TÄTIGKEITSBERICHT

DATENSCHUTZ

2019

Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Hamburg

28. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2019

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

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

Auflage: 800 Exemplare
Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH
Foto Titelseite: www.mediaserver.hamburg.de / Geheimtipp Hamburg
Druck: Beisner Druck GmbH & Co. KG

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

---

vorgelegt im Februar 2020
Prof. Dr. Johannes Caspar
(Redaktionsschluss: 31. Dezember 2019)

INHALTSVERZEICHNIS

Vorwort

Nach mehr als anderthalb Jahren seit Geltung der Datenschutzgrundverordnung (DSGVO) ist es an der Zeit, ein Zwischenfazit der gesetzlichen Regelung zu ziehen. Es gilt zu bewerten, inwiefern sich die vom europäischen Gesetzgeber mit der DSGVO ursprünglich verfolgten Absichten erfüllt haben. Wie hat sich der Datenschutz in Europa, aber auch ganz konkret am Datenschutz-Standort Hamburg seither entwickelt? Ist ein positiver Bewusstseinswandel bei Unternehmen und Behörden, aber auch bei den Bürgerinnen und Bürgern zu konstatieren? Wird das Recht auf informationelle Selbstbestimmung von Seiten der Betroffenen wahrgenommen? Hat sich die Anwendung der DSGVO durch die Aufsichtsbehörden bewährt?

Der vorliegende Tätigkeitsbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) über das Berichtsjahr 2019 beschäftigt sich insbesondere in seiner Einleitung (siehe I) mit der Beantwortung dieser Fragestellungen. Mit Blick auf die gestiegenen Beschwerdezahlen zeigt sich in der Tat eine Verbesserung des Datenschutzbewusstseins der Bürgerinnen und Bürger. Zugleich zeigt die hohe Zahl gemeldeter Datenschutzverletzungen in Hamburg, dass auch den Unternehmen die neuen gesetzlichen Pflichten bewusster geworden sind. Beides führt allerdings auch zu deutlich gestiegenen Arbeitsmengen, die den HmbBfDI vor große Herausforderungen stellen. Aufgrund leider zu geringer personeller Aufstockungen ließ sich die Arbeitslast auch durch Umstrukturierungsmaßnahmen der Behörde nur teilweise auffangen. Daher besteht hinsichtlich der Ressourcen weiterhin ein deutlicher Verbesserungsbedarf.

Eine kritische, ergebnisoffene Evaluation der DSGVO ist eine der zentralen Aufgaben der nahen Zukunft. Gerade auch der Blick auf die großen Internetkonzerne und deren grenzüberschreitende Datenverarbeitung zeigt Schwachstellen in der Anwendung und Umsetzung der Regelung durch die europäischen Datenschutzaufsichtsbehörden. Deren Kommunikation und Entscheidungsprozesse sind oftmals zu langwierig und zu komplex. Während die nationale Durchsetzung der Datenschutzgrundverordnung durch die Aufsichtsbehörden

langsam an Fahrt aufnimmt und die Maßnahmen zur Umsetzung zu greifen beginnen, bleiben im Bereich der grenzüberschreitenden Verarbeitung auf europäischer Ebene viele, gerade grundsätzliche Fälle unter Beteiligung großer globaler Anbieter weithin ungelöst.

Die Diskrepanz zwischen nationalen Verfahren und solchen, die auf europäischer Ebene im komplexen Zusammenspiel zwischen federführender und betroffener Behörde sowie ggfs. dem Europäischen Datenschutzausschuss zu lösen sind, wächst zusehends. Dabei ist – wie auch unter dem früheren Datenschutzrecht – nach wie vor für die Umsetzung der Datenschutzregelungen die Zuordnung zu einer federführenden Behörde von erheblicher Bedeutung. Datenschutz bleibt also auch weiterhin eine Frage der Standortwahl. Diese Entwicklung gibt durchaus Anlass zur Sorge.

Eine Fragmentierung des Datenschutzes in effiziente und zeitlich beschleunigte nationale Verfahren und langwierige europäische Verfahren andererseits sowie eine Zuordnung der verantwortlichen Stellen zu federführenden Behörden mit unterschiedlichen Ausrichtungen und divergierenden nationalen Vollzugsregelungen erschwert und behindert einen harmonisierten und nachhaltigen Schutz von Rechten und Freiheiten Betroffener europaweit. Das System des aufsichtsbehördlichen Vollzugs führt gegenwärtig zu einer Verfestigung der Marktmacht globaler Anbieter, die im Wesentlichen auf ihrer Datenmacht beruht. Immer stärker stellen uns insoweit inländische Unternehmen die Frage nach einem fairen Wettbewerb auf dem gemeinsamen digitalen Markt vor dem Hintergrund des Vollzugs der EU-Datenschutzgrundverordnung.

Eine eigenständige europäische Digitalstrategie muss dem künftig Rechnung tragen. Die Privilegierung von großen marktbeherrschenden Unternehmen war sicher nicht das Ziel der EU-Datenschutzgrundverordnung. Wenn dies mittlerweile so wahrgenommen wird, sollte dies Grund zum Umsteuern sein.

