zunächst die Google LLC als für die Datenverarbeitung verantwortliche Stelle bei Ersuchen von Betroffenen, ob die Anzeige der Suchergebnisse zulässig ist. Das seit Mai 2014 dafür öffentlich zugänglich gemachte Online-Verfahren ist unter der URL *https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit* abrufbar.

Vom 28.05.2014 bis zum 18.12.2017 wurden in Deutschland zu 341.163 URLs Ersuchen an die Google LLC gestellt von denen 47,9 % entfernt und 52,1% nicht entfernt wurden (Europa: von 1.989.531 URLs wurden 43,2% entfernt und 56,8% nicht entfernt). In Europa wurde der größte Anteil mit 20,6 % in Frankreich zu 409.856 URLs gestellt (48,6% entfernt und 51,4% nicht entfernt). In Deutschland – für das der HmbBfDI bei Google-Eingaben allein zuständig ist – wurden nach Frankreich die meisten Ersuchen in Europa mit einem Anteil von 17,6 % gestellt. In den anderen Ländern gab es deutlich weniger Ersuchen (vgl. Großbritannien: 12,7% oder Spanien: 8,5%). Der aktuelle Transparenzbericht des Unternehmens ist unter der URL *https://transparencyreport.google.com/eu-privacy/overview?hl=de* einsehbar.

Wir sind bei der Prüfung und Bearbeitung der Fälle fortlaufend in Kontakt mit der Google LLC und haben das Unternehmen in vielen Fällen zur Entfernung von Suchergebnissen aufgefordert und angehört. Unsere Prüfungen und die Abwägungen der jeweiligen Interessen haben häufig aber auch ergeben, dass die Voraussetzungen zur Entfernung von Suchergebnissen nicht vorliegen. In den seltenen Fällen, in denen wir verwaltungsrechtliche Anordnungen zur Entfernung von Suchergebnissen erlassen haben, ist die Google LLC dem nachgekommen und hat keinen Rechtsbehelf (Widerspruch) eingelegt.

Wir sind weiterhin regelmäßig in Kontakt mit den europäi-

schen Datenschutzbehörden und der Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten (Artikel 29-Datenschutzgruppe). Im Hinblick auf die ab dem 25. Mai 2018 europaweit geltende Datenschutzgrundverordnung wurden in der Artikel 29-Datenschutzgruppe Testfälle mit grenzüberschreitenden Umständen diskutiert. Hierbei ging es insbesondere um Fragen der Zuständigkeit, der gemeinsamen Zusammenarbeit, der inhaltlichen Prüfung sowie Abwägung zwischen dem Recht auf informationelle Selbstbestimmung mit dem öffentlichen Informationsinteresse und der Meinungsfreiheit.

Das oberste französische Verwaltungsgericht hat dem EuGH verschiedene Fragen zur Vorabentscheidung vorgelegt, u.a. ob eine Entfernung von Suchergebnissen wegen europäischen Datenschutzrechten weltweit zu erfolgen hat. Die französische Datenschutzaufsichtsbehörde hatte insoweit im Jahr 2016 ein Bußgeld von 100.000 EUR erlassen, da außereuropäische Suchergebnisse in der Google Suchmaschine nicht entfernt wurden. Die Vorlagefragen betreffen auch die Bedeutung von besonderen personenbezogenen Daten, wie Gesundheit, politische Meinungen und Straftaten, in Quellen von Suchergebnissen. Mit einer Entscheidung ist im Laufe des Jahres 2018 zu rechnen.

5. WhatsApp in Betrieb und Verwaltung

Der Einsatz von WhatsApp zur behördlichen oder unternehmerischen Kommunikation ist nur dann zulässig, wenn die Betroffenen in die Nutzung gegenüber der verantwortlichen Stelle eingewilligt haben.

Der Einsatz von Diensten zur Individualkommunikation wie WhatsApp hat nicht nur im Privatbereich im Berichtszeitraum rasant zugenommen. Auch Unternehmen wollen über diesen

Dienst mit ihren Kunden kommunizieren. Wir erhalten zu diesem Themenfeld verschiedentlich Anfragen und Beschwerden. Allerdings sind wir weder für das Unternehmen WhatsApp Inc. mit Sitz in den USA, noch für andere vergleichbare Anbieter derartiger Dienste der Individualkommunikation zuständig. Die Kontrolle der Einhaltung datenschutzrechtlicher Vorgaben durch dieses Unternehmen wird durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wahrgenommen. Denn hier handelt es sich nach dem gemeinsamen Verständnis der deutschen Aufsichtsbehörden um sog. OTT (Over-the-top)-Dienste, und damit um Telekommunikation. Sie unterfallen dem Telekommunikationsgesetz (TKG) und ihre datenschutzrechtliche Kontrolle obliegt gemäß § 115 Abs. 4 TKG der BfDI.

Anders sieht es jedoch aus, wenn ein Unternehmen in unserem Zuständigkeitsbereich WhatsApp z.B. für den Kundenkontakt nutzt. Eine Übermittlung personenbezogener Daten erfolgt an solche Anbieter immer dann, wenn dieser z. B. Telefonnummern oder andere Kontaktdaten erhält, damit eine Kommunikation überhaupt stattfinden kann. Dies erfolgt in der Regel über einen sogenannten Adressbuchupload, bei dem die gesamte Kontaktinformation eines Geräts an den Anbieter übermittelt wird. Nach unserer Ansicht stellt eine solche Übermittlung zu unternehmerischen Zwecken eine vom Grundsatz her datenschutzrechtlich unzulässige Verarbeitung personenbezogener Daten dar. Denn aus den Nutzungsbedingungen der WhatsApp Inc. wird deutlich, dass sie ihre Nutzer auffordert, die Legitimität der Übermittlung der Daten eigenständig sicherzustellen. Zudem ist nicht vollständig gewährleistet, dass die WhatsApp Inc. die Adressbuchdaten ausschließlich und abschließend für die Erbringung der eigentlichen Kommunikationsdienstleistung verwendet. Die Datenschutzerklärung von WhatsApp ist in diesem Zusammenhang zu unbestimmt und lässt den Schluss zu, dass übermittelte Daten auch über den unmittelbaren Zweck der Diensterbringung hinaus durch das Unternehmen verwendet

werden, etwa zu eigenen wirtschaftlichen Zwecken.

Soweit Unternehmen und Behörden meinen, dennoch nicht auf die Verwendung des Dienstes von WhatsApp verzichten zu können, sollte die Nutzung über ein Endgerät abgewickelt werden, welches bei der Installation der App über ein leeres Adressbuch verfügt. Werden die Unternehmen und Behörden dann direkt über WhatsApp von den Betroffenen kontaktiert, kann (konkludent) von einer Einwilligung der Betroffenen ausgegangen werden. Hier kann eine Ausnahme vom Schriftformerfordernis der Einwilligung gemäß § 4a Abs. 1 S. 3 BDSG gesehen werden, wonach von dieser Formvorschrift abgesehen werden kann, wenn dies wegen der besonderen Umstände angemessen ist. Der HmbBfDI würde das Hinzufügen des Kontakts in das Adressbuch und die weitere Kommunikation über den Dienst der WhatsApp Inc. unter diesen Vorgaben nicht beanstanden.

Rechtssicherer und mit den gesetzlichen Vorgaben zweifelsfrei im Einklang wäre es, wenn die Unternehmen direkt die Nummern mit dem Kunden und Geschäftspartnern austauschen und sich dabei die schriftliche Einwilligung durch die Betroffenen erteilen lassen.

Eine Übermittlung bereits vorhandener Adressdaten an WhatsApp wäre nach unserer Ansicht nur zulässig, wenn dafür gemäß § 4 Abs. 1 BDSG eine entsprechende Rechtsgrundlage existiert. Diese könnte neben der Einwilligung des Betroffenen, bei bestimmten Sachverhaltskonstellationen aufgrund von zivilrechtlichen Verträgen in der Erfüllung eigener Geschäftszwecke oder ausnahmsweise in der Wahrung berechtigter Interessen des jeweiligen Unternehmens liegen. Für öffentliche Stellen wäre eine gesetzliche Rechtsgrundlage erforderlich, die nach unserer Kenntnis allerdings nicht existiert.

In jedem Fall sind bei der Übermittlung der Daten vorab immer

die schutzwürdigen Interessen der betroffenen Kundinnen und Kunden bzw. der Bürgerinnen und Bürger zu beachten. In der Regel können Unternehmen und Behörden nicht davon ausgehen, dass Betroffene die Übermittlung z. B. ihrer Telefonnummer für nicht genauer spezifizierte Zwecke der WhatsApp Inc. hinnehmen müssen. Gerade im Bereich der Verarbeitung personenbezogener Daten zum Zwecke der Werbung und des Marketings setzt das Wettbewerbs- und Datenschutzecht der Datenverarbeitung enge Grenzen und erfordert in der Regel die Erteilung einer Einwilligung der Betroffenen. Dies steht auch im Einklang mit der deutschen Rechtsprechung, die immer wieder den belästigenden Charakter von Werbung festgestellt hat und die Nutzung von Kontaktdaten zu Werbezwecken einem Einwilligungsvorbehalt unterstellt. Die Einwilligung muss jeweils von der Person, deren Kontaktdaten aus dem Adressbuch an die WhatsApp übermittelt werden, unter den Bedingungen des § 4a BDSG bzw. § 5 HmbDSG erteilt werden. Die Annahme, dass schon deshalb eine Einwilligung in die Übermittlung von Adressdaten an die WhatsApp Inc. vorliegt, weil der Betroffene selbst Nutzer von WhatsApp ist, ist abzulehnen. Denn Dienste wie WhatsApp ziehen aus der Information, wer mit wem verbunden ist, zusätzliche Schlüsse.

6. Google Home

Digitale Sprachassistenten erscheinen bequem, schaffen jedoch zahlreiche Risiken für die Privatsphäre. Es besteht ein großer Bedarf für datenschutzrechtliche Überprüfungen.

Konsumenten, die Dienste und Dienstleistungen aus dem Internet ohne manuelle Aktivität wie Klicken oder Tippen nutzen möchten, finden ein immer größer werdendes Angebot an digitalen Sprachassistenten vor. Neben Diensten, die im Betriebssystem von PCs, Tablets oder Smartphones enthalten sind, werden zunehmend eigenständige Geräte angeboten, die nahezu komplett über Sprache gesteuert werden. An die-

ser Entwicklung ist auch das Unternehmen Google beteiligt. Einerseits durch Assistenzdienste in den Betriebssystemen Android und ChromeOS, neuerdings aber auch mit eigenständigen Geräten unter dem Namen „Google Home" bzw. „Google Home Mini". Für die Nutzer versprechen diese Geräte die Möglichkeit der rein sprachlichen Interaktion mit Google. So können Dienste wie Websuche oder persönliche Einkaufs- und Terminplanung ohne Verwendung eines PCs oder Smartphones genutzt werden. Auch lässt sich die Wiedergabe von Musik- oder Videodateien über die heimische Stereoanlage oder das lokale TV-Gerät steuern.

Zur Nutzung des Google Home-Dienstes muss das Gerät in das Heimnetzwerk des Nutzers eingebunden werden und darüber Zugriff auf das Internet erhalten. Anschließend wird die Einrichtung per App vorgenommen. Ist diese abgeschlossen, erfolgt die Kommunikation des Gerätes mit dem Benutzer nur noch über Mikrofon, Lautsprecher sowie einige Leuchtdioden. Das Gerät lauscht dann permanent auf die vordefinierten Aktivierungsworte „OK Google" bzw. „Hey Google". Werden diese erkannt, zeichnet es die Mikrofonsignale auf und überträgt diese an Google-Server. Dort wird die in der Aufnahme enthaltene Anfrage oder der Befehl per Sprachanalyse ausgelesen und analog einer Texteingabe bei der Google Suchmaschine beantwortet. Das Ergebnis wird an das Google-Home-Gerät zurückgesandt und dort in synthetischer Sprache über den Lautsprecher ausgegeben. Die Reaktion kann auch im Ansteuern der Hardware eines Drittherstellers erfolgen, z.B. Ein- oder Ausschalten von Lampen oder anderen Geräten.

Durch einen internetbasierenden digitalen Sprachassistent installiert ein Nutzer einen permanenten akustischen Kanal für Dritte in sein persönliches Lebensumfeld. Dabei erhält er wenig Transparenz darüber, was konkret dort stattfindet oder wie, wann und von wem der Übertragungskanal tatsächlich genutzt wird. Ebenfalls ist für Nutzer kaum steuerbar, was

später mit den erhobenen akustischen Informationen passiert. Die übertragenen Audiosignale, welche oft nicht nur die Nutzerstimme, sondern auch Umgebungs- und Wohnungsgeräusche oder Stimmen anderer Menschen enthalten, werden häufig für lange Zeit beim jeweiligen Anbieter gespeichert (siehe *https://www.heise.de/mac-and-i/meldung/Apple-bewahrt-Siri-Daten-bis-zu-zwei-Jahre-lang-auf-1846278.html*). So entstehen dort mit der Zeit immer schärfere Sprach- und Sprechprofile von Personen.

Solche Datenspeicherungen wecken Begehrlichkeiten. So versuchte die US-Polizei bereits durch Beantragung des Zugriffs auf Audioaufnahmen eines Amazon Echo Gerätes einen Mordfall aufzuklären (siehe *https://www.heise.de/newsticker/meldung/Ermittlungen-zu-mutmasslichem-Mord-Amazon-haendigt-Alexa-Aufnahmen-aus-3646131.html*).

Es ist zu befürchten, dass Zugriffe auf Daten von Sprachassistenten in Zukunft zu den verschiedensten Zwecken Normalität werden. Nicht nur in den USA aufgrund der dort niedrigeren Datenschutzhürden, sondern vielleicht irgendwann auch in Europa.

Auch für Kriminelle oder unbekannte Dritte eröffnen Sprachassistenten neue Überwachungsmöglichkeiten. Wie für jedes mit dem Internet verbundene Endgerät besteht die Gefahr, dass sie über Sicherheitslücken gekapert und missbraucht werden. Im Zweifel sind motivierte Hacker stets erfolgreicher als Produktentwickler oder Ingenieure, die niemals alle Fehler und Schwachstellen in ihren Produkten voraussehen oder ausmerzen können. So haben Forscher bereits 2014 demonstriert, wie ein Smart-TV-Gerät durch Einbringen einer als Mediendatei getarnten Schadsoftware per WLAN derart kompromittiert werden kann, dass am Ende die vor dem Gerät sitzenden Zuschauer über die Kamera und das Mikrofon

des Gerätes ausgespäht werden konnten. (siehe *https://pdfs.semanticscholar.org/f55c/0d6c95b8c1a8d8817ab768c80ad0652e314b.pdf*).

Abschließend ist festzustellen, dass der Trend zu internetbasierenden Sprachassistenten für den jeweiligen Nutzer, aber auch für dessen soziales Umfeld und letztlich für die gesamte Gesellschaft ein nicht zu unterschätzendes Risiko darstellt. Neben der zunehmenden Überwachung des öffentlichen Raums u.a. aus Sicherheitsgründen hält durch diese Geräte die Überwachung und gleichzeitig die Überwachbarkeit in der eigenen Wohnung Einzug. Dabei erfolgt dieser Schritt selbstbestimmt und freiwillig, weil sich die Nutzer einen Komfortgewinn versprechen. Welche konkreten Risiken sie sich damit einhandeln, ist den meisten jedoch unbekannt und im Detail noch nicht ermittelt.

Der HmbBfDI wird diese Technologie daher verstärkt beobachten und überprüfen. Dies betrifft die konkrete Datenübermittlung ebenso wie die allgemeine Funktionsweise des Dienstes Google Home und die Verarbeitung der Daten in der Google Cloud.

RECHTSVERBINDLICHE ANORDNUNGEN UND BUSSGELDER IV.

1. Anordnung gegen einen Kfz-Dienstleister

Im Berichtszeitraum haben wir eine Anordnung gegen ein Unternehmen erlassen, welches Dienstleistungen für Autovermieter erbringt. Dieses überwacht seine Beschäftigten bei der Arbeit in unzulässigem Maß.