Prof. Dr. Johannes Caspar
Februar 2020

EINLEITUNG I.

EINLEITUNG

1. Die Situation der Behörde im zweiten Jahr der DSGVO – Datenschutz als Individualrechtsgarantie mit großer Nachfrage, aber langer aufsichtsbehördlicher Lieferzeit

Die Datenschutzgrundverordnung hat den Datenschutz nicht nur im europäischen, sondern auch im nationalen und internationalen Maßstab tiefgreifend verändert. Die gestiegene Bedeutung des Schutzes der Privatsphäre durch die Schaffung europaweit verbindlicher Vorschriften zum Schutz Betroffener, wie auch die Verankerung weitgehenderer Verpflichtungen für Datenverarbeiter haben die Anforderungen an die Behörden beim Vollzug der Datenschutzregelungen erheblich erhöht.

Aufgrund der neuen wesentlich schärfern Vollzugs- und Sanktionsinstrumente der Aufsichtsbehörden sind im Bereich des Datenschutzes gerichtliche Verfahren mittlerweile an der Tagesordnung. Dies gilt sowohl für Klagen Betroffener auf ein behördliches Einschreiten des Beauftragten für Datenschutz und Informationsfreiheit als auch für Rechtsbeschwerden von Verantwortlichen, die sich gegen die Verhängung von Bußgeldern oder den Erlass von Anordnungen durch die Aufsichtsbehörde wenden. Drohende Millionenbußen verändern zusehends das Anforderungsprofil an den Datenschutz und führen zu einer stärkeren juristischen Professionalisierung aller sich mit dieser Thematik beschäftigenden Akteure auf Seiten der Aufsichtsbehörden und tatsächlich auch auf Seiten der verantwortlichen Stellen.

Der Einsatz von Vollzugsinstrumenten nach Maßgabe der DSGVO erforderte die Schaffung einer behördeninternen Stelle, die auf eine gerichtliche Vertretung und eine den Rechtsförmlichkeiten entsprechende Abfassung insbesondere von Bußgeldbescheiden wie auch von behördlichen Anordnungen spezialisiert ist. Seit Anfang 2019 nimmt daher im Zuständigkeitsbereich des HmbBfDI ein Justitiariat den Erlass von Maßnahmen sowie die gerichtliche Vertretung der Behörde wahr. Dieses fungiert gleichzeitig als Vorprüfungsstelle, um Beschwerden, bei denen Entscheidungen in einem beschleunigten Verfahren ergehen können, zügig zu

bescheiden. Insgesamt bindet die Zunahme von Klagen erhebliche Ressourcen der Behörde, sie ist aber auch ein positives Zeichen für eine stetige Verrechtlichung des Datenschutzes und für ein zunehmendes Rechtsbewusstsein von Bürgerinnen und Bürgern.

Die gerichtliche Auseinandersetzung über Interpretation und Anwendung der Vorschriften der DSGVO wird langfristig zu mehr Rechtssicherheit führen. Ein großer Teil der Kritik an der DSGVO ist auf die Unbestimmtheit ihrer Begriffe und die Unklarheit der aus ihr resultierenden Rechtsfolgen zurückzuführen. Neuen Regelungen ist jedoch grundsätzlich immanent, dass sie erst durch die juristische Praxis, insbesondere durch die Auslegung der Gerichte, geformt werden. Bevor nach dem konkretisierenden Gesetzgeber gerufen wird, sollte die Rechtspraxis Gelegenheit bekommen, über offene Auslegungsfragen der DSGVO zu entscheiden. Dabei sind Rechtsschutzverfahren, seien sie von Betroffenen oder von Verantwortlichen gegen die Entscheidungen von Aufsichtsbehörden eingelegt, durchaus Wege zu mehr Rationalität und Klarheit auf diesem durch die DSGVO grundlegend neu gestalteten Rechtsgebiet. Der Vermeidungseffekt, der über Jahrzehnte die Rechtspraxis unter dem alten Bundesdatenschutzgesetz bestimmte und dazu führte, dass durch fehlende Aktivitäten von Behörden, aber auch wegen fehlender Klagerechte Betroffener, richterliche Rechtsfortbildung kaum erfolgte, hat eher zur einer Erstarrung des Datenschutzrechts geführt. In einigen Jahren werden viele der Auslegungsfragen geklärt sein, die derzeit in der gesamten Breite der DSGVO teilweise sogar unter Aufsichtsbehörden umstritten sind.

Die Zunahme von Beschwerden im Jahr der Einführung der DSGVO 2018 war immens. Demgegenüber hat sich die Eingangszahl im Berichtsjahr 2019 noch einmal um weitere fast 25 % Prozent erhöht (siehe dazu Kapitel VI.1). Es wird damit klar, dass es sich nicht um einen einmaligen Effekt handelt, sondern um eine sich verstetigende Entwicklung. Die Menschen machen in immer stärkerem Maße von ihren Rechten auf dem Gebiet des Datenschutzes Gebrauch. Gleichzeitig bestätigt sich, dass Stellenwert und Bedeutung des Daten-

schutzes in der fortschreitenden Entwicklung der Digitalisierung rasant zunimmt. Dass die Menschen die Rechte der DSGVO nutzen, ist zunächst eine sehr gute Nachricht. Andererseits befindet sich die Behörde durch die große Nachfrage jedoch längst jenseits der Kapazitätsgrenze. Trotz einer zwischenzeitlich erfolgten Verstärkung des Personals führen sowohl die qualitativen als auch quantitativen Aufgabenzuwächse dazu, dass die Zahl der schriftlichen Eingänge die Zahl der erledigten Ausgänge im Berichtszeitraum um ca. 15 Prozent überstiegen (VI 1). Vor dem Hintergrund der aus 2018 noch offenen Verfahren ist dies eine alarmierende Nachricht. Sollte diese Tendenz trotz bereits ergriffener und zum Teil noch umzusetzender Umstrukturierungsmaßnahmen der Behörde und einer personellen Aufstockung nicht umkehrbar sein, stellt sich die Frage nach der mittelfristigen Handlungsfähigkeit der Behörde.

Bereits heute ist klar: Immer komplexere Verfahren sowie eine steigende Anzahl von Beschwerden machen anlässlich des Doppelhaushalts 2021/22 die Forderung nach einer weiteren personellen Aufstockung alternativlos. Allein die Arbeitszeit, die aufgewendet werden muss, um die bestehenden Eingänge abzuarbeiten, verhindert eine zeitnahe Bearbeitung neuer Eingänge. Für Bürgerinnen und Bürger bedeutet dies in der Praxis leider häufig lange Wartezeiten nach Beschwerden und Anfragen bei der Behörde. Nach den Regeln der DSGVO muss jede betroffene Person innerhalb von drei Monaten über den Stand oder das Ergebnis einer eingereichten Beschwerde in Kenntnis gesetzt werden. Die damit verbundenen berechtigten Erwartungen auf eine zügige Bearbeitung werden aufgrund der derzeitigen Situation der Behörde leider allzu häufig enttäuscht.

Es ist insoweit erfreulich, dass die Hamburgische Bürgerschaft den Antrag von Abgeordneten der Fraktionen der SPD und der Grünen gerichtet auf die künftige Sicherstellung einer angemessenen personellen Ausstattung des oder der Hamburgischen Beauftragten für Datenschutz (Drucksache 21/17929 sowie Plenarprotokoll vom 14. August 2019, S. 7957ff) mit großer Zustimmung der Fraktionen angenommen hat. Dabei geht es darum, dass der Senat gemeinsam

mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ersucht wird, im Rahmen der Haushaltsberatungen 2021/22 über die Auswirkungen einer zunächst befristeten Maßnahme zur Stellenverstärkung mit zwei Vollzeitäquivalenten zu berichten. In der Folge wird daher zeitnah zu prüfen sein, ob eine angemessene Ausstattung im Rahmen der DSGVO erreicht wurde.

Die Entwicklung wird insgesamt in den nächsten Monaten weiter beobachtet werden, damit im Rahmen der Verhandlungen zum nächsten Haushalt entsprechende Bedarfe angemeldet werden können und die Lieferzeiten des Datenschutzes für Bürgerinnen und Bürger künftig verbessert werden.

2. Datenschutz fragmentiert – Dysfunktionalitäten im Vollzug: Umsteuern erforderlich!

Die Datenschutzgrundverordnung hat wesentliche Verbesserungen für den Schutz von Rechten und Freiheiten Betroffener gebracht. Gleichzeitig wurden zeitgemäße Pflichten für die verantwortlichen Stellen verankert. Das Ganze wurde mit wirksamen Sanktionsinstrumenten verklammert, die dem Datenschutz ein erheblich höheres Gewicht verschaffen. Vor allem die Möglichkeit, Bußgelder in einer Höhe des 67-fachen des bisher geltenden Rahmens (20 Millionen Euro statt bislang 300.000 Euro) bzw. bis zu einer Höhe von 4 % des jährlichen weltweiten Umsatzes eines Unternehmens zu verhängen, haben bei den verantwortlichen Stellen zu einer erheblich stärkeren Beachtung der Datenschutzanforderungen geführt.

Leider droht diese positive Wirkung immer stärker in Frage gestellt zu werden, denn der aufsichtsbehördliche Vollzug funktioniert bei der grenzüberschreitenden Datenverarbeitung nicht annähernd zufriedenstellend. So sind selbst am Ende des zweiten Jahres nach Wirksamwerden der DSGVO bislang keine rechtlichen Sanktionen gegenüber großen globalen Diensteanbietern bei der grenzüberschreitenden Datenverarbeitung verhängt worden. Das ist besonders deshalb problematisch, als es im Verlauf des Zeitraums viele Be-

richte über Datenschutzverstöße und -pannen dieser Unternehmen und unzählige Beschwerden von Bürgerinnen und Bürger wie auch von Datenschutz-Organisationen dagegen gegeben hat. So richteten sich die ersten Beschwerden nach DSGVO überhaupt gegen solche Anbieter im Bereich sozialer Netzwerke, mobiler Betriebssysteme und von Chatting-Diensten.