Dies betrifft insbesondere Arbeitsabläufe wie die Entgegennahme und Reinigung von Leihfahrzeugen. Die Betriebsstätte des Unternehmens wird mit insgesamt 26 Videokameras überwacht. Wir wurden durch die Beschwerde eines Beschäftigten auf das Unternehmen aufmerksam, der sich durch die umfängliche Videoüberwachung in seinem Recht auf informationelle Selbstbestimmung verletzt sah. Bei der durchgeführten Kontrolle haben wir festgestellt, dass sämtliche Bereiche, in denen sich die Beschäftigten des Unternehmens aufhalten müssen, um ihrer Arbeit nachzugehen, von Kameras erfasst werden. Dies hielten wir mit Blick auf die vorgetragenen Zwecke und geschilderten Vorfälle für unverhältnismäßig und damit für unzulässig. Da das Unternehmen in einem Zeitraum von über zwei Jahren und nach umfangreicher schriftlicher Korrespondenz, in der die Rechtslage ausführlich geschildert wurde, keine Bereitschaft zeigte, den Betrieb der Kameras einzuschränken, war es aus unserer Sicht erforderlich, eine Anordnung zu erlassen. Mit dieser Anordnung wurde das Unternehmen verpflichtet, 11 der 26 Kameras während der Betriebszeiten auszuschalten und 3 weitere Kameras anders auszurichten. Gegen diese Anordnung hat das Unternehmen nach erfolglosem Widerspruch Klage erhoben.

Das Verwaltungsgericht Hamburg (VG Hamburg) hat über die Klage noch nicht entschieden. Es hat in der mündlichen Verhandlung erkennen lassen, dass es unsere Rechtsauffassung insoweit teilt, als es die durchgeführte Videoüberwachung ebenfalls teilweise für rechtswidrig hält. Gleichzeitig hat es in Frage gestellt, ob für die Anordnung die richtige

Rechtsgrundlage gewählt wurde. Unter Umständen komme erst bei Nichtbefolgung einer Anordnung nach § 38 Abs. 5 Satz 1 BDSG eine Untersagung einzelner Verfahren nach § 38 Abs. 5 Satz 2 BDSG in Betracht. Das Gericht diskutierte die Auffassung, dass die von uns angeordnete Abschaltung der Kameras während der Geschäftszeiten keine Maßnahme zur Beseitigung festgestellter Verstöße nach § 38 Abs. 5 S. 1 BDSG sei, sondern die Untersagung von Verfahren im Sinne des § 38 Abs. 5 S. 2 BDSG, da jede Kamera als ein einzelnes Verfahren anzusehen sei. Wir sehen dies anders und konnten zur Begründung eine Reihe von Gerichtsentscheidungen aus ganz Deutschland anführen. Diese sind für das VG Hamburg jedoch nicht bindend. Kommt es in unserem Fall zu der oben dargestellten Auffassung, könnte die Entscheidung lauten, dass die teilweise rechtswidrige Videoüberwachung des Unternehmens weiter durchgeführt werden kann. Wir müssen hier zunächst das Urteil des VG Hamburg abwarten. Dieses wird wohl erst knapp vor der Anwendbarkeit der Datenschutzgrundverordnung ergehen.

2. Bußgeldverfahren gegen einen Gastronomiebetrieb

Das AG Hamburg hat die Geschäftsführerin eines Gastronomiebetriebs zur Zahlung eines Bußgelds wegen unzulässiger Videoüberwachung verurteilt.

Im Berichtszeitraum haben wir ein Bußgeldverfahren gegen die Geschäftsführerin eines Gastronomieunternehmens durchgeführt. In dem Restaurant waren fünf Kameras durchgehend in Betrieb und auf die Kundensitzplätze in den Gasträumen des Restaurants gerichtet. Die Videoaufzeichnungen wurden nach etwa einem Monat gelöscht. Die Betreiberin teilte uns zu den Zwecken der Videoüberwachung mit, dass die Installation der Kameras zwingende Voraussetzung sei, um der Begehung von Diebstahls- und Raub- oder Körperverletzungsdelikten vorzu-

beugen. Die Videokameras dienten auch der Beweisführung und Aufklärung von Straftaten. In der Vergangenheit habe es Hausfriedensbrüche gegeben und bei einem Tresoraufbruch sei Bargeld entwendet worden. Allein schon die Tatsache, dass alkoholische Getränke im Betrieb veräußert würden, genüge als Rechtfertigung für den Einsatz von Videoüberwachung. Das Betreten des Gastraumes durch die mit einem Videoüberwachungshinweis versehene Tür sei eine konkludente Einwilligung der Gäste in die Überwachung.

Eine Zulässigkeit der Videoüberwachung der Gasträume ergab sich aus diesem Vortrag nicht. Die vorgenommene Videoüberwachung sowie die Speicherung und Nutzung des Bildmaterials hätten durch eine wirksame Einwilligung der Betroffenen oder eine Rechtsvorschrift erlaubt sein müssen. Daran fehlte es in diesem Fall. Einwilligungen der von der Videoüberwachung betroffenen Gäste konnte die Geschäftsführerin nicht vorlegen. Nach gefestigter Rechtsprechung willigen die Gäste durch das Betreten eines mit entsprechenden Videoüberwachungshinweisen versehenen Bereiches auch nicht konkludent in die Überwachung und die damit einhergehende Datenerhebung und -verarbeitung ihrer Bildaufnahmen ein. Die Videoüberwachung war zumindest aufgrund der überwiegenden schutzwürdigen Interessen der Gäste und der Beschäftigten, die sich dort aufhalten, während der Öffnungszeiten auch nicht nach § 6b BDSG erlaubt. Besondere Umstände, die im Einzelfall dazu führen können, den wirtschaftlichen Interessen von Gastronomen ein höheres Gewicht einzuräumen als den Interessen der betroffenen Gäste, konnte die Geschäftsführerin nicht darlegen. Ein Tresoraufbruch, der sich außerhalb der Öffnungszeiten ereignet hat und der Verkauf alkoholischer Getränke sind jedenfalls keine besonderen Umstände, die eine Videoüberwachung von Sitzbereichen während der Öffnungszeiten rechtfertigen können.

Das AG Hamburg ist unserer Begründung des Bußgeldbe-

scheids im Wesentlichen gefolgt und hat die Geschäftsführerin wegen der vorsätzlichen unbefugten Erhebung und Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind, zur Zahlung eines niedrigen vierstelligen Bußgeldes verurteilt. Das Gericht berücksichtigte mildernd, dass die Interessen der Beschäftigten aufgrund deren Einwilligung nicht berührt gewesen seien. Die Einwilligungserklärungen der Beschäftigten hatte die Geschäftsführerin erst in der mündlichen Verhandlung vorgelegt. Das Gericht hat wohl nicht näher geprüft, ob die vorgelegten Einwilligungen der Beschäftigten den Anforderungen des § 4a BDSG genügen und hier insbesondere, ob die Einwilligungen freiwillig erteilt wurden. Dies bedauern wir.

3. Bußgelder wegen Verwendung von Geodaten

Anschriftendaten allein dürfen nicht verwendet werden, um einer Person einen Scoringwert zuzuordnen.

Im Jahr 2016 erreichte uns die Beschwerde einer Petentin, die eine Selbstauskunft nach § 34 Bundesdatenschutzgesetz (BDSG) bei der Auskunftei Bürgel eingeholt hatte und mit dem Inhalt der Auskunft nicht einverstanden war. Ihr war mitgeteilt worden, dass über sie keine Daten gespeichert waren. Gleichzeitig hatte das Unternehmen in dem Jahr vor der Auskunftserteilung jedoch in zwei Fällen an andere Unternehmen einen Scorewert über die Petentin übermittelt, aus dem hervorging, dass die „Person unbekannt/Anschrift bekannt; Statistisches Ausfallrisiko: Durchschn." sei. Diese Auskunft an die anfragenden Unternehmen war durch Bürgel mit dem Zusatz versehen worden, dass der übermittelte Scorewert … keine Aussagekraft über die persönliche Bonität der Petentin (dort namentlich genannt) zulasse, da zu ihrer Person keine Informationen vorliegen würden.

Wir haben gegen Bürgel in dieser Sache ein Bußgeld in Höhe von 15.000€ erlassen, weil die Übermittlung der personenbezogenen Daten der Petentin unzulässig war. Für die Übermittlung eines Scorewertes über Personen, der allein auf der Anschrift beruht, gibt es keine Rechtfertigung. Zwar enthält das BDSG mit § 28b eine Regelung, die das Scoring grundsätzlich erlaubt, die darin vorgesehenen Voraussetzungen waren jedoch in keiner Weise erfüllt. Insbesondere wird ausdrücklich geregelt, dass für die Berechnung des Wahrscheinlichkeitswertes nicht ausschließlich Anschriftendaten genutzt werden dürfen.

Dagegen legte das Unternehmen Einspruch mit der Begründung ein, es habe sich nicht um personenbezogene Daten gehandelt, da über die Petentin ja keine Daten vorgelegen hätten, was auch den anfragenden Unternehmen mitgeteilt worden sei. Das Amtsgericht Hamburg (233 OWi 12/17) hat sich unserer Bewertung, dass es sich um personenbezogene Daten im Sinne des BDSG handelt, angeschlossen. Zwar wird man davon ausgehen können, dass die Erhebung und statistische Auswertung des statistischen Ausfallrisikos an einer Wohnadresse nicht in jedem Fall als personenbezogenes Datum anzusehen ist. Sobald dieses statistische Ausfallrisiko jedoch wie hier einer einzelnen Person zugeordnet wird, handelt es sich um eine Einzelangabe über persönliche und sachliche Verhältnisse einer bestimmten Person und damit um ein personenbezogenes Datum. Erkennbar ist dies auch schon daran, dass der Scorewert der Betroffenen direkt zugeordnet wird und gerade durch die Zuordnung zu ihrer Person auch Auswirkungen im Wirtschaftsverkehr haben kann. Maßgeblich dabei ist, dass die zunächst rein statistisch aus anonymisierten Daten ermittelten Scorewerte im zweiten Schritt einer konkreten Person zugeordnet werden und die Grundlage für eine Prognose über das wahrscheinliche Verhalten dieser Person in der Zukunft bilden.

Nachdem gegen das Urteil zunächst Rechtsbeschwerde eingelegt worden war, wurde diese später wieder zurückgezogen, sodass das Urteil rechtskräftig geworden ist.

Im Anschluss haben wir weitere 5 Fälle, die uns nach Einleitung des ersten Verfahrens bekannt geworden waren, mit einem Bußgeld in Höhe von jeweils 4.000€ belegt. Grund für die geringere Höhe der Bußgelder war die Tatsache, dass das konkret beanstandete Scoringverfahren eingestellt wurde. Die Verhängung dieser Bußgelder wurde ohne Einspruch rechtskräftig.

4. Safe Harbor und Privacy Shield - Kontrollen und Bußgeldverfahren

Im Berichtszeitraum haben wir auf die großen Veränderungen bei der Zulässigkeit von Datenübermittlungen in Drittländer reagiert und eine hohe Anzahl von Unternehmen geprüft.

Im Anschluss an die Entscheidung des Europäischen Gerichtshofs zur Zulässigkeit von Datenübermittlungen auf der Grundlage von Safe Harbor (ausführlich dazu 25. TB, X 1.) haben wir, wie bereits im 25. Tätigkeitsbericht angekündigt, Auskünfte über die Datenübermittlungen von Unternehmen in die USA eingeholt und im Anschluss daran auch rechtliche Maßnahmen ergriffen.

Zunächst schrieben wir im Januar 2016 weit mehr als 30 international agierende hamburgische Unternehmen an und befragten sie danach, ob und auf welcher Rechtsgrundlage sie Übermittlungen personenbezogener Daten in die USA vornehmen. Explizit wurde Auskunft darüber verlangt, ob solche Übermittlungen noch auf der Grundlage des mittlerweile ungültigen Safe Harbor-Abkommens erfolgen. Dabei stellte sich heraus, dass die weit überwiegende Anzahl der geprüf-

ten Unternehmen rechtzeitig nach Bekanntwerden der Unzulässigkeit der Verwendung von Safe Harbor eine Umstellung auf andere Instrumente der Datenübermittlung in Drittländer vorgenommen hatte. Lediglich in 3 Fällen waren im Anschluss an die Kontrolle Bußgeldbescheide geboten, die mittlerweile rechtskräftig geworden sind. Diese Unternehmen übermittelten auch nach einer Frist von mehr als einem halben Jahr nach dem Urteil des Europäischen Gerichtshofs personenbezogene Daten auf der Grundlage von Safe Harbor in die USA und handelten daher unzweifelhaft rechtswidrig. Erst im Laufe des Bußgeldverfahrens erfolgte jedoch auch dort eine Anpassung an zulässige Rechtsinstrumente.

Eine weitere Prüfung von Datenübermittlungen in Drittländer – unter Einbeziehung der Möglichkeit, auch das mittlerweile verabschiedete Privacy Shield verwenden zu können – wurde in 10 Bundesländern gleichzeitig ab November 2016 vorgenommen. In Hamburg haben wir insgesamt 11 Firmen geprüft. Dabei haben wir nicht, wie bei der Prüfung Anfang desselben Jahres, speziell international tätige Firmen ausgesucht, sondern bewusst darauf geachtet, dass einerseits sehr unterschiedliche Branchen geprüft werden und gleichzeitig sowohl große, als auch sehr kleine Unternehmen angeschrieben wurden. Auf diese Weise konnten wir überprüfen, ob auch kleineren Unternehmen bewusst ist, dass etwa die Nutzung von Clouddiensten durchaus mit der Übermittlung personenbezogener Daten in Drittländer verbunden sein kann.

Neben dem ausführlichen Anschreiben wurde jeweils ein Fragebogen übersandt, auf dem neben einer Reihe von Fragen die Antworten anzukreuzen waren. Ein beigefügtes Informationsblatt sorgte dafür, Missverständnisse zu vermeiden. Im Rahmen dieser Kontrolle zeigte sich die Vielfalt des Umgangs mit personenbezogenen Daten durch die angeschrieben Unternehmen. Einige übermittelten keine Daten in Drittländer, andere nur in die USA, wieder andere auch in sonstige Dritt-

staaten. Safe Harbor wurde nicht mehr verwendet, aber Privacy Shield kam bereits zum Einsatz, ebenso wie Einwilligungen, Standardvertragsklauseln und die Übermittlung in Staaten, für die eine Angemessenheitsentscheidung der EU-Kommission vorliegt. In keinem dieser Fälle mussten wir feststellen, dass unzulässige Übermittlungen personenbezogener Daten in Drittstaaten vorgenommen wurden. Auf weitere Maßnahmen konnte daher verzichtet werden.

Abgesehen von diesen Prüfungen in Hamburg haben wir 2016 nach einem Beschluss der Art. 29-Gruppe der EU-Kommission zusammen mit der Bundesbeauftragten für Datenschutz und Informationsfreiheit zum Thema Safe Harbor einen europaweiten Austausch zwischen den Aufsichtsbehörden organisiert. In einem ersten Schritt wurden alle Aufsichtsbehörden mit einem Fragebogen angeschrieben und darüber befragt, welche Schritte sie zur Umsetzung der Entscheidung des Europäischen Gerichtshofs zur Zulässigkeit von Datenübermittlungen auf der Grundlage von Safe Harbor in die Wege geleitet haben. Die Ergebnisse wurden in einer Sitzung unter Beteiligung der hessischen, französischen, spanischen und ungarischen Aufsichtsbehörde ausgetauscht. Dabei stellte sich heraus, dass die vorher teilweise noch offenen Fälle sich mittlerweile erledigt oder keinen grenzüberschreitenden Bezug in der EU hatten. Weitere Prüfungen, die eine europaweite Koordinierung durch die Aufsichtsbehörden erforderlich gemacht hätten, erübrigten sich daher.

5. XING – Bußgeldverfahren wegen unzulässiger Nutzung von Kontaktdaten rechtskräftig abgeschlossen

Unsere Ahndung der Verwendung von Adressdaten durch XING hat das Unternehmen zum Anlass genommen, Datenschutz zu einem Markenkern des Dienstes machen zu wollen.

Im Berichtszeitraum erhielten wir immer wieder Beschwerden im Zusammenhang mit Einladungs-E-Mails für das Netzwerk für berufliche Kontakte XING, die die Betroffenen ungefragt von Dritten zugesandt bekamen. Dies geschah, obwohl die Betroffenen weder selbst dem Netzwerk angehörten, noch dass sie bis zu diesem Zeitpunkt einen direkten Mailkontakt mit der einladenden Person hatten.