Das Selbstverständnis und das Geschäftsmodell einiger Internetkonzerne ist bis heute trotz der Datenschutzgrundverordnung mit Blick auf die Gewährleistung der Rechte Betroffener problematisch. Das offenkundige Auseinanderfallen zwischen dem Recht, das sich in der DSGVO niedergeschlagen hat, und dem tatsächlichen Rechtsvollzug bei der grenzüberschreitenden Datenverarbeitung markiert die größte Schwachstelle des neuen Datenschutzrechts. Anstrengungen sind erforderlich, gerade bei der Massendatenverarbeitung durch globale Internetdiensteanbieter einen hohen Vollzugsgrad durchzusetzen. Schließlich war eines der zentralen Ziele der DSGVO, den Schutz der Privatsphäre gegenüber multinationalen Internetdienstleistern zu stärken.

Es gibt derzeit verschiedene Ursachen, weshalb ein effektiver und effizienter Vollzug nicht stattfindet. Zum einen braucht es Zeit, bis die Maßnahmen durch die Behörden greifen. Auch die Aufsichtsbehörden mussten sich zunächst einmal auf die neuen Regelungen durch die DSGVO einstellen. Einige Fälle, die zu rechtlichen Sanktionen führten und die gerichtlich überprüft wurden, stammen noch aus der Zeit vor Inkrafttreten der DSGVO und richten sich noch nach dem alten Recht. Zum anderen erschweren die komplexen Vorschriften im Bereich des grenzüberschreitenden Vollzugs, die eine federführende und verschiedene betroffene Behörden einbinden und dem Prinzip einer einzelnen Anlaufstelle eines Datenverarbeiters in der EU (sog. One-Stop-Shop) folgen, den Vollzug erheblich. Weitgehende Informations- und Kooperationsanstrengungen zwischen den beteiligten Aufsichtsbehörden, aber auch mit dem Europäischen Datenschutzausschuss, hemmen schnelle Entscheidungen. Die Regelungen zum aufsichtsbehördlichen Handeln erweisen sich in der

Realität als schwerfällig und verlagern die Auseinandersetzungen über Sanktionen auf eine interne Ebene der gemeinsamen behördlichen Abstimmungen. Unterschiedliche Sichtweisen, voneinander abweichende Verfahrensbestimmung und divergierende rechtskulturelle Verständnisse über den Einsatz von Vollzugsinstrumenten zwischen den Behörden der Mitgliedstaaten führen in der Praxis zu weiteren Effizienzeinbußen.

Auch der mit einer weitgehenden Unabhängigkeit der federführenden Behörde verbundene sog. One-Stop-Shop, der in Europa jedem hier vertretenen Unternehmen eine Aufsichtsbehörde als Single Point of Contact zuweist, ist problematisch. Als zentrales Vollzugsdefizit ist derzeit das Ausbleiben von Entscheidungsentwürfen durch die zuständigen federführenden Behörden am Ort des Sitzes der verantwortlichen Stellen auszumachen. Die federführenden Behörden fungieren im grenzüberschreitenden Bereich als Initiatoren von aufsichtsbehördlichen Verfahren. Tun sie nichts, so kommt es auch zu keiner Ahndung von Verstößen, da das gemeinsame aufsichtsbehördliche Verfahren dann ohne Input bleibt. Insbesondere fehlen verfahrensrechtliche Korrektive für den Fall, dass federführende Behörden untätig bleiben und über lange Zeiträume keine Entwürfe über Entscheidungen in das Verfahren einbringen.

Um auszuloten, welche Maßnahmen zur Beseitigung derzeitiger Defizite zu ergreifen sind, ist die anstehende Evaluation durch die EU-Kommission, die gemäß Art. 97 DSGVO bis zum 25. Mai 2020 zu erfolgen hat, von hoher Bedeutung. Hier gilt es, gerade auch legislative Korrekturen zu einer Optimierung der Vollzugssituation zu prüfen. Es bedarf eines schnellen Handelns, damit Vollzugsgerechtigkeit und Rechtsschutz Betroffener möglichst bald ausreichend hergestellt werden.

Schließlich haben die unterschiedlichen Vollzugstandards auch nachteilige Auswirkungen auf einen fairen Wettbewerb zwischen den Unternehmen auf dem gemeinsamen Markt. Die Schaffung einheitlicher rechtlicher Regelungen zur Harmonisierung des Daten-

schutzstandards reicht nicht aus. Entscheidend ist, dass gegenüber konkurrierenden Unternehmen innerhalb des gemeinsamen Marktes auch einheitliche Vollzugstandards greifen. Dies ist nicht gegeben, solange die Verfahren bei grenzüberschreitenden Datenschutzverstößen, denen insbesondere global agierende Datenverarbeiter unterliegen, nicht oder nur in weit geringerem Ausmaß zum Abschluss kommen als im nationalen Vollzug. Diese Situation wird zunehmend auch von deutschen bzw. Hamburger Unternehmen beklagt, deren Wettbewerber ihre Hauptniederlassungen in einem anderen Mitgliedstaat haben und damit der Kontrolle anderer federführender Datenschutzbehörden unterliegen.

Auffassungen, die darauf abzielen, bereits vor der anstehenden Evaluation von einer legislativen Revision der bestehenden Vorschriften durch die EU-Kommission abzusehen, weil damit eine Diskussion über die künftige Ausrichtung des Datenschutzes aktiviert würde, vermögen vor diesem Hintergrund letztlich nicht zu überzeugen. Bereits vor der Durchführung einer Evaluation gegen eine gesetzliche Reformierung von Bestimmungen zu sein, die sich in der Praxis als nicht sinnvoll erwiesen haben, hieße das Ergebnis der Evaluation vorwegzunehmen. In Art. 97 Abs. 5 DSGVO ist ausdrücklich bestimmt, dass die Kommission gegebenenfalls geeignete Vorschläge zur Änderung der DSGVO vorlegt. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit wird sich an der Evaluation beteiligen und sich im Rahmen seiner Aktivitäten im Europäischen Datenschutzausschuss dafür einsetzen, dass die asymmetrische Vollzugssituation das Projekt der Datenschutzgrundverordnung nicht auf lange Sicht in Frage stellt.

PRÜFUNGEN II.

1. Data Breach bei der Polizei

Insgesamt sind durch die Polizei Hamburg im vergangenen Jahr fünf sog. Data Breach-Meldungen erfolgt, von denen drei nicht den gesetzlichen Anforderungen entsprachen. In einem Fall hat der HmbBfDI die Polizei formell verwarnt. Alle diese Vorfälle hat der HmbBfDI zum Anlass genommen, sich an den Polizeipräsidenten zu wenden um auf die bestehenden Mängel in der Zusammenarbeit hinzuweisen.

Durch Einführung einer Reihe von Regelwerken in 2018, insbesondere der Richtlinie (EU) 2016/680 (sog. JI-Richtlinie) und der auf ihr beruhenden Gesetze sowie der DSGVO und des HmbDSG sind neben der Beibehaltung von alten Beteiligungs- und Kooperationspflichten gegenüber der Aufsichtsbehörde neue datenschutzrechtliche Anforderungen für die Polizei Hamburg hinzugekommen. Zu den neuen Verpflichtungen gehört die Meldung von Sicherheitsbrüchen, die zu Risiken für die betroffenen Personen führen (sog. Data Breaches). Die Rechtslage bei der Verarbeitung personenbezogener Daten durch die Polizei ist komplex:
Da die DSGVO auf die Datenverarbeitung im Rahmen der Strafverfolgung und der straftatbezogenen Gefahrenabwehr keine Anwendung findet, sondern diese Bereiche durch die JI-Richtlinie und die auf ihr beruhenden Vorschriften reguliert werden, ist im Rahmen jedes Data Breaches zu prüfen, welche Gesetzeswerke im konkreten Fall Anwendung finden. Die Polizei verarbeitet im Rahmen der ihr zugewiesenen klassischen Polizeitätigkeiten nämlich personenbezogene Daten sowohl im Bereich der JI-Richtlinie, als auch im Anwendungsbereich der DSGVO z.B. in Personalangelegenheiten. Zwar unterscheiden sich die Vorschriften hinsichtlich der Vorgaben im Falle eines Data Breaches kaum. Die Abhilfemöglichkeiten des HmbBfDI bei Feststellung eines Verstoßes sind jedoch im Bereich der DSGVO umfangreicher. So kommt es im Hinblick auf die für den HmbBfDI zu ergreifenden Maßnahmen ganz erheblich darauf an, in welchem Bereich der Polizei sich der Data Breach ereignet. Zudem waren die

Abhilfemöglichkeiten im Bereich der JI-Richtlinie aufgrund der noch nicht (vollständig) erfolgten Umsetzung der Richtlinie ins nationale Recht zum Zeitpunkt der Data Breaches erheblich eingeschränkt.

Sowohl nach Art. 31 JI-Richtlinie als auch nach Art. 33 DSGVO hat die Polizei als Verantwortliche Fälle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Kenntnis der Verletzung der Aufsichtsbehörde zu melden, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Ziel der Meldepflicht ist, dass Informationen schnellstmöglich die Aufsichtsbehörde erreichen, damit sich diese ein Bild von der Lage verschaffen kann. Die Meldepflicht steht in engem Zusammenhang mit der ggf. vorliegenden Verpflichtung der Polizei zur Benachrichtigung der Betroffenen nach Art. 34 DSGVO bzw. Art. 31 JI-Richtlinie, die in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden erteilten Weisung erfolgen soll (vgl. Ew. 62 d. JI-Richtlinie). Verspätete und/oder nicht vollständige Meldungen führen demgegenüber dazu, dass der HmbBfDI als datenschutzrechtliche Aufsichtsbehörde nicht in der Lage ist, die ihm zugewiesenen Aufgaben in der Effektivität ausüben zu können, wie es vom (europäischen) Gesetzgeber vorgesehen ist.

Bei drei von fünf dem HmbBfDI in 2019 durch die Polizei Hamburg gemeldeten Data Breaches ist eine den Anforderungen des Gesetzes entsprechende Meldung nicht in der vorgesehen Frist von 72 Stunden erfolgt.