Nach unseren Recherchen und der Auskunft des Anbieters erfolgten diese zu Recht kritisierten Einladungen aufgrund einer Funktion namens „2nd degree invites". Über die Funktion „E-Mail-Kontakte zu XING einladen" haben Mitglieder die Möglichkeit, die Adressdaten von Kontakten aus ihren Webmail-Accounts oder bei mobiler Nutzung von ihren Endgeräten über einen Adressbuchupload an die XING SE zu übertragen. War einer der Kontakte bereits bei XING registriert, bestand die Möglichkeit, der betroffenen Person eine Anfrage für den Beitritt zum engeren Netzwerk der einladenden Person über die Plattform zu senden. Bei der Übertragung der Adressbuchdaten wurden häufig auch Kontakte von Personen hochgeladen, die noch nicht auf der Plattform registriert waren. In diesen Fällen wurde dem hochladenden Nutzer unmittelbar danach vorgeschlagen, diese Personen zur Registrierung auf die Plattform einzuladen. Sie erhielten dann eine entsprechende Einladungsmail von XING, in der die einladende Person kenntlich gemacht wurde.

Allerdings wurden die Kontaktdaten dieser Nichtnutzer von XING auch dann weiter gespeichert, wenn sie auf die Einladung nicht reagierten oder bereits keine Einladung an sie versandt worden war. Der Betreiber begann Mitte des Jahres 2015, die Kontaktdaten bisher nicht registrierter Nutzer auch anderen Mitgliedern als potentiellen Kontakt vorzuschlagen („2nd degree invites"). Diese Nutzer waren am Vorgang des ursprünglichen Adressbuchuploads nicht beteiligt. Wenn jedoch XING davon ausging, dass zwischen dem vom Upload betroffenen Nichtnutzer eine Beziehung zu dem anderen Mitglied bestehen könnte, konnte dieser Nutzer an den Nichtnutzer über die Plattform eine Einladungsmail versenden, um damit sein eigenes Netzwerk auf der Plattform zu erweitern. Der betroffene Nichtnutzer konnte sich durch das Anklicken eines Links in der Einladungs-Mail aus der Liste austragen lassen und die Kontaktdaten für die weitere Kontaktaufnahme sperren lassen.

Wir sahen in der Nutzung der Kontaktdaten der Nichtnutzer durch andere Nutzer des Dienstes als diejenigen, die die Daten bereitgestellt hatten, eine unzulässige Verarbeitung personenbezogener Daten. Denn XING konnte sich auf keine Rechtsgrundlage für diese Form der Datenverarbeitung berufen. Die Einladungsmails waren auf der Grundlage entsprechender Rechtsprechung des BGH nicht nur als Einladung des Mitglieds, sondern auch als Werbung für das Netzwerk zu bewerten. Für den Zweck der Werbung dürfen allerdings sowohl nach dem BDSG als auch dem UWG E-Mail-Adressen nur nach der vorherigen Einwilligung der Betroffenen genutzt werden.

Aufgrund des Umfangs der erhobenen Adressen und der aus unserer Sicht eindeutigen Rechtslage leiteten wir ein Bußgeldverfahren ein. Bereits während des Bußgeldverfahrens beendete das Unternehmen die beanstandete Praxis, verhielt sich auch im Verlauf des Verfahrens umfänglich kooperativ und war an einer datenschutzkonformen Lösung interessiert.

Dies konnte bei der Bemessung des Bußgeldes positiv gewürdigt werden.

Zudem nahm das Unternehmen das Verfahren zum Anlass, in einen regelmäßigen, inhaltlichen Austausch mit unserer Behörde bezüglich der Verbesserung der Geschäftsprozesse im Sinne des Privacy by Design zu treten. Das Unternehmen hat uns gegenüber dargelegt, Datenschutz zu einem Markenkern des eigenen Angebotes machen zu wollen. Wir begrüßen dies und haben unsere Bereitschaft erklärt, dies in dem durch die DSGVO gesetzten rechtlichen Rahmen und innerhalb unserer kapazitären Möglichkeiten zu unterstützen. Wir erwarten nun von dem Unternehmen, die selbst gesetzten Ziele umzusetzen.

6. Anordnung zu Privatsphäre-Bestimmungen bestandskräftig

Unsere langjährige Auseinandersetzung um die Profilbildung bei Google steht vor dem Abschluss. Google hat unsere Anordnung anerkannt und umgesetzt.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat im September 2014 im Wege der Anordnung das Unternehmen Google zu Maßnahmen verpflichtet, die die Verknüpfung von Nutzungs-, Bestands- und Inhaltsdaten verschiedener Google-Dienste in dem von Google durchgeführten Umfang datenschutzrechtlich zulässig macht (siehe 25. TB, V 1.3). Die Anordnung war Bestandteil einer mit anderen europäischen Aufsichtsbehörden (Frankreich, Großbritannien, Italien, Niederlande, Spanien) abgestimmten Reaktion auf eine Änderung der Datenschutzbestimmungen von Google, mit der eine dementsprechende Profilbildung verkündet wurde. Google hatte dagegen bereits 2015 Klage vor dem Verwaltungsgericht eingelegt.

Das Unternehmen hat in zweierlei Weise auf diese Anordnung reagiert. Zum einen wurden Anpassungen an den Google-Diensten vorgenommen und erheblich erweiterte Einwilligungen der Nutzer eingeholt, die den erhöhten Nutzungsumfang berücksichtigen – teilweise sogar über das von uns gefordert Maß hinaus. Zum anderen hat Google sich gerichtlich gegen unsere Anordnung gewehrt und dabei auch grundsätzliche Voraussetzungen wie unsere Zuständigkeit in Frage gestellt. Trotz dieser verfahrensmäßigen Bestreitung unserer Anordnung kamen die praktischen Umsetzungsprozesse unserer Anforderungen auf gutem Weg voran. Google bot so über lange Zeit ein recht widersprüchliches Bild zwischen Übererfüllung und Totalverweigerung.

Das gerichtliche Verfahren kommt nun jedoch zum Abschluss. Google hat gegenüber dem Verwaltungsgericht Hamburg (VG) eine Erledigungserklärung abgegeben, die auch die Übernahme der Gerichtskosten einschließt. Wir haben uns der Erledigung angeschlossen, so dass das Gericht über diesen Antrag entscheiden muss. Wir erwarten mit einem positiven Beschluss des VG dann den endgültigen Abschluss des Rechtsstreits.

Im Ergebnis wird die Anordnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit damit rechtskräftig. Dies ist für beide Seiten ein gutes Ergebnis, als es an der Umsetzung der wesentlichen Inhalte der Anordnung keine Zweifel geben kann. Lediglich ein nachrangiger Aspekt in Hinblick auf Dokumentationspflichten hinsichtlich der Umsetzung der Vorgaben ist nach wie vor offen. Hier liegt die Zusage der Google LLC vor, dies zügig zu erledigen.

Während die damalige Anordnung hauptsächlich auf die Desktop-Dienste von Google ausgerichtet war, hat sich mittlerweile die Nutzung weiter auf den Bereich der Smartphones verschoben. Das Android-System mit seinen vielfältigen Da-

tenerfassungen und -verarbeitungen liegt demgegenüber jedoch datenschutzrechtlich noch in großen Teilen im Dunkeln. Dass es dringend erforderlich ist, dort genauer hinzusehen, zeigen Vorfälle wie die Erhebung von Lokalisierungsdaten in Form von Mobilfunkzellen, auch wenn der Nutzer die Ortung des Geräts deaktiviert hat. Dies erfolgte seit Anfang 2017 auf allen Android-Geräten. Ob es sich um eine Art von technischem Pilotversuch handelte, ohne dass Google die Daten tatsächlich benötigt oder überhaupt ausgewertet hat, wie uns das Unternehmen auf Anfrage mitteilte, bleibt zu prüfen.

Dieser erstaunliche Vorgang lässt eine Reihe von Fragen offen. Wir haben daher angeregt, diesen Bereich auf europäischer Ebene stärker in den Blick zu nehmen. Dies stieß auf erhebliche Resonanz bei anderen europäischen Aufsichtsbehörden.

7. Google-Suchergebnisse – Verwaltungsgericht Hamburg weist Klagen gegen den HmbBfDI zurück

Das Verwaltungsgericht Hamburg hat festgestellt, dass es keinen Anspruch darauf gibt, den HmbBfDI zu verpflichten, aufsichtsbehördliche Maßnahmen bzw. Anordnungen gegen Dritte zu erlassen um geltend gemachte Rechte durchzusetzen. Vielmehr besteht nach derzeitiger Rechtslage bei Eingaben ein petitionsgleiches Recht auf Prüfung und Mitteilung.

In drei verwaltungsgerichtlichen Verfahren begehrten die Kläger die Verpflichtung des HmbBfDI, anzuordnen, dass die Google LLC die Entfernung von Suchergebnissen in deren Internetsuchmaschine vornimmt. Demgegenüber hat das Verwaltungsgericht Hamburg festgestellt, dass die Regelungen des BDSG den Betroffenen, die sich in ihren Rechten verletzt sehen, lediglich ein petitionsgleiches Recht auf Befassung vermitteln. Die Aufsichtsbehörde hat demnach die Eingabe

entgegenzunehmen, zu prüfen, und das Ergebnis mitzuteilen. Ein Anspruch auf ein bestimmtes Tätigwerden besteht hingegen nicht. Auch die Befugnis der Aufsichtsbehörden Anordnungen gegen für Datenverarbeitungen Verantwortliche zu erlassen, vermittelt Betroffenen kein subjektives Recht. Dieses Normverständnis ergibt sich aus dem Wortlaut, der Normsystematik, dem Normzweck und Wille des Gesetzgebers. Auch die Datenschutzrichtlinie 95/46/EG enthält eine klare systematische Trennung zwischen den Eingriffsbefugnissen der Kontrollstelle mit insoweit bestehendem Rechtsweg gegen beschwerende Eingriffe und andererseits dem jeder Person zustehenden Zugangsrecht mit der Verpflichtung der Kontrollstelle auf Befassung und Information der Betroffenen. Zudem hat der EuGH keine verbindliche Auslegung der Richtlinie vorgenommen, aus der sich eine Rechtswegeröffnung für Entscheidungen über Eingaben ergäbe. Das Verwaltungsgericht Hamburg hat damit unsere Auffassung zur derzeit geltenden Rechtslage bestätigt. Die Urteile sind bislang nicht rechtskräftig. In zwei Fällen wurde die Berufung zum Oberverwaltungsgericht zugelassen.

8. Facebook / WhatsApp – Geplanter Massendatenabgleich zunächst gestoppt – VG Hamburg bestätigt HmbBfDI

Durch rasches und entschiedenes aufsichtsbehördliches Vorgehen konnten wir erreichen, dass die Daten deutscher WhatsApp-Nutzer bislang nicht an Facebook übermittelt wurden.

Aufgrund entsprechender Pressemitteilungen über die Änderung der Nutzungs- und Geschäftsbedingungen des Betreibers des Kurznachrichtendienstes WhatsApp vom 25. August 2016 wurde uns bekannt, dass das Unternehmen u.a. die Telefonnummer und verschiedene technische Informationen seiner Nutzer an Facebook übermitteln wollte. Grundlage für

diese Übermittlung sollte die Einwilligung der Nutzer sein, die als Teil einer Änderung der Nutzungs- und Datenschutzbestimmungen von WhatsApp ausgestaltet war.

WhatsApp war im Jahr 2014 von Facebook übernommen worden. Aufgrund von Bedenken unter anderem der US-amerikanischen Federal Trade Commission bezüglich der Beachtung der Nutzerinteressen bei der Übernahme hatte WhatsApp im Jahr 2014 erklärt, ohne entsprechende Einwilligung der Nutzer keine Nutzerdaten zu übermitteln. WhatsApp schuf einen Vertrauenstatbestand, indem es erklärte: „Heute geben wir unsere Partnerschaft mit Facebook bekannt, die uns erlaubt, unsere einfache Mission fortzusetzen. … Und das wird sich für euch, unsere Benutzer, ändern: Nichts." (*https://blog.whatsapp.com/499/Facebook, 19. Februar 2014*)

Nach dem Bekanntwerden der geplanten Übermittlung der Daten der WhatsApp-Nutzer an Facebook prüften wir die datenschutzrechtliche Rechtmäßigkeit der eingeholten „Einwilligung". Wir waren und sind der Auffassung, dass die Informationen an die Nutzer unzureichend, teilweise sogar irreführend waren, die Nutzer keine echte Wahl hatten und zudem die gesetzlichen Anforderungen an die Freiwilligkeit der Erteilung der Einwilligung nicht erfüllt wurden. Diese Feststellung, der damit einhergehenden, möglichen Verletzung der Interessen von ca. 35 Millionen deutschen Nutzen und der Befürchtung, die Übermittlung könnte auch die Daten aus den Adressbüchern der Nutzer erfassen, leiteten wir ein aufsichtsbehördliches Verfahren gegen das Unternehmen Facebook als Empfänger der Daten ein. Eine Prüfung der Datenverarbeitung des Unternehmens WhatsApp war uns nicht möglich. Denn die Zuständigkeit für die Kontrolle der Einhaltung datenschutzrechtlicher Vorgaben durch WhatsApp liegt bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (vgl. III 5).

Insoweit forderten wir Facebook zu einer Stellungnahme auf. Wir sahen es aufgrund der bereits erwähnten Feststellungen und den durch das Unternehmen gegebenen Antworten für erforderlich an, gegen Facebook Ende September 2016 eine für sofort vollziehbar erklärte Anordnung zu erlassen. Denn es handelt sich hier um einen Austausch personenbezogener Daten zwischen zwei selbstständigen Unternehmen, ohne dass dafür eine entsprechende Rechtsgrundlage vorlag. Datenschutzrechtlich ist dabei unerheblich, dass beide Unternehmen derselben Unternehmensgruppe angehören. Facebook und WhatsApp verarbeiten die Daten ihrer jeweiligen Nutzer auf Grundlage ihrer eigenen Nutzungs- und Datenschutzbedingungen. Weder die Datenschutzrichtlinie noch die zukünftig geltende DSGVO kennen ein sogenanntes Konzernprivileg. Im Ergebnis bedeutet dies, dass die Übermittlung von personenbezogenen Daten von einer Tochtergesellschaft zu einer anderen Tochtergesellschaft wie die Übermittlung zwischen zwei Unternehmen bewertet werden muss, die nicht demselben Konzern angehören.

Auf europäischer Ebene formierte sich ebenfalls Widerstand gegen die Pläne der Unternehmen WhatsApp und Facebook, Nutzerdaten miteinander auszutauschen. Die Art.-29-Datenschutzgruppe richtete eine sogenannte Task-Force ein, an der auch wir beteiligt sind, und teilte WhatsApp im Oktober 2016 mit, dass sie nicht davon überzeugt sei, dass die Einwilligungen der Nutzer rechtswirksam seien.

Gegen die Anordnung legte Facebook Widerspruch ein und stellte den Antrag, die sofortige Vollziehung der Anordnung auszusetzen. Gleichzeitig erklärte das Unternehmen allerdings ebenfalls, keine Nutzerdaten deutscher WhatsApp-Nutzer zu erheben. Diese Festlegung hat das Unternehmen bisher nicht zurückgenommen. Im April 2017 entschied das Verwaltungsgericht Hamburg über den Antrag von Facebook zu unseren Gunsten. Es ging in seinem Beschluss einerseits

davon aus, dass die Behauptung Facebooks, nicht an deutsches Datenschutzrecht gebunden zu sein, nicht ohne Weiteres vertretbar ist und dass die Gründe zugunsten einer Aufrechterhaltung der Anordnung schwerer wiegen würden als die Gründe, Facebook die Erhebung der Daten zu erlauben. Das Gericht stellte fest, dass unsere Anordnung nicht offensichtlich rechtswidrig sei und kam zu dem Schluss, dass die Interessen Facebooks und WhatsApp an dem Datenaustausch nicht die Schutzinteressen der 35 Millionen deutschen WhatsApp-Nutzer überwiegen.

Gegen diese gerichtliche Entscheidung hat Facebook Beschwerde vor dem Oberverwaltungsgericht eingelegt. Das Gericht hat bisher nicht entschieden. Zwischenzeitlich hat in einem Verfahren des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vor dem EuGH, Generalanwalt Bot seine Stellungnahme u.a. zur Frage der Anwendbarkeit nationalen Datenschutzrechts abgegeben. Bemerkenswert daran ist, dass er die von Facebook unter anderem auch in unserem Verfahren vorgebrachten Argumente gegen eine Anwendung des nationalen Datenschutzrechts auf der Grundlage der bisherigen Rechtsprechung des EuGH verwirft. Wir sehen uns daher weiterhin auf dem richtigen Weg und bewerten die Stellungnahme des Generalanwaltes als Bestätigung für unsere, auch in diesem Gerichtsverfahren, vertretene rechtliche Position.