- Die Meldung eines noch im Jahre 2018 erfolgten und der Polizei zur Kenntnis erlangten Datenschutzverletzung aus dem Anwendungsbereich der DSGVO wurde dem HmbBfDI erst im Jahr 2019 gemeldet. Dabei handelte es sich um eine schwerwiegende Offenlegung einer Vielzahl von Emailadressen aufgrund der Fehlversendung einer Email aus dem Bereich der Personalverwaltung. Darunter befanden sich auch besonders schützenswerte Daten, deren Offenlegung für die persönliche Sicherheit der Betroffe-

nen erhebliche Konsequenzen haben konnten. Der von der Polizei Hamburg für die verspätete Meldung angeführten Gründe, dass eine abschließende Bewertung der Sachlage zunächst nicht möglich gewesen sei, sowie Feiertags- und Urlaubsabwesenheit, stellt in dieser abstrakten Form keine ausreichende Begründung i.S.d. Art. 33 DSGVO dar. Ein halbes Jahr nach Geltungsbeginn der DSGVO konnte auch nicht erfolgreich eingewendet werden, dass eine Implementierung des Meldeverfahrens mit Prüfungs- und Bewertungskriterien noch nicht vollständig abgeschlossen sei. Der HmbBfDI hat daher von seinen in Art. 58 Abs. 2 DSGVO vorgegebenen Abhilfebefugnissen Gebrauch gemacht und die Polizei formell verwarnt.

- Dessen ungeachtet meldete die Polizei eine im Februar 2019 vorgefallene Datenschutzverletzung wieder verspätet erst im März 2019. Gegenstand des meldepflichtigen Vorfalls war die weisungswidrige Nutzung eines kommerziellen Messenger-Dienstes zur Verbreitung von personenbezogenen Daten eines unter Tatverdacht stehenden Kollegen aus einem dienstlichen Lagebericht durch Polizeibeamte. Dieser Vorfall, der dem Bereich der JI-Richtlinie zuzuordnen ist, war zunächst nur disziplinarrechtlich gewürdigt worden, eine Bewertung auf dem Gebiet des Datenschutzes fand durch die Polizei dagegen nicht statt.

- Von der Polizei aufgrund des vorherigen Data Breaches angekündigte Maßnahmen, konnten nicht verhindern, dass es im Oktober 2019 erneut zu einer verspäteten Meldung kam. Die Polizei Hamburg hatte sich zwar im Zeitfenster der 72 Stunden beim HmbBfDI gemeldet, jedoch nicht mit den ihr zu dem Zeitpunkt möglichen und obliegenden Mindestinformationen i.S.d. JI-Richtlinie bzw. DSGVO. Dem HmbBfDI wurde lediglich zur Kenntnis gebracht, dass eine nicht näher bezeichnete Datenschutzverletzung mittlerweile behoben sei und man sich gegen die Benachrichtigung von Betroffenen entschieden habe. Es wurde vorgeschlagen, dass sich der HmbBfDI in einem in 1-2 Wochen stattfindenden Treffen vor Ort durch den Leitungsstab

der Polizei die Vorgänge näher erläutern lassen solle. Zu weiteren Auskünften im schriftlichen Verfahren war die Polizei trotz Zusicherung größtmöglicher Vertraulichkeit durch den HmbBfDI nicht bereit. Letztlich wurde zwei Werktage später vor Ort mitgeteilt, dass es sich um einen Sicherheitsbruch handelt, der sich ereignete, weil im Rahmen einer Neugestaltung einer Ordnerstruktur ein Fehler bei der Rechtevergabe zum Zugang von einem Ordner verursacht wurde, der besonders schützenswerte personenbezogene Daten enthält. Mitarbeiter der Polizei, denen der Zugang zu personenbezogenen Daten in diesem Ordner bisher nicht zustand, haben somit die theoretische Möglichkeit des Zugangs erhalten. Die für die Betroffenen hieraus resultierenden Gefahren waren immens.

Die Häufung verspäteter Meldungen lässt befürchten, dass bei einigen Teilen der Polizei keine hinreichende Sensibilisierung für die Meldepflichten gegenüber dem HmbBfDI und dessen Aufgabenwahrnehmung besteht. Der HmbBfDI hat diese Vorfälle zum Anlass genommen in einem Brief an den Hamburgischen Polizeipräsidenten auf die bestehenden Defizite in der Kommunikation mit dem HmbBfDI als Aufsichtsbehörde hinzuweisen. Ziel soll es insbesondere sein, einen Prozess zur Optimierung von Handlungsabläufen und Personalverstärkung im Bereich des Datenschutzes bei der Polizei anzustoßen.

2. VIDEOÜBERWACHUNG HANSAPLATZ

Seit 1. August 2019 werden der Hansaplatz und angrenzende Straßen im Stadtteil St. Georg von der Polizei Hamburg videoüberwacht. Der HmbBfDI überprüft, ob die gesetzlichen Voraussetzungen dafür vorliegen.