In der Branche der Anbieter von Telemedien, der sozialen Netzwerke und Dienstleister aller Art ist eine Tendenz zu Unternehmensaufkäufen und „Mergern“ zu erkennen, aus denen immer größere Konzerne entstehen. Es wird daher unserer Aufgabe sein, im europäischen Verbund eventuelle Übermittlungen von Informationen innerhalb solcher Konzerne zu überwachen und ggfs. die erforderlichen Maßnahmen zum Schutz der Grundrechte der betroffenen Nutzerinnen und Nutzer zu ergreifen.

V. BERATUNGEN UND DATENSCHUTZ-KOMMUNIKATION

1. Fortschritt nur mit weniger Sicherheit bei Endgeräten der FHH?

Mit der neuen Endgeräte-Richtlinie wird der bisherige Sicherheitsstandard reduziert.

„Die Bedeutung der Endgerätesicherheit wird in den nächsten Jahren deutlich steigen". Das war eine Kernaussage einer Veranstaltung des Innovationhubs. Diese Kooperation ist aus der Zusammenarbeit des Senats mit dem Unternehmen CISCO nach der Unterzeichnung des Memorandum of Understanding zwischen der FHH und dem Unternehmen 2014 hervorgegangen und dient dem Austausch von Behörden und Akteuren der privaten und der öffentlichen Wirtschaft zu digitalen Fragestellungen. Und wie sieht die Praxis aus? Im Berichtszeitraum wurde eine neue Endgeräte-Richtlinie in Kraft gesetzt. In dieser Richtlinie werden die technischen Mindestanforderungen für die Datensicherheit und den Datenschutz festgeschrieben. Sie regelt insbesondere den Betrieb für Arbeitsplatzrechner, Notebooks, Tablets und Smartphones und IT-Zubehör sowie die Nutzung privater Endgeräte und IT-Zubehör für die Verarbeitung dienstlicher Daten.

Das konnten wir erreichen:

- Grundsätzlich dürfen dienstliche Daten auf privaten Endgeräten nicht verarbeitet werden. Diesen Grundsatz, der in der bisherigen Richtlinie enthalten war, wollte die Finanzbehörde zunächst streichen. Diese Streichung konnten wir verhindern.

- Auch konnten wir erreichen, dass dienstliche Daten mit sehr hohem Schutzbedarf nicht auf privaten Endgeräten und Speichermedien verarbeitet werden dürfen. Dies sind z.B. Daten, bei deren Verarbeitung eine Gefährdung für Leib und Leben der Betroffenen bestehen kann, wenn die Sicherheit der Verarbeitung nicht gewährleistet ist.

Verschiedene kritische Knackpunkte konnten wir jedoch (noch) nicht verhindern:

- Mit der neuen Endgeräte-Richtlinie verlieren die IT-Stellen die Hoheit über die mobilen Geräte, die nicht vom IT-Dienstleister zentral administriert werden, also z.B. dienstliche Smartphones oder Tablets. Musste bisher auf allen dienstlichen Geräten die eingesetzte Software durch die IT-Stellen freigegeben werden, so kann jetzt jeder Nutzer in Eigenverantwortung zusätzliche Software auf den dienstlichen Geräten installieren. Zwar weist die Finanzbehörde drauf hin, dass der Benutzer sensible Daten bewusst auf das Endgerät überträgt und somit die Verantwortung trägt, wenn diese Daten mit einer von ihm installierten Software verarbeitet werden. Wie die Beschäftigten diese Verantwortung jedoch wahrnehmen sollen, ohne die Möglichkeit zu haben, z.B. neue Apps zu testen, ist völlig offen. Auch läuft der Hinweis der Finanzbehörde ins Leere, dass schutzwürdige Daten auf nicht zentral administrierten Endgeräten verschlüsselt zu speichern sind, da diese für die Verarbeitung auf dem mobilen Gerät unverschlüsselt vorliegen und dann ggf. zweckentfremdet werden können. Eine Maßnahme, um dieser Gefährdung zu begegnen, ist ein Mobile-Device-Management. Diese Maßnahme ist Stand der Technik. Dennoch hat die Finanzbehörde diese Schutzmaßnahme in der Endgeräte-Richtlinie nicht festgeschrieben. Wir setzen uns weiter dafür ein, dass dies realisiert wird. Die Finanzbehörde hat nun immerhin für Smartphones und Tablets ein „Proof of Concept (POC)“ angekündigt. Gleichzeitig sieht sie es aber nicht als Ziel an, mit einem solchen Mobile-Device-Management die Hoheit für diese Geräte wieder zu erlangen.

- Insbesondere vor dem Grundsatz von „Digital First“, der vom Senat proklamiert wird, ist lediglich eine „Anlehnung“ an die Standards des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), den Grundschutz, nicht ausreichend. Zum einen muss Grundschutz als Mindeststandard gewährleistet werden. Dazu gehören auch entsprechende Sicherheitsnachweise. Zum anderen sollte die

Infrastruktur auch auf hohen Schutzbedarf ausgerichtet werden und entsprechende Anforderungen gewährleisten, da Daten mit hohem Schutzbedarf regelmäßig in der FHH Infrastruktur verarbeitet werden. Mit der Formulierung „Orientierung an Grundschutz" hält sich die Finanzbehörde bewusst die Möglichkeit offen, nicht sämtliche Maßnahmen, die nach Grundschutz erforderlich wären, umzusetzen, sondern es reicht die Kenntnisnahme und die Risikoübernahme in einzelnen Fällen aus. Einer sicheren Verarbeitung dient dies jedoch dann nicht. Auch ist der Hinweis wenig hilfreich, dass für besonders zu schützende Anwendungen weitere Maßnahmen hinzukommen können, um den erhöhten Schutzanforderungen Rechnung zu tragen, wenn bereits in der bereitgestellten Infrastruktur regelhaft besonders schützenswerte Daten verarbeitet werden.

- Zwar wurde festgeschrieben, dass grundsätzlich von der jeweiligen Dienststelle bereitgestelltes IT-Zubehör (wie z.B. Kameras, USB-Sticks, Kopfhörer) an dienstlichen Endgeräten zu nutzen ist. Privates IT-Zubehör kann jedoch bei Vorliegen eines dienstlichen Interesses an die IT-Infrastruktur angeschlossen werden. Es wurden weder Kriterien für dienstliches Interesse genannt, noch wurde eine Anzeigepflicht für die Nutzung privatem IT-Zubehör eingefügt.

- Ergänzungen zu den Mindestanforderungen, die einzuhalten sind, wenn dienstliche Daten auf privaten Endgeräten verarbeitet werden, hat die Finanzbehörde nicht vorgenommen. Allein der Hinweis auf das „Merkblatt – Regelungen für die mobile IT-Nutzung (Mobiles Computing)", das auch für Zugriffe über das Internet auf die dienstliche Infrastruktur von externen privaten Rechnern einschlägig ist („Zuvex"), ist hierfür nicht ausreichend. Dort wird nicht einmal ein Kennwortschutz vorgeschrieben sondern nur „empfohlen". Auch können nach der aktuellen Endgeräte-Richtlinie dienstliche Daten mit hohem Schutzbedarf, wie z.B. Sozialdaten, auf privaten Rechnern verarbeitet werden.

Wenn personenbezogene Daten auf IT-Geräten nach Maßgabe der neuen Endgeräte-Richtlinie verarbeitet werden, werden die Anforderungen an § 8 HmbDSG nicht immer erfüllt, da nicht die erforderlichen Maßnahmen getroffen werden, um die Ausführungen der Vorschriften dieses Gesetzes zu gewährleisten. Aus diesen Gründen bleiben unsere Bedenken gegen die Endgeräte-Richtlinie bestehen.

2. Digitale Stadt

2.1 Koordinierungsrunde Digitale Stadt

Das Leitbild der Digitalen Stadt kann nur mit einer starken Datenschutzkomponente zu einem nachhaltigen Erfolg werden.

Hamburg hat sich auf den Weg hin zur „Digitalen Stadt" begeben. Dies ist u.a. Gegenstand entsprechender Senatsbeschlüsse und -drucksachen (siehe 25. TB, VI 2.1). Die dabei verfolgte Strategie sieht eine Reihe von zentral organisierten Strukturen vor, um die einzelnen fachlichen Aktivitäten zu koordinieren und zu unterstützen.

In der Senatskanzlei (Amt Medien) wurde dafür die Leitstelle Digitale Stadt geschaffen. Diese lädt u.a. zur „Koordinierungsrunde Digitale Stadt" ein, in der neben Fachbehörden auch viele andere wichtige Player (Hochschulen, Landesbetriebe, Hochbahn, Dataport etc.) vertreten sind. Unsere Behörde nimmt regelmäßig an diesen Runden teil, um die datenschutzrechtlichen Aspekte der dort vorgestellten Projekte in den Fokus zu rücken.

Diese Koordinierungsrunde arbeitet dem Lenkungskreis auf Ebene der Staatsräte zu, der letztlich entscheidungsgebend für Projekte und Themen der Digitalen Stadt ist. Auch dort ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit vertreten, so dass die institutionelle Einbindung unserer Behörde bei dem Thema gewährleistet sein sollte.

Wir beteiligen uns durch Stellungnahmen, fachliche Mitarbeit und Beratungen bei datenschutzrechtlichen Fragen in vielfältiger Weise an diesen Themen. Wir sind uns mit den Akteuren der verschiedenen Ebenen einig, dass die Digitale Stadt Hamburg nur dann ein Erfolg werden kann, wenn Datenschutz und Datensicherheit bereits konzeptionell und damit frühzeitig und durchgreifend berücksichtigt werden. Es gilt nun, dieses gemeinsame Verständnis in den konkreten Projekten umzusetzen.

2.2 Digital First – Pläne für eine digitale Verwaltung

Datenschutz und Datensicherheit müssen von Anfang an integraler Bestandteil der Projektarbeit sein.

Mit der Senatsdrucksache „Digital First – Chancen der Digitalisierung für eine bürgerfreundliche und moderne Verwaltung" (Drs. 2016/03060) werden insbesondere vier Leitlinien zur Nutzung der Digitalisierung festgeschrieben. So sollen die Dienstleistungen der Verwaltung zukünftig einfach und bequem, aufwands- und kostenarm, verlässlich und zügig sowie möglichst orts- und zeitunabhängig in Anspruch genommen werden können.

Ausdrücklich ist der Ansatz der Drucksache zu begrüßen, die Anforderungen des Datenschutzes und der Datensicherheit in der Planungsphase einzubeziehen. Die Beachtung der Datensicherheit und des Datenschutzes sind wesentliche und erfolgsentscheidende vertrauensbildende Faktoren gegenüber den Bürgerinnen und Bürgern. Daher sollte von Beginn an und standardmäßig der Stand der Technik im Hinblick auf Datenschutz und Datensicherheit garantiert und im gesamten Prozess der technischen und organisatorischen Umsetzung beachten werden (Privacy by Design).

Bei der organisatorischen und technischen Neuausrichtung

von Verwaltungsprozessen, die mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten einhergehen, sind die datenschutzrechtlichen Rahmenbedingungen hinreichend bestimmt und transparent gesetzlich zu verankern. Die Konzepte der rechtlichen, organisatorischen und technischen Optimierung von Verwaltungsprozessen, vor allem derjenigen, die den Basisdiensten zugrunde liegen, sollten aus unserer Sicht noch stärker konkretisiert werden. Dies gilt insbesondere für die Weiterentwicklung der rechtlichen Rahmenbedingungen des Datenschutzrechts. Wir haben daher erneut empfohlen, mit einem E-Government-Gesetz, wie dies im Bund und in anderen Bundesländern erlassen wurde, den notwendigen rechtlichen Rahmen für die Digitalisierung und Optimierung von Verwaltungsverfahren und -prozessen im Hinblick auf die Basisdienste und Fachverfahren zu schaffen. Hamburg sollte hier künftig nicht abseits stehen.

Die Leitlinien von Digital First

- Proaktive, insbesondere antragslose Erbringung von Verwaltungsdienstleistungen
  Soweit möglich soll die Verwaltung ihre Dienstleistungen initiativ erbringen und die Verfahren entsprechend proaktiv, etwa unter Reduzierung von Antrags- oder sonstigen Mitwirkungserfordernissen, durchführen. Die Zielsetzung, trotz der Verringerung der Datenverarbeitung dennoch bestimmte unterschiedslos gewährte Leistungen zu bescheiden, wird von uns begrüßt. Wie bereits allgemein festgestellt, bedarf dies jedoch einer entsprechenden gesetzlichen Regelung. Wir haben auch darauf hingewiesen, dass bei der Umsetzung dieses Prinzips mögliche stigmatisierende und diskriminierende Effekte vermieden werden müssen.

- Vermeidung von mehrfachen Dateneingaben
  Bürgerinnen und Bürger sollen dazu ihre Daten aus früheren Verfahren von den seinerzeit verfahrensführenden Behörden und Verwaltungseinheiten in dem Moment zur

Verfügung gestellt bekommen können, indem sie diese Daten im Zuge eines neuen Verfahrens benötigen (z.B. bei der Antragstellung). Es soll dann ausschließlich in der Entscheidung der jeweiligen Bürgerin, des jeweiligen Bürgers bzw. Unternehmens liegen, ob und mit welchen Änderungen diese Daten im neuen Verfahren verwendet und der hier verfahrensführenden Behörde oder Verwaltungseinheit übermittelt werden. Diese Zielsetzung haben wir ebenfalls ausdrücklich begrüßt. Wir werden im weiteren die Realisierung gerade unter dem Fokus eng begleiten, dass einerseits die Hoheit der Bürgerinnen und Bürger über diese verwendeten Daten bestehen bleibt und eine Nutzung nur mit ihrer ausdrücklicher Zustimmung und aktiven Mitwirkung möglich. Andererseits muss der Aufbau eines parallelen Verfahrens bzw. Datenspeichers (Data Warehouse) ausgeschlossen bleiben.

- Automatisierung

  Dieses Potenzial der Automatisierung soll nach den Vorstellungen des Senats, soweit rechtlich zulässig, stärker als bisher genutzt werden, um in geeigneten Verwaltungsverfahren eine Konzentration der personellen Ressourcen auf solche Verwaltungsarbeiten zu erreichen, die einer Ausführung durch den Menschen bedürfen. Was die digitalen Techniken übernehmen können, sollen sie grundsätzlich auch übernehmen.

  Wir haben hierzu auf die Gefahr hingewiesen, dass bestehende und gesetzlich vorgesehene Entscheidungsspielräume der Sachbearbeitung sowohl auf Tatbestands- als auch Rechtsfolgenseite durch automatisierte Prozesse verringert werden könnten. Eine benutzerorientierte IT-Unterstützung sollte die Sachbearbeitung gerade auf solche Entscheidungsspielräume hinweisen, die die Sachbearbeitung unter Würdigung aller entscheidungsrelevanten Umstände und des vorgesehenen gesetzlichen Rahmens verantwortlich nutzen. Automatisierte Einzelfallentscheidungen sollten nur im Rahmen gebundener Entscheidungen erfolgen. Sie müssen den Vorgaben von Art. 22 DS-

GVO folgen. Zudem sollte gesetzlich gewährleistet sein, dass auch diese Entscheidungen durch die individuelle Sachbearbeitung überprüft und revidiert werden können.

- Digitaler Zugang, digitale Kommunikation und digitale Dienstleistungen als Regel
  Um das Potenzial digitaler Technologien noch stärker zu nutzen, kündigt der Senat an, dass der Zugang zur und die Kommunikation mit der Verwaltung vorrangig digital ausgestaltet werden soll. Etwaige Verwaltungsgebühren sollen die Bürgerinnen, Bürger und Unternehmen online bezahlen können. Ihnen sollen dazu die gängigen, niedrigschwelligen und zuverlässigen Zahlungsmethoden angeboten werden. Für Bürgerinnen und Bürger, die digitale Angebote der Verwaltung nicht nutzen wollen oder können, sollen Unterstützungs- und Ergänzungsangebote entwickelt werden. Aufgrund unserer Stellungnahme wurde in die Senatsdrucksache auch mit aufgenommen, dass nach Möglichkeit auch anonyme und pseudonyme Bezahlsysteme angeboten werden sollen. Zudem haben wir eingefordert, dass bei der Inanspruchnahme von Unterstützungsangeboten dieselben Anforderungen an die Vertraulichkeit und Integrität der Kommunikation und Interaktion gewährleistet sein müssen. Bereits in der Phase der Planungen sollten dies explizit verdeutlicht werden.

Bezüglich der Ausgestaltung der zentralen technischen Infrastruktur waren wir eng in den Planungsprozess eingebunden. Dagegen haben wir zwar wiederholt die Aufarbeitung der anstehenden rechtlichen Rahmenbedingungen eingefordert, diese sind jedoch noch kaum vorangeschritten. Seit Sommer 2017 befindet sich das Projekt Digital First in einer Phase der Neuausrichtung, mit der eine stärkere Orientierung an einigen wenigen schnell realisierbaren Pilotprojekten erfolgen soll. Bei einem solchen Vorgehen ist wichtig, dass auch hier die Gewährleistung der Datensicherheit und des Datenschutzes umfassend erfolgt und weder zeitlich nach hinten verschoben wird, noch an Bedeutung verliert.

2.3 Strategie Intelligente Transportsysteme (ITS)

Mit der Strategie Intelligente Transportsysteme soll die digitalisierte Mobilität in Hamburg Fahrt aufnehmen. Datenschutz muss Beifahrer sein und darf nicht auf der Strecke bleiben.

Mit der Senatsdrucksache 2016/00784 „Strategie Intelligente Transportsysteme für Hamburg" hat der Senat seine Zielvorstellungen aus der Drucksache 2015/0014 „Strategie Digitale Stadt" (vgl. 25.TB, VI 2.1) für den Bereich intelligenter Verkehrssysteme konkretisiert.

Ziel ist, bis etwa 2030 die verschiedenen Verkehrssysteme durch Digitalisierung und Vernetzung so zu optimieren und in eine Rahmenarchitektur einzubinden, dass diese zu größerer Verkehrssicherheit, Verlässlichkeit, Effizienz und Umweltschutz beitragen sowie sonstige, im Einzelnen noch nicht absehbare Mehrwerte generieren und Hamburg dadurch eine führende Position im Bereich intelligenter Mobilität einnimmt. Dazu soll auch die Ausrichtung des ITS-Weltkongresses im Jahr 2021 beitragen, um die man sich 2017 erfolgreich beworben hat.

Zur Umsetzung wurden acht Handlungsfelder (Daten, Informationen, Intelligente Verkehrssteuerung und -lenkung, Intelligente Infrastruktur, Intelligentes Parken, Mobilität als Service, Intelligente Fahrzeuge, Innovationsförderung) mit jeweils einer Vielzahl von Projekten ins Auge gefasst, um aus der Vielfalt technischer Innovationen die für den öffentlichen Sektor und für Hamburg relevanten Entwicklungen zu identifizieren, zu bewerten und zu fördern.

Bereits frühzeitig hatten wir darauf hingewiesen, dass es das Thema Datenschutz als Querschnittsthema nicht nur in den Handlungsfeldern Daten und Information, sondern in allen Handlungsfeldern und Einzelprojekten erfordert, frühzeitig zu klären, inwieweit personenbezogene Daten betroffen

sind und ob die bestehenden gesetzlichen Anforderungen eingehalten werden können bzw. ausreichend sind.

Zur Umsetzung der Strategie wurde eine umfängliche Projektstruktur entwickelt. Neben Lenkungs- und Arbeitskreis, an denen wir jeweils beratend teilnehmen, wurde als Bindeglied zwischen den Handlungsfeldern und den konkreten Projekten eine weitere Ebene, die so genannten „Paten", etabliert. Zur Sensibilisierung haben wir Hinweise zu einer vorgezogenen Datenschutzprüfung eingebracht, die in einem anstehenden Workshop für Paten und Projektleiter erläutert und vertieft werden sollen. Mit wenigen einzelnen Projekten hat es bereits konkretere Gespräche gegeben.

Zu Redaktionsschluss wurde mitgeteilt, dass das auch vom Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) geförderte Thema „Automatisiertes und vernetztes Fahren" (dt. AvF, engl. c-its) im Handlungsfeld „Intelligente Fahrzeuge" exemplarisch und schwerpunktmäßig verfolgt und datenschutzrechtlich betreut werden solle. Dieser Bereich ist gekennzeichnet durch die Schlagworte Vehicle-to-Vehicle-, Vehicle-to-Infrastructure- und Vehicle-to-X-Kommunikation, wobei die Vernetzung derzeit lediglich die Kommunikation zwischen Fahrzeugen untereinander und zur Infrastruktur über vorgeschriebene Standards abgedeckt werden kann, für die sichere Kommunikation mit sonstigen Verkehrsteilnehmern (Vehicle-to-X) verlässliche Systeme aber offenbar noch fehlen.

Die datenschutzrechtliche Beratung in diesem Bereich begegnet vielfältigen Herausforderungen:

a) Kapazität und Zuständigkeit
Nicht zuletzt wegen der bei Redaktionsschluss in den verschiedenen Handlungsfeldern etwa 60 aktiv gesetzten Projekte ist eine umfassende proaktive Beratung mit den vor-

handenen Ressourcen durch unsere Behörde derzeit nicht leistbar. Dies gilt insbesondere vor dem Hintergrund, dass die Einzelprojekte völlig unterschiedliche Komplexität und Entwicklungsstadien aufweisen, und zwar vom (unverbindlichen) Ideenstadium bis hin zu eingeführten Projekten. Wir haben daher gebeten, dass die Projekte bei datenschutzrechtlichen Fragen unmittelbar selbst auf uns zukommen mögen.
Hinzu kommen der noch unklare Rechtsrahmen (siehe unter b) und das unter der Ägide der Datenschutzgrundordnung (DS-GVO) künftig verstärkt erforderliche und daher schon im Berichtszeitraum zu berücksichtigende Erfordernis einer zumindest europaweit möglichst einheitlichen Meinungsbildung. Unsere Behörde kann damit letztlich allein weder verbindliche Vorgaben für Hamburgische Behörden und erst recht nicht für private international und auch außereuropäisch agierende Player formulieren. Gleichwohl engagieren wir uns sowohl in der Begleitung des Projekts als auch in der datenschutzpolitischen Diskussion, um das Thema voranzubringen. Dabei bleibt es nicht aus, dass einzelne Handlungsfelder intensiver im Fokus sind als andere.

b) Rechtlicher Rahmen

Datenschutz hat die Rechte jedes einzelnen Verkehrsteilnehmers, egal in welcher Rolle, zu wahren, und zwar von der personenbezogenen Datenerhebung bis zur Löschung oder unumkehrbaren Anonymisierung; intelligente Verkehrslösungen bauen dagegen auf umfassende und vernetzte Datenverarbeitung, der sich der einzelne insbesondere im Bereich des Straßenverkehrs nicht entziehen kann. Diesen Zielkonflikt gilt es angemessen auf möglichst breiter Ebene zu lösen.
Dabei ist in dem eher international orientierten Verkehrsbereich nicht immer leicht zugrunde zu legen, welche Daten in welchen Zusammenhängen als personenbezogen behandelt werden müssen. Dies unterliegt zum einen mitglieds-

staatlichen Regelungen. So gelten in Deutschland anfallende Fahrzeugdaten aufgrund der Tatsache, dass Kennzeichen und Fahrzeugidentnummer gesetzlich als personenbezogen definiert sind, ebenfalls als personenbezogen. Die Frage des Personenbezugs von IP-Adressen ist erst kürzlich auf europäischer Ebene gerichtlich geklärt worden. Auch die Rechtsvereinheitlichung im Zuge der DSGVO und die damit einhergehende Verstärkung der Zusammenarbeit der Datenschutzaufsichtsbehörden wird hier zu einer Vereinheitlichung beitragen.
Die bestehenden rechtlichen Regelungen auf europäischer und Bundesebene bieten bislang noch keinen hinreichend bestimmten, dem Gesetzesvorbehalt genügenden Rechtsrahmen, der zu diesem komplexen Thema auch nur annähernd einen angemessenen Ausgleich zwischen öffentlichen Interessen und den Interessen der Betroffenen herbeiführt.
Die europäischen Regelungen kennen bisher nur beim Unfall-Notrufsystem eCall konkrete datenschutzrechtliche Anforderungen, beschränken sich bei der Zielsetzung intelligenter Verkehrssysteme bisher aber darauf, dass diese, soweit personenbezogene Daten verarbeitet werden, den sehr allgemeinen Regelungen der EG-Datenschutzrichtlinie, künftig also denen der Datenschutzgrundverordnung (DSGVO) genügen müssen.

Wir haben uns im Berichtszeitraum deshalb auf den verschiedensten Ebenen dafür eingesetzt, für den Bereich ITS hinreichend bestimmte spezialgesetzliche Grundlagen zu schaffen.

- Im Rahmen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) haben wir uns mit der Entschließung „Gesetzentwurf zur Aufzeichnung von Fahrdaten völlig unzureichend“ erfolgreich für eine Konkretisierung der datenschutzrechtlichen Anforderungen im Zusammenhang mit der Novellierung des Straßenverkehrsgesetzes (StVG) zur Regelung automatisierten

und teilautomatisierten Fahrens eingesetzt. Thematisch bezieht sich die Entschließung jedoch im Wesentlichen auf haftungsrechtliche Regelungen.

- Im Rahmen der Internationalen Datenschutzkonferenz (ICDPPC) in Hongkong vom 25. - 29.9.2017 haben wir den von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eingebrachten Entwurf einer Entschließung zu automatisierten und vernetzten Fahrzeugen unterstützt und die Aufnahme weiterer Forderungen zum Einsatz Algorithmen gestützter Entscheidungen („Künstliche Intelligenz") eingebracht.
- Im Rahmen der Artikel-29-Gruppe, die seitens der EU-Kommission hinsichtlich einer speziellen technischen Ausgestaltung der Fahrzeugvernetzung über unverschlüsselte, aber zertifizierte Nachrichten konsultiert wurde, haben wir erfolgreich die Forderung nach einer spezialgesetzlichen Regelung des Themas auf europäischer Ebene in die Stellungnahme eingebracht ebenso wie im Übrigen die Übernahme der Forderungen der ICDPPC.

c) Künstliche Intelligenz

Daneben haben wir uns sowohl gegenüber dem Deutschen Ethikrat zu seiner Jahrestagung zum Thema „Autonome Systeme" als auch gegenüber der vom BMVI eingesetzten „Ethik-Kommission „Automatisiertes und vernetztes Fahren" dafür eingesetzt, auch die Problematik des Einsatzes künstlicher Intelligenz in Form der in Fahrzeugen und Infrastruktureinrichtungen implementierten Algorithmen und der auf sie gestützten automatisierten Einzelentscheidungen zu thematisieren:

Die Zulassung einer Technik, die über Leben und körperliche Unversehrtheit aller am Straßenverkehr teilnehmenden Menschen entscheidet, muss vom Gesetzgeber gewollt, angemessen und abschließend geregelt werden und darf nicht auf die bloße meist interessengeleitete Auslegung der allgemeinen Verarbeitungsregelungen nach DSGVO durch die Anwender, von den Autoherstellern über Infrastrukturanbie-

ter bis zu Start-Ups mit unterschiedlichsten Geschäftsideen, gestützt werden. Der insoweit nach derzeitiger Rechtslage allein anwendbare Art. 22 DSGVO lautet:

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.
(2) Absatz 1 gilt nicht, wenn die Entscheidung
a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.
(3) In den in Absatz 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.
(4) Entscheidungen nach Absatz 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 beruhen, sofern nicht Artikel 9 Absatz 2 Buchstabe a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

Zu den unter dem Aspekt des Profiling geschützten Bereichen gehören nach Erwägungsgrund 71 auch Auswer-

tungen von Verhalten, Aufenthaltsort und Ortswechsel. Die Vorgaben in Art. 22 DSGVO werden gegenwärtig mit Blick auf das automatisierte Fahren und den Einsatz von selbstlernenden Systemen nicht erfüllt: Die Entscheidungen automatisierter Systeme dienen nicht der Erfüllung eines Vertrages und können auch wirksam nicht auf eine Einwilligung aller nur denkbaren Betroffenen gestützt werden; durch die auf Algorithmen basierten Einzelentscheidungen können die Betroffenen (Fahrer sowie alle anderen denkbaren Verkehrsteilnehmer) zudem an Leib und Leben in erheblicher Weise beeinträchtigt werden.
Leider konnten diese Hinweise von der Ethik-Kommission in ihrem Bericht „Automatisiertes und vernetztes Fahren" aus zeitlichen Gründen nicht mehr berücksichtigt werden.

d) Generierung von Mehrwerten
Auch im Bereich ITS bestehen weitgehend Erwartungen unter dem Stichwort Big Data, einmal angefallene Daten zu vernetzen und für weitere, auch verkehrsfremde Zwecke nutzen zu können. Ohne eine spezifische unions- oder mitgliedsstaatliche Regelung, die ausdrücklich mögliche weitere Zwecke zulässt und Umfang und Grenzen der Bearbeitung regelt, werden die Grenzen des Art. 6 DSGVO zu beachten sein. Nach dem dazu gehörigen Erwägungsgrund 50 kann eine weitere Verarbeitung nur für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche Forschungszwecke oder für statistische Zwecke angenommen werden. Der Betrieb personenbezogener Datawarehouses ist per se weiterhin nicht zulässig. Vor diesem Hintergrund werden Fragen nach hinreichender Anonymisierung und zu Gefahren der Reidentifizierbarkeit an Bedeutung gewinnen, die für jeden Zweck neu geprüft und daher nicht pauschal vorab geklärt werden können.

e) ITS-Testfeld Hamburg
Hamburg wird im Jahre 2021 den ITS-Weltkongress aus-

tragen und strebt bis dahin den Aufbau von Testfeldern für verschiedene Anwendungsszenarien an. Sowohl Wirtschaftsunternehmen als auch wissenschaftlichen Forschungsinstitutionen soll die Möglichkeit der Teilnahme eröffnet werden. Zum Teil werden die Anwendungen ohne Personenbezug arbeiten. Überwiegend werden jedoch personenbezogene Daten zur Grundlage der Verarbeitung gemacht. Dies gilt insbesondere auch für den Bereich des automatisierten und vernetzten Fahrens.

Grundsätzlich haben die Betroffenen aber auch im öffentlichen Straßenraum das Recht, sich unbeobachtet zu bewegen. Erst recht müssen sie sich ohne entsprechende Wertentscheidung des Gesetzgebers keinen Daten verarbeitungsbedingten erhöhten Gefährdungen von Leib und Leben aussetzen.

Auch hier gilt der Gesetzesvorbehalt: Sobald durch die Verarbeitung personenbezogener Daten in das informationelle Selbstbestimmungsrecht eingegriffen wird, bedarf es hinreichend bestimmter Befugnisnormen, die Art und Umfang der Verarbeitung zulassen. Zusätzlich ist dann die Sicherheit der Verarbeitungsvorgänge und der Daten nach § 8 HmbDSG, künftig nach Art. 32 DSGVO, zu gewährleisten. Dazu gehören auch der Grundsätze „Keine Testung mit Echtdaten“ und „Pilotierung mit Echtdaten ausschließlich unter Einhaltung aller datenschutzrechtlichen Anforderungen“ (vgl. u.a. die Orientierungshilfe „Datenschutz und Datensicherheit in Projekten“ der Datenschutzkonferenz des Bundes und der Länder, 2009, Seiten 3, 5). Typischerweise erfolgt die Testung zweckgebunden erst auf der Grundlage bestehender Befugnisnormen. Soll im Bereich der ITS-Strategie dieses Verhältnis nun umgekehrt und die Testung zu allgemeinen Erprobungszwecken von Technik im Rahmen eines Echtbetriebs auf Hamburger Straßen vorverlegt werden, ist jeweils zu prüfen, ob bestehende Vorschriften hierfür, etwa zur

gesetzlich definierten Aufgabenwahrnehmung öffentlicher Stellen, bereits ausreichen oder zusätzliche Regelungen geschaffen werden müssen.