Im Dezember 2018 erhielt der HmbBfDI Kenntnis davon, dass die Polizei Hamburg beabsichtige, am Hansaplatz in St. Georg eine Videoüberwachung zu installieren. Den HmbBfDI erreichten in

diesem Zusammenhang zahlreiche Presseanfragen und Rückfragen von besorgten Bürgerinnen und Bürgern, die von der geplanten Videoüberwachung voraussichtlich betroffen waren, sodass er eine Prüfung dieser von der Polizei geplanten Maßnahmen einleitete.

Als Rechtsgrundlage gab die Polizei § 8 Abs. 3 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) an. Danach darf die Polizei zur vorbeugenden Bekämpfung von Straften öffentlich zugängliche Straßen, Wege und Plätze mittels Bildübertragung offen beobachten und Bildaufzeichnungen von Personen anfertigen, soweit an diesen Orten wiederholt Straftaten der Straßenkriminalität begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung derartiger Straftaten zu rechnen ist (sogenannte offene präventive Videoüberwachung). Es muss sich bei dem überwachten Gebiet also im Vergleich zu anderen Teilen der Stadt um einen sog. Schwerpunkt der Straßenkriminalität handeln. Zudem muss die Polizei eine negative Prognose für die weitere Entwicklung der Kriminalitätslage anstellen. Nicht gestattet ist dagegen die Videoüberwachung von Gebäuden, Gebäudeteilen und Flächen, die zwar öffentlich zugänglich sind, aber nicht zu den öffentlich zugänglichen Straßen, Wege und Plätzen gehören (sog. private zones). Die Polizei Hamburg muss daher durch eine entsprechende Ausrichtung der Kamera oder einer Verpixelung sicherstellen, dass insbesondere keine Hauseingänge und Fenster von Wohngebäuden oder Geschäftsräumen überwacht werden.

Gerne hätte der HmbBfDI das Vorliegen dieser Voraussetzungen geprüft. Weitere Informationen, insbesondere die für eine Überprüfung der Rechtmäßigkeit der geplanten Videoüberwachung dringend erforderliche Kriminalstatistik, ließen jedoch auf sich warten: So hatte die Polizei die Übersendung dieser Unterlagen zwar bis Mitte Januar 2019 angekündigt, auf Nachfrage des HmbBfDI nach dem Verbleib dieser Unterlagen dagegen immer wieder mitgeteilt, dass sich diese Unterlagen beim Leitungsstab befänden und daher noch nicht übermittelt werden könnten. Der HmbBfDI musste die Beschwerdeführer also immer wieder darauf vertrösten, dass diese Rückmeldung er-

halten würden, wenn die für die weitere Prüfung erforderlichen Unterlagen vorlägen. Es sorgte daher für eine gewisse Überraschung, als der HmbBfDI davon Kenntnis erlangte, dass die Polizei bereits im Juni 2019 einen Testbetrieb der Videoüberwachungsanlage plante und am 1. August 2019 in den Echtbetrieb überging. Denn auch bis zu diesem Zeitpunkt waren die für eine Überprüfung der geplanten Überwachung dringend erforderlichen Unterlagen dem HmbBfDI nicht übermittelt worden. Vielmehr erhielt er diese mit Schreiben vom 1. August 2019 und damit parallel zum Übergang in den Echtbetrieb der Videoüberwachung.

Der HmbBfDI verschaffte sich am 22. September 2019 vor Ort einen Überblick über die Maßnahme. Dabei ging es vor allem darum, zu prüfen, ob auf die Videoüberwachung seitens der Polizei angemessen hingewiesen wurde und diese so ausgerichtet wurden, dass sie keinerlei Hauseingänge oder Wohngebäude erfassten, bzw. diese mit angemessenen Filtern geschützt waren. Im Nachgang ergaben sich noch eine Reihe von Fragen, sowohl hinsichtlich technischer als auch rechtlicher Belange, die noch abschließend geprüft werden müssen.

Die dargelegten Verzögerungen hat der HmbBfDI jedoch zum Anlass genommen, auf diese – und andere aufgetretenen Mängel bei der Zusammenarbeit mit der Polizei – in einem förmlichen Anschreiben an den Polizeipräsident hinzuweisen (vgl. auch unter II. 1):

Die auf Art. 26 der JI-Richtlinie beruhende neue Regelung in § 74 PolDVG sieht ganz allgemein vor, dass der Verantwortliche mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten muss. Durch verspätete Einbindungen, aber auch verspätete Übermittlung relevanter Dokumente, kommt die Polizei Hamburg dieser Verpflichtung nach Eindruck des HmbBfDI in vielen Fällen nicht hinreichend nach. Dies führt dazu, dass der HmbBfDI als datenschutzrechtliche Aufsichtsbehörde leider nicht immer in der Lage ist, die ihm zugewiesenen Aufgaben in der Effektivität ausüben zu können, wie es vom (europäischen) Gesetzgeber vorgesehen ist.

Über das Ergebnis der Prüfung wird der HmbBfDI im kommenden Tätigkeitsbericht berichten.

3. Verdeckte Videoüberwachung der Polizei im Kleinen Schäferkamp

Der Presse war Anfang Februar 2019 zu entnehmen, dass durch eine in einer Trinkflasche eingebaute und auf einer Fensterbank einer Seniorenresidenz platzierte Kamera ein auf der gegenüberliegenden Straßenseite befindliches Wohnprojekt und ein sogenannter Infoladen, beide der linken Szene zugeordnet, mit einer Videokamera überwacht worden sein sollen. Eine Prüfung ergab ernsthafte Zweifel an der Zulässigkeit der verdeckten Maßnahme.