Schon frühzeitig hatten wir deshalb darauf hingewiesen, dass außerhalb des Bereichs wissenschaftlicher Forschung Behörden und assoziierten Unternehmen ein Probe- oder Testbetrieb mit Echtdaten ohne ausdrückliche gesetzliche Grundlage nur unter engen Voraussetzungen möglich ist und jedenfalls dann nicht in Betracht kommen kann, wenn potentiell jedermann von dieser Verarbeitung betroffen ist. Vor allem darf eine solche Vorgehensweise dann nicht die weitest mögliche Testung unter Laborbedingungen ersetzen. Das StVG und die konkretisierenden Vorschriften der Straßenverkehrsordnung (§ 6 Abs. 1 Nr. 16 StVG i.V.m. § 45 Abs. 1 StVO) kennen bisher nur die Möglichkeit, die Straßennutzung zur Erforschung des Verkehrsverhaltens, des Unfallgeschehens oder zur Erprobung verkehrssichernder und verkehrsregelnder Maßnahmen zu beschränken. Eine Regelung zum Umgang mit personenbezogenen Daten zu Testzwecken im Normalverkehr enthalten die Erprobungsregelungen bisher nicht.

Nach Auskunft des Projekts ergebe sich das im Internetauftritt des BMVI aufgeführte „Testfeld Hamburg" lediglich konkludent aus der Förderung nach der Förderrichtlinie des BMVI „Automatisiertes und vernetztes Fahren auf digitalen Testfeldern in Deutschland". Das BMVI bezeichnet dort die Testfelder gerade nicht als abgeschlossene Testgelände, sondern als „Labor unter Realbedingungen".

Wir haben nochmals nach der Entscheidung über die Austragung des ITS-Weltkongresses 2021 die Prüfung der Schaffung einer gesetzlichen Grundlage angeregt und unsere Beratung angeboten.

3. Smart Meter Rollout in Hamburg

Die Stromnetz Hamburg GmbH bereitet die flächendeckende Einführung von intelligenten Messsystemen und modernen Messeinrichtungen vor.

Die Digitalisierung der Energiewende hat begonnen. Mit dem Messstellenbetriebsgesetz (MsbG) hat der Gesetzgeber den Grundstein für eine neue Mess- und Kommunikationsinfrastruktur gelegt. Damit besteht eine Verpflichtung zur Modernisierung der Messstellen. Bis 2032 sollen alle im Hamburger Stadtgebiet befindlichen Stromzähler durch intelligente Messsysteme und moderne Messeinrichtungen ersetzt werden. Die Stromnetz Hamburg GmbH muss diesem gesetzlichen Auftrag entsprechen und hat den Smart Meter Rollout dem HmbBfDI vorgestellt.

Gesetzgeberisches Ziel ist der Aufbau eines intelligenten Energieversorgungsnetzes. Dieses soll den steigenden Anteil erneuerbarer Energien mit der Stromnachfrage harmonisieren. So sollen Verbraucher in die Lage versetzt werden, verbrauchsintensive Geräte gezielt dann einzuschalten, wenn besonders viel Strom eingespeist wird und damit günstiger ist. Daneben können Smart Meter weitere Zwecke erfüllen, wie die Identifikation von „Stromfressern".

Ein solches Modell birgt allerdings Risiken für das Recht auf informationelle Selbstbestimmung. Aus Verbrauchsmenge und -zeitpunkt können Einblicke in die private Lebensgestaltung gewonnen werden. Je granularer dabei Verbrauchsdaten gespeichert und übermittelt werden, desto präziser können diese Rückschlüsse erfolgen. Auch die unmerkliche Datenerhebung durch die automatische Übermittlung stellt eine Gefahr dar. Das Ziel größtmöglicher Vernetzung steht damit im Widerspruch zum Gebot sparsamer Datenerhe-

bungen. Diesen Konflikt hat das MsbG teilweise sinnvollen Lösungen zugeführt.

Den gesetzlichen Vorgaben entsprechend kommt unterhalb eines Jahresverbrauchs von 6.000 kWh grundsätzlich eine moderne Messeinrichtung zum Einsatz. Diese verfügen nicht über eine Kommunikationseinheit und bieten daher keine Möglichkeit fernausgelesen zu werden. Es handelt sich damit um elektronische Zähler, die im Unterschied zu den derzeit verwendeten Ferraris-Zählern, die Verbrauchshistorie speichern und ausschließlich lokal anzeigen können. Die Übertragung des Verbrauchswertes erfolgt wie bisher über analoges Ablesen und Übermitteln. Der Großteil der Haushalte der Hamburgerinnen und Hamburger wird nach Angaben der Stromnetz Hamburg GmbH aufgrund dieser Verbrauchsschwelle mit modernen Messeinrichtungen ausgestattet werden. Nach Schätzungen sind dies rund 90% der hamburgischen Haushalte.

Oberhalb dieser Verbrauchsschwelle kommen intelligente Messsysteme zur Anwendung. Dabei handelt es sich um moderne Messeinrichtungen, die um ein sog. Gateway erweitert sind. Diese Gateways ermöglichen die Kommunikation und damit die Fernauslesung der Verbrauchsdaten. Aufgrund der Fernauslesung sind sie geeignet, das Recht auf informationelle Selbstbestimmung zu gefährden. Dementsprechend sind die Anforderungen an die technische Sicherheit der Geräte und der Übertragung hoch.

Das MsbG sieht eine Zertifizierungspflicht sowohl der ‚Smart-Meter-Gateways', als auch des sog. ‚Smart-Meter-Gateway-Administrators' vor. Die Zertifizierungen werden durch das Bundesamt für Sicherheit in der Informationstechnik vorgenommen. Daneben sind weitere Schutzmechanismen vorgesehen. So werden bei einem Verbrauch unter 10.000 kWh lediglich Jahresverbrauchswerte übertragen.

Oberhalb dieser Verbrauchsschwelle kann die Auslesung in 15-minütiger Auflösung erfolgen. Das Gesetz begrenzt die zum Datenumgang Berechtigten sowie die Zweckrichtung der Datenverarbeitungen.

Dieses Maßnahmenkorsett ist geeignet, die Gefahren für das Recht informationeller Selbstbestimmung zu begrenzen. Durch das Abstufungssystem im Hinblick auf die Jahresverbrauchswerte werden sich die überwiegende Zahl der Hamburgerinnen und Hamburger einer granularen Fernauslesung nicht ausgesetzt sehen.

Trotz dieses positiven Befundes darf nicht verkannt werden, dass das MsbG eine Verpflichtung zur Digitalisierung beinhaltet. Der verpflichtende Einbau stellt ein Einfallstor zur Einschränkung der informationellen Selbstbestimmung dar. So kann der Messstellenbetreiber auch unterhalb der Verbrauchsschwelle von 6.000 kWh intelligente Messsysteme installieren. Die Ausstattung steht dabei weitgehend im Ermessen des Messstellenbetreibers und ist insbesondere nicht von einer Einwilligung des Anschlussinhabers abhängig. Die Stromnetz Hamburg GmbH hat uns indes bisher keine Pläne vorgestellt, ob diese Norm zur Anwendung kommen soll.

Anschlussteilnehmer können sich darüber hinaus auch freiwillig für den Einbau eines intelligenten Messsystems entscheiden. Mittels Einwilligungen können ferner weitere, zweckfremde Datenübermittlungen ermöglicht oder Verbrauchsinformationen über ein Onlineportal sichtbar gemacht werden. Derartige Einwilligungen sind kritisch zu sehen. Das MsbG stellt allein auf die Einwilligung des Anschlussnutzers ab und lässt die Rechte anderer Betroffener, wie etwa Mitbewohner, unberücksichtigt. Eine Lösung für diese Problematik ist bisher nicht in Sicht.

Wir werden in allen Prozessstadien, auch im Hinblick auf die

vorgenannten Fragestellungen, unser Augenmerk auf die Umsetzung des Rollouts richten.

4. Videoüberwachungskonzept für Einkaufszentren

Nach dem Inkrafttreten des Videoüberwachungsverbesserungsgesetzes wird die Videoüberwachung in Einkaufzentren voraussichtlich ausgeweitet werden.

Im Berichtszeitraum wandte sich ein Unternehmen an uns und bat um Beratung über die Voraussetzungen eines datenschutzkonformen Einsatzes von Videoüberwachungstechnik auf der Grundlage des Videoüberwachungsverbesserungsgesetzes. Das Unternehmen betreibt bundesweit eine große Anzahl von Einkaufszentren. Gegenüber diesem Unternehmen hatten wir im Jahr 2010 angeordnet, die auf die Ladenpassagen/Ladenstraßen gerichteten Kameras eines in Hamburg gelegenen Einkaufszentrums abzubauen (vgl. 23. TB, IV 1.2). Dieser Anordnung folgte das Unternehmen und es baute die entsprechenden Kameras auch in seinen anderen Einkaufzentren im Bundesgebiet ab. Mit dem Inkrafttreten des Videoüberwachungsverbesserungsgesetzes haben sich die Voraussetzungen für einen datenschutzkonformen Einsatz von Videoüberwachungstechnik in Einkaufszentren geändert (vgl. 26. TB, III 1.). Auch wenn erhebliche verfassungsrechtliche Bedenken gegen die neue Regelung bestehen, haben wir sie zu beachten und anzuwenden. Dies gilt jedenfalls für den Zeitraum bis zur unmittelbaren Anwendbarkeit der Datenschutzgrundverordnung (DSGVO). Sollte diese Regelung im Widerspruch zur DSGVO stehen, wofür unseres Erachtens vieles spricht, geht die Regelung der DSGVO grundsätzlich der innerstaatlichen Bestimmung vor.

Wir begrüßen die Initiative des Unternehmens, vor der ge-

planten Ausweitung der Videoüberwachung auf Ladenpassagen und Ein-/Ausgänge den Austausch mit uns zu suchen. Umso bedauerlicher ist es, dass das vom Unternehmen vorgelegte Grobkonzept aus Kostengründen kein Live-Monitoring vorsieht. Wenn Videoüberwachungsmaßnahmen überhaupt eine präventive Wirkung im Sinne einer Verhinderung von Straftaten entfalten können, dann setzt dies ein Live-Monitoring durch Sicherheitsmitarbeiter und nicht nur eine Speicherung der Bilddaten voraus. Ansonsten ist kein Eigreifen möglich, die Bilder können lediglich für die Rekonstruktion einer Straftat hilfreich sein. Den Opfern ist damit in aller Regel wenig geholfen.

Wir haben mit der Betreiberin der Einkaufzentren in zwei Gesprächen die folgenden datenschutzrechtlichen Eckpunkte einer auf das Videoüberwachungsverbesserungsgesetz gestützten Ausweitung der Videoüberwachung erörtert:

- Gegen ein im Vergleich zur Speicherung der Bilddaten weniger eingriffsintensives Monitoring der Bereiche bestehen keine datenschutzrechtlichen Bedenken. Dies ist sogar wünschenswert.
- Gegen eine anlassbezogene Speicherung von Bilddaten bestehen ebenfalls keine datenschutzrechtlichen Bedenken. Dies bedeutet, dass immer dann, wenn ein konkreter Verdacht im Hinblick auf die Begehung von Straftaten oder Amokläufen im Einkaufszentrum besteht, eine Videoüberwachung selbstverständlich zulässig ist.
- Eine anlasslose Speicherung der Videodaten während der Geschäftszeiten eines Einkaufszentrums könnte im sog. Black-Box-Verfahren ebenfalls zulässig sein. Dies legt die Gesetzesbegründung nahe, die als Ziel der Regelung auch die Erleichterung der Ermittlungstätigkeit von Polizei und Staatsanwaltschaft anführt. Den Interessen der von der Videoüberwachung betroffenen Besucher der Einkaufzentren kann in solchen Fällen durch eine kurze Speicherdauer Rechnung getragen werden. Eine entsprechend kurze Speicherdauer sieht das Konzept des Betreibers vor. Außerhalb

der Geschäftszeiten könnte auch eine längere Speicherung der Daten zulässig sein.

- Bereiche des Einkaufzentrums, in denen sich Menschen typischerweise länger zur Erholung und zur Entspannung aufhalten, sind von der Videoüberwachung auszunehmen. Hierzu zählen insbesondere die Gastronomiebereiche eines Einkaufszentrums, also insbesondere die Food-Courts. Dies kann durch den Einsatz eines Privacy-Filters erfolgen, der bei dem Verdacht einer Terror- oder Amoklage sofort aufgehoben werden kann.
- Ein direkter Zugriff der Polizei auf die Videoüberwachungsanlage der Einkaufzentren im Fall von Terror-/Amoklagen kann ebenfalls zulässig sein. Dies richtet sich nach dem Polizeirecht der jeweiligen Länder.

Wir werden die konstruktiven Gespräche mit dem Unternehmen im Jahr 2018 fortführen.

5. Vertretung der Bundesländer in der Artikel 29-Gruppe

Hamburg vertritt die Länderinteressen bei der gemeinsamen europäischen Zusammenarbeit der Datenschutzbehörden. Diese Funktion hat in der aktuellen Vorbereitungsphase auf die kommende Datenschutzgrundverordnung erhebliche Bedeutung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat im Oktober 2015 beschlossen, dass künftig der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit die Bundesländer bei der gemeinsamen Arbeitsgruppe der europäischen Aufsichtsbehörden in Brüssel vertritt.

In dieser Arbeitsgruppe, die nach demjenigen Artikel der europäischen Datenschutzrichtlinie (DSRL) benannt ist, auf deren Grundlage sie arbeitet, treffen sich Vertreter der Da-

tenschutzbehörden aller EU-Mitgliedstaaten ca. alle zwei Monate zu zweitägigen Sitzungen in Brüssel. Ihre Aufgaben sind in Artikel 30 der DSRL beschrieben:

> „Die Gruppe hat die Aufgabe,
>
> **a)** alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen;
> **b)** zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen;
> **c)** die Kommission bei jeder Vorlage zur Änderung dieser Richtlinie, zu allen Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken;
> **d)** Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben."

Die wesentliche Funktion dieser europäischen Zusammenarbeit liegt also in der Vereinheitlichung des Datenschutzes innerhalb der EU, d.h. sowohl einer gemeinsamen Rechtsauslegung als auch einer vergleichbaren oder sogar gemeinsamen Vollzugspraxis. Die Art. 29-Gruppe hat dafür eine Reihe von permanenten und fallbezogenen fachlichen Untergruppen (Subgroups, Task Forces) eingerichtet, in die die europäischen Aufsichtsbehörden ebenfalls Vertreter auf Arbeitsebene entsenden. Das Ergebnis schlägt sich in Form von Arbeitspapieren (Working Documents), Leitlinien (Guidelines), Stellungnahmen (Opinions), Pressemitteilungen und anderen öffentlich zugänglichen Dokumenten nieder (siehe *http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083*).

Mitunter weniger deutlich nach außen hin sichtbar, aber in der Praxis von erheblicher Relevanz ist das gemeinsame Auftreten von mehreren Datenschutzbehörden aus der Art 29-Gruppe bei Datenschutzverstößen durch Unternehmen, die in mehreren europäischen Ländern tätig sind. Die Erfahrung zeigt, dass solche konzertierten Aktionen – trotz der teilweise recht unterschiedlichen Sanktionsmöglichkeiten und verfahrensrechtlichen Bestimmungen in den Mitgliedstaaten – wesentlich größeres Gewicht haben und bei den Unternehmen für mehr Bereitschaft an durchgreifenden Lösungen sorgen, als eine einzelne Aufsichtsbehörde dies könnte.

Aufgrund der föderalen Struktur Deutschlands nehmen bei der Art. 29-Gruppe Bundes- und Ländervertreter die Vertretung gemeinsam wahr. Viele der behandelten Themen fallen in die Zuständigkeit sowohl des Bundes als auch der Länder. Die Aufsicht über die Wirtschaft wiederum liegt (mit Ausnahmen) bei den Behörden der Länder. Wir stimmen uns daher in der Vor- und Nachbereitung der Treffen in Brüssel nicht nur mit den anderen Aufsichtsbehörden in den Bundesländern, sondern ebenso mit der Bundesdatenschutzbeauftragten eng ab. Dies erfolgt aufgrund der langjährigen engen Kooperation der Beteiligten meist problemlos und auch im Lauf der Sitzung, wenn neue Fragestellungen auftauchen oder Änderungen zur Abstimmung stehen. Ein gemeinsames Auftreten wird dabei nicht nur durch Absprachen zwischen Bundes- und Landesvertreter gefördert. In wichtigen Einzelfällen ist es auch gelungen, den gemeinsamen Vertretern in der Art. 29-Gruppe durch einen entsprechenden Beschluss der DSK ein imperatives Mandat zu geben. Es wäre wünschenswert, wenn diese Form der Mandatierung stärker genutzt würde. Allerdings ist es schwierig, die Arbeitsweisen und -rhythmen der nationalen und der europäischen Ebene gut aufeinander abzustimmen.

Mit Geltung der Datenschutzgrundverordnung (DSGVO) im Mai 2018 wird die Art. 29-Gruppe ihre Grundlage verlieren. An ihre Stelle tritt dann der Europäische Datenschutzausschuss (EDSA bzw. EDPB, European Data Protection Board). Dieser Ausschuss hat erheblich mehr Aufgaben und Kompetenzen als die bisherige Art. 29-Gruppe. Er verfügt als Organ der EU über eine eigene Rechtspersönlichkeit und kann verbindliche Beschlüsse fassen, die die Aufsichtsbehörden direkt binden. Dies ist erforderlich, da dann in allen Mitgliedstaaten die DSGVO unmittelbar gilt und einheitlich angewendet werden muss. Dadurch soll es Unternehmen künftig nicht mehr gelingen, durch Wahl ihres Sitzes eine möglicherweise milde Behandlung durch die dortige Aufsichtsbehörde zu erfahren.

Abgesehen von dieser zusätzlichen formalen Ebene ist zu erwarten, dass der EDSA in Hinblick auf die Ausrichtung der Art. 29-Gruppe ein hohes Datenschutzniveau sowohl innerhalb der EU als auch über deren Grenzen hinaus zu fördern, Kurs halten wird. Die Vertreterin bzw. der Vertreter der Länder im EDSA wird künftig nicht mehr durch die DSK, sondern durch den Bundesrat bestimmt. Dieser wählt die Leiterin oder den Leiter der Aufsichtsbehörde eines Landes für die Dauer von fünf Jahren. Eine Lösung mit Kontinuität für die schwierige Übergangsphase von der DSRL zur DSGVO bzw. von der Art 29-Gruppe zum EDSA wäre hier sicherlich ein sinnvoller Weg.

6. Maßnahmenplan für Datenverarbeitung in Vorbereitung auf die DSGVO

Die DSGVO wird ab dem 25. Mai 2018 Geltung haben. Für die verantwortlichen Stellen wird dies weitreichende Auswirkungen nach sich ziehen. Das betrifft zunächst einmal private Unternehmen, die ihre Unternehmensprozesse auf die DSGVO umstellen sollten. Aber auch für öffentliche Stellen ergeben sich Änderungsbedarfe, die sich künftig ebenfalls aus der DSGVO ableiten und – da die Regelungen in Zukunft nicht mehr zwischen öffentlichen und privaten Stellen differenzieren – im Wesentlichen auch für diese unmittelbar gelten.

Die Datenschutzkonferenz des Bundes und der Länder hat insoweit in diesem Zusammenhang ein sogenanntes Kurzpapier veröffentlicht, das einen Maßnahmenplan für Unternehmen vorstellt, der Schritte zur Implementierung eines Datenschutzkonzepts für die Erfüllung der Regelungen aus der DSGVO enthält. Da mit Inkrafttreten der neuen Regelung sowohl im Bereich privater Unternehmen, aber auch im Bereich öffentlicher Stellen der FHH Prüfungen geplant sind, sollte die Gelegenheit wahrgenommen werden, die Zeit bis zur Geltung der Regelung zu nutzen und noch einmal das Konzept für den Datenschutz kritisch zu überprüfen.

Das Kurzpapier rät dazu, im Unternehmen eigens ein Projekt zur Umsetzung der DSGVO zu starten. In dessen Rahmen sollte eine Bestandsaufnahme erfolgen über sämtliche Verfahren, die personenbezogene Daten verarbeiten. Hierbei gilt es, einen Soll-Ist-Abgleich mit Blick auf die neuen Regelungen vorzunehmen. Die wesentlichen Stichworte für einen solchen Abgleich lauten: Prozesse im Unternehmen, Rechtsgrundlagen, Betroffenenrechte, technisch-organisatorische Maßnahmen, Dienstleistungsbeziehungen, Dokumentationspflichten, Datenschutz-Folgenabschätzung, Meldepflichten,

Datensicherheit und Zertifizierung. Das Kurzpapier kann in unserem Internetangebot heruntergeladen werden: *https://www.datenschutz-hamburg.de/uploads/media/DSK_Kurzpapier_Nr_8_Massnahmenplan.pdf*.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit steht für Fragen und zur Beratung über die Anforderungen und Umsetzungsvorgaben gern zur Verfügung.

7. Presse- und Öffentlichkeitsarbeit

Die Pressearbeit beim HmbBfDI verzeichnet auch für die Jahre 2016 und 2017 eine hohe Anzahl an Anfragen. Neben besonders erhöhten Werten z.B. im Zusammenhang mit unserer Anordnung gegen Facebook, den Bußgeldern bezüglich Safe Harbor oder dem G20-Gipfel in Hamburg ist auch ein zunehmendes Interesse aus der universitären und schulischen Welt an Datenschutzthemen festzustellen.

Die schon in den Vorjahren recht hohe Anzahl an Anfragen seitens der Presse und Medien hat sich auch im Berichtszeitraum 2016/2017 weitgehend bestätigt. Das Thema Datenschutz mit seinen vielen gesellschaftspolitischen, rechtlichen sowie technischen Facetten hat eine deutlich gesteigerte mediale Relevanz erlangt, was – als ein Spiegel gesellschaftlicher Meinungsbildungsprozesse betrachtet – positiv zu werten ist. Datenschutz hat in der Presse- und Medienlandschaft das frühere Stigma einer Thematik für Spezialisten abgelegt und ist quasi in der Mitte der gesellschaftlichen Wahrnehmung angekommen. Dafür mag auch sprechen, dass uns zunehmend Anfragen im Zusammenhang mit universitären oder schulischen Projekten mit Datenschutz-Bezug erreicht haben.

Insbesondere das soziale Netzwerk Facebook, für das der HmbBfDI aufgrund seiner deutschen Niederlassung in Ham-

burg datenschutzrechtlich zuständig ist, stand häufig im Fokus der eingegangenen Presseanfragen. Gerade die Anordnung unserer Behörde hinsichtlich des Datenaustauschs zwischen Facebook und WhatsApp im September 2016 hat hier zu einem Peak der Anfragezahlen geführt. Auch ausländische Medien haben in diesem Zusammenhang verstärktes Interesse gezeigt. Ähnliches lässt sich hinsichtlich der von uns verhängten Bußgelder im Zusammenhang mit Safe Harbor sagen.

Des Weiteren bildete der G20-Gipfel in Hamburg im Juli 2017 einen Schwerpunkt der Presseanfragen. Datenschutzrechtliche Aspekte des polizeilichen Einsatzes wurden ein ums andere Mal abgefragt, insbesondere die Maßnahmen der Videoüberwachung und die sogenannte „schwarze Liste" akkreditierter Journalisten.

Neben diesen zentralen Schwerpunkten wurde aber auch das übrige Spektrum datenschutzrechtlicher Themen abgefragt: so die Entscheidungen des Europäischen Gerichtshofs, beispielsweise zu den Fluggastdaten, oder Fragen des Online-Handels, der Videoüberwachung im öffentlichen Bereich und des internationalen Datenverkehrs, um nur einige zu nennen. Auch in die Zukunft gerichtete Aspekte wie Autonomes Fahren, Künstliche Intelligenz oder Chip-Implantate erlangen zunehmend mediale Bedeutung.

Im Berichtszeitraum 2016/2017 haben uns insgesamt 549 Presseanfragen erreicht, das sind ca. 12% weniger als in den Jahren 2014 und 2015 (626). Im Durchschnitt wurden rund 23 Anfragen pro Monat von uns bearbeitet.

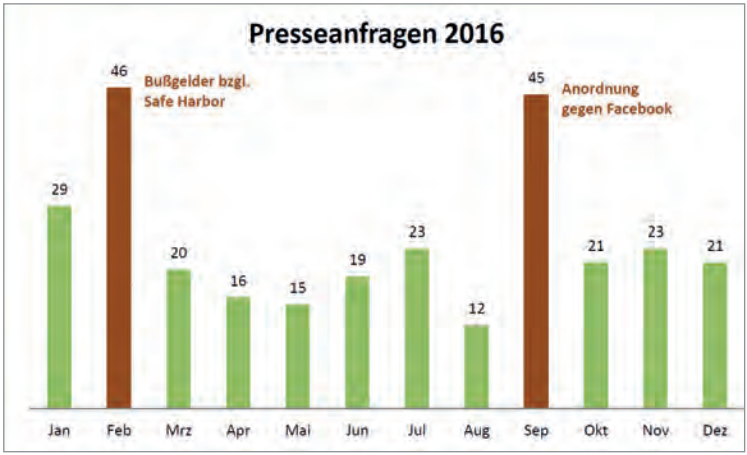


Abb. 1: Presseanfragen 2016 pro Monat mit Kennzeichnung „besonderer Ereignisse“

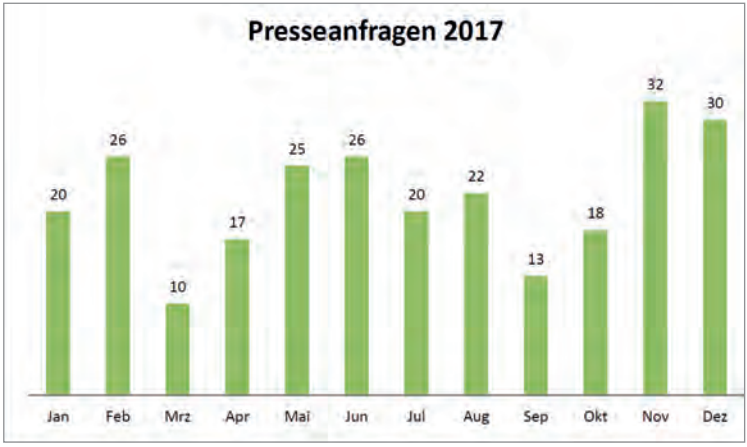


Abb. 2: Presseanfragen 2017 pro Monat

Während im Jahr 2017 die monatliche Verteilung der Presseanfragen relativ gleichverteilt ausfiel, zeigten sich in 2016 die beiden auffälligen Peaks im Februar und September im Zusammenhang mit Safe Harbor und Facebook. Was die Internet-Konzerne Facebook und Google anbelangt, so machten die Anfragen hierzu ca. 27% aller Presseanfragen aus.

Damit setzte sich hier der Anfragerückgang seit 2014/2015 (noch 39% der Gesamtzahl) weiter fort. Insbesondere hinsichtlich Google hat sich die Zahl der Anfragen auffallend reduziert: Waren es 2014/2015 noch 149, so schlugen 2016/2017 hier nur mehr 24 Anfragen zu Buche.

Was die Herkunft der anfragenden Medien anbelangt, so bilden überregionale Medien wie schon im vorangegangenen Berichtszeitraum den Schwerpunkt. Seitens der ausländischen Medien sind die Anfragen im Jahr 2017 auffällig zurückgegangen, wie die nachstehende Tabelle verdeutlicht:

Presseanfragen...	2016 (2014)	2017 (2015)	Gesamt (2014/2015)
regionaler Medien:	55 (111)	72 (73)	127 (184)
überregionaler Medien:	179 (169)	174 (164)	353 (333)
ausländischer Medien:	56 (50)	13 (59)	69 (109)
Gesamt:	290 (330)	259 (296)	549 (626)

Tabelle 1: Presseanfragen beim HmbBfDI 2016/2017, Klammerzusätze: Presseanfragen 2014/ 2015 zum Vergleich

Neben den Tätigkeitsberichten des vergangenen Berichtszeitraums gab es in den Jahren 2016 und 2017 keine weiteren Veröffentlichungen im Printbereich. In unserem Internet-Angebot haben wir indes zahlreiche Informationen, Kurzpapiere und Handreichungen mit Blick auf die ab Mai 2018 geltende EU-Datenschutzgrundverordnung eingestellt. Daneben haben wir im Berichtszeitraum 19 Pressemitteilungen veröffentlicht.

Zudem haben der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit sowie einige Mitarbeiterinnen und Mitarbeiter unseres Hauses erneut Vorträge und Präsentationen zu verschiedenen Themen des Datenschutzes durchgeführt und sich an Gesprächsrunden oder Podiumsdiskussionen beteiligt.

INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT VI.

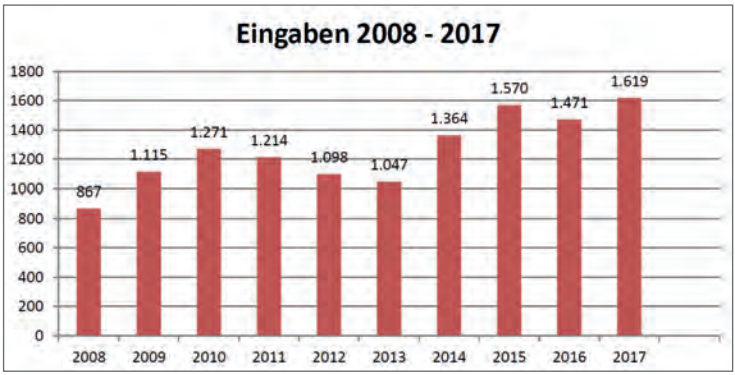
1. Statistische Informationen

1.1 Beratungen der Bürgerinnen und Bürger (Eingaben-Statistik)

Datenschutzrechtlich Beschwerden steigen weiter an

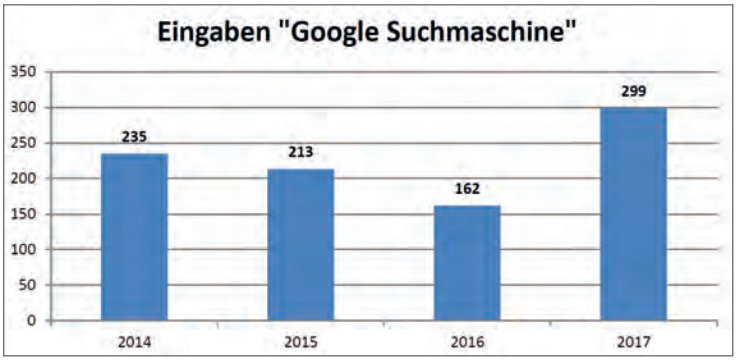
Bürgerinnen und Bürger, die der Ansicht sind, bei der Verarbeitung ihrer personenbezogenen Daten in ihren Rechten verletzt worden zu sein, können sich zur Durchsetzung ihrer Rechte oder zur Klärung der Rechtslage an den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit wenden. Diese sogenannten Eingaben haben auch in den Jahren 2016 und 2017 wieder einen erheblichen Teil des Tagesgeschäfts der Mitarbeiterinnen und Mitarbeiter ausgemacht.

1.471 Eingaben im Jahr 2016 belegen im 10-Jahres-Vergleich der datenschutzrechtlichen Eingaben beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit den dritten Platz nach 2015 (1.570)*. Dieser bisherige Spitzenwert wurde im Jahr 2017 deutlich überholt, denn mit 1.619 Eingaben im Jahr 2017 haben sich mehr Bürgerinnen und Bürgern mit ihren Beschwerden an uns gewandt, als jemals zuvor*:



** bereinigt um die Eingaben bzw. Beschwerden zu Google Street View, da es sich hier um ein einmaliges Phänomen handelte und die 400 Eingaben damals auf zumeist problemlos abzuhelfenden Beschwerden über die fehlende Verpixelung nach dem Antrag Betroffener zurückgingen.*

Damit bewahrheitet sich unsere Prognose aus dem letzten Tätigkeitsbericht, dass sich durch unsere Zuständigkeit für Facebook und Google die Entwicklung der Eingabenzahlen verstärken wird (vgl. 25. TB, 1), denn einen großen Anteil dieser datenschutzrechtlichen Eingaben machen die Anträge auf Löschung aus den Ergebnissen der Google Suchmaschine auf Grundlage des Urteils des Europäischen Gerichtshofs vom 13. Mai 2014 (C-1341/12) aus (vgl. 25. TB, V 1.1). Nachdem es nach 2014 den Anschein hatte, dass sich diese Eingaben nach dem anfänglichen Boom auf einem etwas niedrigeren Niveau stabilisieren würden, sind die Zahlen im Jahr 2017 wieder deutlich angestiegen:



Es ist damit zu rechnen, dass diese Eingaben nach dem derzeitigen Stand auch mit Geltung der DSGVO weiterhin durch die nationalen Behörden abzuarbeiten sein werden. Neben der Verfolgung von Verstößen, die sich häufig aus den Eingaben von Bürgerinnen und Bürgern ergeben, gehört es aber auch zu unseren Aufgaben, Bürgerinnen und Bürger sowie verantwortliche Stellen in datenschutzrechtlichen Fragen zu beraten. Viele dieser Beratungen erfolgen unmittelbar aus den Eingaben, oft werden wir aber auch außerhalb dieses Instruments von Bürgerinnen und Bürgern um Rat gebeten, von verantwortlichen Stellen sowieso.

So haben wir im Jahr 2016 insgesamt 3.388 statistisch erfasste Beratungen durchgeführt, davon haben wir 2.027-mal Bürgerinnen und Bürger sowie 1.163-mal datenschutzrechtlich verantwortliche Stellen beraten. Mit einer Gesamtzahl von 2.502 wurde der Wert aus 2016 im Jahr 2017 nicht wieder erreicht, wobei sowohl die Zahl der Beratungen von Bürgerinnen und Bürger (1.625) als auch die Zahl der Beratungen von verantwortlichen Stellen (874) deutlich unter den Vorjahreszahlen liegt. Neu hinzugekommen ist das direkte Fragerecht von Abgeordneten der Hamburgischen Bürgerschaft, das sich nach der Änderung der Hamburgischen Verfassung unmittelbar aus dem neuen Art. 60a ergibt (vgl. I). 2017 haben uns drei solche Fragen erreicht, die wir statistisch als Beratungen von Abgeordneten erfassen.

1.2 Stellungnahmen in Gesetzgebungsverfahren

Datenschutz hat hohen Stellenwert im Rechtssetzungsverfahren

Soweit datenschutzrechtliche Belange berührt werden, ist der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit an Gesetzgebungsverfahren zu beteiligen. Die Beteiligung erfolgt in der Regel durch Stellungnahmen unserer Behörde, die durch die federführende Behörde abgerufen wird.

Im Berichtszeitraum haben wir 59 (2016) bzw. 32 (2017) solcher Stellungnahmen abgeben. Leider gibt es keine Statistik darüber, wie oft unsere datenschutzrechtlichen Einwände, wenn wir welche hatten, dann auch Berücksichtigung fanden.

1.3 Statistik Bußgelder und Anordnungen

Datenschutzverstöße werden wenn nötig sanktioniert.

In der Mehrheit der Fälle kann Datenschutzverstößen durch kooperativen Dialog mit der verantwortlichen Stelle abgeholfen werden. Wo dies nicht möglich ist oder die Schwere des Verstoßes gleichwohl eine Sanktion geboten erscheinen lässt, werden Bußgelder verhängt oder Anordnungen erlassen.

In den Jahren 2016 und 2017 wurden 22 Bußgeldbescheide erlassen. Im Vergleich zum vorherigen Berichtszeitraum bedeutet dies einen Anstieg um 36 %. Drei Verfahren gehen auf eine Prüfaktion zurück, bei der mehr als 30 international agierende Hamburger Unternehmen im Hinblick auf die Umsetzung des Urteils des Europäischen Gerichtshofs zur Ungültigkeit des Safe-Harbor-Mechanismus' angeschrieben wurden (siehe oben IV 4.).

In Zukunft ist mit deutlich höheren Bußgeldbeträgen zu rechnen. Art. 83 Abs. 1 DSGVO verlangt Sanktionen, die „wirksam, verhältnismäßig und abschreckend" sind. Art. 83 Abs. 5 DSGVO erhöht die Obergrenze des Bußgeldrahmens um das 67-fache auf bis zu 20.000.000 Euro pro Verstoß beziehungsweise auf bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens. Diese Maßgaben werden auch bei den niedrigen und mittleren Bußgeldern eine deutliche Erhöhung zur Folge haben.

Bußgeldverfahren

Tatbestand § 43 Abs.1 Nr.		Sachverhalt	Bußgeld in €	Einspruch (E) bzw. kein Einspruch (N)	ggfs. Verfahren vor dem Amtsgericht
	1	Veröffentlichung eines Werbefilms ohne Einwilligung der Protagonisten	5.000,00	N	
	1	Datenübermittlung in die USA auf Grundlage der ungültigen Safe-Harbor-Entscheidung	9.000,00	N	
	1	Datenübermittlung in die USA auf Grundlage der ungültigen Safe-Harbor-Entscheidung	11.000,00	N	
	1	Datenübermittlung in die USA auf Grundlage der ungültigen Safe-Harbor-Entscheidung	8.000,00	N	
	1	Offenbarung von Kundendaten durch mangelhafte Entsorgung von Akten in öffentlich zugänglichen Altpapiercontainern	1.050,00	N	
10		Nichterteilung einer Auskunft	2.000.00	N	
	1	Videoüberwachung von Gästen und Arbeitnehmern in einem Gastronomiebetrieb	5.000,00	E	Reduzierung auf 1.000 €
	7	nicht erfolgte Mitteilung	500,00	N	
	1	unzulässige Übermittlung von Scorewerten durch Auskunftei	15.000,00	E	Bestätigung der Anordnung
	1	unzulässige Übermittlung von Kundendaten	1.000,00	N	
	1	unzulässige Übermittlung von Kundendaten	2.000,00	N	
10	1	Werbung an 45 Empfänger im offenen E-Mail-Verteiler	2.500,00		Einspruch eingelegt, später zurückgezogen
	1	Drittstaatenübermittlung von Kundendaten ohne Rechtsgrundlage	2.000,00	N	
	1	unzulässige Übermittlung	12.000,00	N	
8a		verspätete Auskunft	1.500,00	N	
8a		verspätete und unvollständige Auskunft	2.000,00	N	
8a		verspätete Auskunft	1.500,00	N	
8a		verspätete Auskunft	1.500,00	N	
	1	Nutzung von Adressdaten - Freunde Finden 2nd degree invite	19.800,00	N	
	1	unzulässige Übermittlung von Scorewerten durch eine Auskunftei in fünf Fällen	20.000,00	N	
5b		Zusendung von Werbung per E-Mail trotz Widerspruchs	1.000,00	N	
8a		verspätete Auskunft	1.500,00	N	

Anordnungen gemäß § 38 Abs. 5 S. 1 BDSG zielen darauf ab, einen gegenwärtigen Datenschutzverstoß zu beenden oder die Wiederholung eines Verstoßes zu untersagen. Bislang können solche förmlichen Verpflichtungen nur gegen nichtöffentliche Stellen ausgesprochen werden. Unter der DSGVO werden auch Anordnungen gegen öffentliche Stellen ausgesprochen werden.

Anordnungen

Sachverhalt	Status
Videoüberwachung in einer Betriebsstätte eines Kfz-Dienstleisters	laufendes Gerichtsverfahren
Videoüberwachung eines Gastronomiebetriebs	rechtskräftig
Blockierung eines Google-Suchergebnisses	rechtskräftig
Untersagung der Erhebung von WhatsApp-Daten durch Facebook	laufendes Gerichtsverfahren
Blockierung von Google-Suchergebnissen	rechtskräftig

Es wurden keine Strafanträge gestellt.

Im Berichtszeitraum sind folgende gerichtliche Entscheidungen für bzw. gegen uns ergangen:

Gerichtliche Entscheidungen

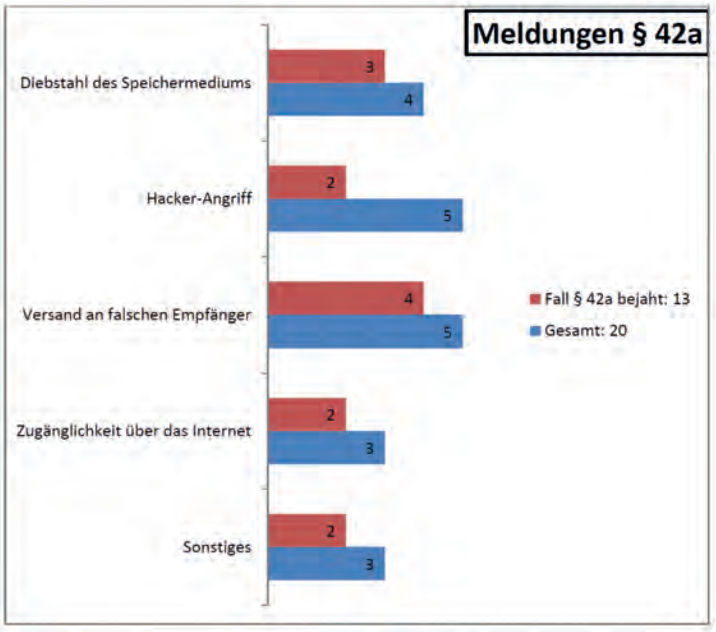
Gericht	Klagegrund	Entscheidung	ggfs. Rechtsmittel
AG Hamburg	Klage gegen unseren Bußgeldbescheid wegen unzulässiger Datenübermittlung einer Auskunftei	Klage abgewiesen	Rechtsbeschwerde eingelegt und zurückgenommen; Urteil rechtskräftig
AG Hamburg	Klage gegen unseren Bußgeldbescheid wegen Videoüberwachung in Gastronomie	Ordnungswidrigkeit bestätigt,	Bußgeldhöhe reduziert, Urteil rechtskräftig
VG Hamburg	Klage gegen unsere Anordnung auf Unterlassung der Zusammenführung von Daten verschiedener Google-Dienste	Verfahren für erledigt erklärt; unsere Anordnung dadurch rechtskräftig	Beschluss rechtskräftig

VG Hamburg	Antrag im einstweiligen Rechtsschutz gegen unsere Anordnung, die pseudonyme Nutzung von Facebook zuzulassen	Antrag stattgegeben	Beschluss rechtskräftig; bestätigt durch OVG Hamburg
VG Hamburg	Antrag im einstweiligen Rechtsschutz gegen unsere Anordnung, die Datenerhebung von Facebook bei WhatsApp zu unterlassen	Antrag abgelehnt	Beschluss nicht rechtskräftig; Beschwerde beim OVG Hamburg eingelegt
VG Hamburg	Klage auf Verpflichtung, eine aufsichtsbehördliche Anordnung gegen Google zu erlassen (Entfernung/Löschung von Suchergebnissen)	Klage abgewiesen	Urteil noch nicht rechtskräftig
VG Hamburg	Klage auf Verpflichtung, eine aufsichtsbehördliche Anordnung gegen Google zu erlassen (Entfernung/Löschung von Suchergebnissen)	Klage abgewiesen	Urteil noch nicht rechtskräftig; Berufung beim OVG Hamburg eingelegt
VG Hamburg	Klage auf Verpflichtung, eine aufsichtsbehördliche Anordnung gegen Google zu erlassen (Entfernung/Löschung von Suchergebnissen)	Klage abgewiesen	Urteil noch nicht rechtskräftig; Berufung beim OVG Hamburg eingelegt

1.4 Meldepflicht nach § 42a BDSG

Die Zahl der angezeigten Datenpannen ist auf gleichbleibendem Niveau.

Im Berichtszeitraum erreichten uns wieder zahlreiche Meldungen über Datenschutzvorfälle, bei denen Daten besonders sensibler Kategorien unberechtigt Dritten zur Kenntnis gelangt sind. Künftig ist mit einem erheblichen Anstieg der Vorfälle zu rechnen, da Art. 33 DSGVO die Meldepflicht nicht mehr auf die Verletzung des Schutzes von Daten aus bestimmten Kategorien beschränkt, sondern jegliche personenbezogene Daten betrifft.



1.5 Register

Es sind nur wenige Registermeldungen hinzugekommen.

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die nach § 4d einer Meldepflicht unterliegen. Diese Pflicht betrifft automatisierte Verarbeitungen, in denen geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung, zum Zweck der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung gespeichert werden.

	Anzahl 2016/2017	Veränderung seit 2014/2015
Speicherung zum Zwecke der Übermittlung		
Adresshändler	16	+1
Informationsdienste	5	+/- 0
Auskunfteien/Warndienste	11	+1
Speicherung zum Zwecke der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung	28	+1
Gesamtzahl aller Registereinträge	60	+3

2. Aufgabenverteilung (Stand: 1.1.2018)

Der Hamburgische Beauftragte
für Datenschutz und Informationsfreiheit
Klosterwall 6
20095 Hamburg

Tel.: 040/42854-4040
Fax: 040/42841-4000
E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.datenschutz-hamburg.de

Telefonliste		**040/42854-Durchwahl**
Dienststellenleiter:	Prof. Dr. Johannes Caspar	-4040
Stellvertreter:	Ulrich Kühn	-4054
Vorzimmer:	Heidi Niemann	-4040

Telefonliste	040/42854-Durchwahl
Presse- und Öffentlichkeitsarbeit, IT-Leitung, Internetangebot des HmbBfDI	
Martin Schemm	-4044
Beauftragter für den Haushalt, Verwaltungs- und Personalleiter	
Arne Gerhards	-4153
Haushaltsplanung und -bewirtschaftung, Berichtswesen	
Robert Flechsig	-4060
Gebühren und Bußgelder, Beschaffung, Aus- und Fortbildung	
Rolf Nentwig	-4043
Vorzimmer, Geschäftsstelle	
Heidi Niemann	-4040
Registratur, Geschäftsstelle	
Katharina Schmidt	-4042
Übergreifende Infrastrukturprojekte, Hamburg-Gateway, technisch-organisatorische Beratung und Prüfung	
Dr. Sebastian Wirth	-4053
Technisch-organisatorische Beratung und Prüfung	
Jutta Nadler	-4055
Technisch-organisatorische Beratung und Prüfung	
Eike Mücke	-4126

Telefonliste	040/42854-Durchwahl
Netzwerke und mobile Geräte, technisch-organisatorische Beratung und Prüfung Roland Schilling	-4048
Informationsfreiheit/Transparenz, Videoüberwachung, Auskunftsanspruch nach Presserecht Dr. Christoph Schnabel	-4047
Informationsfreiheit/Transparenz und Videoüberwachung Cornelia Goecke	-4141
Informationsfreiheit/Transparenz, Videoüberwachung, gewerbliche Dienstleistungen Barbara Görnandt	-4050
Grundsatzfragen des HmbDSG, Gesundheitswesen und medizinische Forschung, Schule und Bildungswesen, Sozialwesen Matthias Jaster	-4062
Verkehr, Wirtschaftsverwaltung, Bezirks- und Parlamentsangelegenheiten, Wahlen und Volksabstimmungen, Hochschul- und Bibliothekswesen, behördliche Datenschutzbeauftragte, Landwirtschaft Eva-Verena Scheffler	-4064
Sicherheit und Justiz, Waffenrecht, private Sicherheitsdienste und Detekteien, Rechtsanwälte und Notare, Ausländerwesen Okşan Karakuş	-4049

Telefonliste	040/42854-Durchwahl
Statistik, Pass- und Ausweisangelegenheiten, Personenstands- und Archivwesen, Kultur Uta Kranold	-4046
Grundsatzfragen des BDSG, Grundsatzfragen Internationales, Auskunfteien Helga Naujok	-4058
Beschäftigtendatenschutz, Geodaten, Kreditwirtschaft, Versand- und Onlinehandel, Gewerkschaften Dr. Jens Ambrock	-4059
Finanz-, Steuer- und Rechnungswesen, Handel und Industrie, Steuerberater und Wirtschaftsprüfer, Vereine und Parteien Heike Wolters	-4052
Werbung- und Adresshandel, Markt- und Meinungsforschung, Bauen und Wohnen, Versicherungen, Wasserversorgung und Energiewirtschaft Richard Heyer	-4045
Technische Grundsatzfragen bei Medien, Telemedien, Telekommunikation und E-Government, Netzwerke, Biometrie, technisch-organisatorische Beratung und Prüfung bei Informationsfreiheit und Kultur Ulrich Kühn	-4054
Juristische Grundsatzfragen bei Medien, Telemedien, Telekommunikation und E-Government, elektronischer Rechtsverkehr, Kultur Dr. Moritz Karg	-4051

Telefonliste	**040/42854-Durchwahl**
Beratung und Prüfung bei Medien, Telemedien, Telekommunikation, E-Government, technisch-organisatorische Beratung und Prüfung bei Videoüberwachung	
Herr Schneider	-4061
Juristische Grundsatz- und Sachbearbeitung bei Suchmaschinenlöschung, Medien und Telemedien	
Herr Schröder	-4144
Juristische Grundsatz- und Sachbearbeitung bei Suchmaschinenlöschung	
Frau Jacobson, Frau Weber	-4142

Titelbild, Foto: Martin Schemm
Layout: Inga Below, Kameko Design
Druck: print74

Herausgeber:
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6
20095 Hamburg
Tel.: 040/42854-4040 (Geschäftsstelle)
Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de

Der Hamburgische Beauftragte
für Datenschutz und Informationsfreiheit

Hamburg