Aus Medienberichten konnte der HmbBfDI im Februar 2019 entnehmen, dass im dritten Stock einer Seniorenresidenz im Kleinen Schäferkamp im Hamburger Schanzenviertel eine in einer Cola-Flasche versteckte Videokamera entdeckt wurde, die laut Berichterstattung von der Polizei Hamburg stammen sollte. Auf Nachfrage wurde dem HmbBfDI von der Polizei Hamburg dies weitgehend bestätigt. Es sollte sich bei dem Einsatz der Kamera um eine personenbezogene Observation handeln. Nach Angaben der Polizei wurde die Kamera am 7. Dezember 2018 eingerichtet und am 6. Februar 2019 wieder abgebaut. Bei der im Bereich der Gefahrenabwehr bzw. Straftatenverhütung angesiedelten Maßnahme habe es sich um eine Datenerhebung durch den verdeckten Einsatz technischer Mittel nach § 10 Abs. 1 PolDVG im Rahmen einer längerfristigen Observation nach § 9 Abs. 1 PolDVG gehandelt.

Eine längerfristige Observation i.S.d. Norm ist eine planmäßig angelegte Beobachtung, die innerhalb einer Woche länger als 24 Stunden oder über den Zeitraum einer Woche hinaus vorgesehen ist oder tatsächlich durchgeführt wird. Zulässig ist sie nur dann, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bun-

des oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist (§ 9 Abs. 1 S. 1 Nr. 1 PolDVG) oder Tatsachen die Annahme rechtfertigen, dass eine Person Straftaten von erheblicher Bedeutung begehen wird (§ 9 Abs. 1 S. 1 Nr. 2 PolDVG). Der Einsatz von technischen Mitteln nach § 10 Abs. 1 PolDVG, zu denen neben dem Anfertigungen von Bildaufnahmen und Bildaufzeichnungen auch technische Mittel zur Ermittlung des Aufenthaltsortes (z.B. GPS-Sender) zählen, unterliegt ganz ähnlichen Voraussetzungen. Für längerfristige Observationen, als auch die Anfertigung von Bildaufnahmen und Bildaufzeichnungen, sieht das Gesetz zudem eine schriftliche Anordnung des Polizeipräsidenten vor (vgl. § 9 Abs. 2 i.V.m. § 10 Abs. 2 S. 1 PolDVG), die sich der HmbBfDI zur Prüfung hat vorlegen lassen.

Der HmbBfDI hat am 19. Februar 2019 zudem einen Ortsbesuch im Kleinen Schäferkamp durchgeführt. Schwerpunkt der Vorortprüfung war, ob tatsächlich, wie zuvor von der Polizei gegenüber dem HmbBfDI angegeben, keine privaten Wohnräume vom Bildausschnitt der Kamera erfasst wurden. Denn das Filmen von Hauseingängen zu privaten Wohnräumen ist wesentlich eingriffsintensiver und würde daher erhöhten gesetzlichen Voraussetzungen unterliegen.

Nach umfangreicher Prüfung hat der HmbBfDI ernsthafte Zweifel an der Rechtmäßigkeit der Maßnahme, sowohl im formellen als auch im materiellen Bereich. Auf diese kann hier jedoch wegen der Einstufung der Sache als Verschlusssache leider nicht näher eingegangen werden. Der HmbBfDI wird die aus dieser Prüfung gewonnenen Erkenntnisse zum Anlass nehmen, die Einhaltung der materiellen und verfahrensrechtlichen Anforderungen bei verdeckten Maßnahmen durch die Polizei in Zukunft genauer zu prüfen. Dies nicht zuletzt auch, weil dem HmbBfDI diesbezüglich neue Prüfplichten übertragen worden sind: Ab 2022 hat der HmbBfDI nach § 73 PolDVG die Einhaltung der Vorschriften zur längerfristigen Observation (Neu: § 20 PolDVG) als auch zum verdeckten Einsatz technischer Mittel (Neu: 21 PolDVG) ab 2022 im Abstand von höchstens zwei Jahren zu kontrollieren. Auch zwischenzeitlich wird eine Überprüfung derartiger Maßnahmen erfolgen.

Die Anordnung längerfristiger Observationen ist zukünftig unter einen Richtervorbehalt gestellt. Diese auf der Rechtsprechung des Bundesverfassungsgerichts beruhende Ergänzung ist ausdrücklich zu begrüßen, weil nunmehr in Zukunft stets eine (weitere) unabhängige Stelle eine Prüfung vornimmt.

4. IT-VERFAHREN ZENTRALER MELDEBESTAND

Die Meldebehörden speichern die Protokolle der automatisierten Abrufe der Sicherheits- und Strafverfolgungsbehörden, obwohl das Bundesmeldegesetz explizit festlegt, dass dies ausschließlich durch die Sicherheits- und Strafverfolgungsbehörden zu erfolgen hat.

Das IT-Verfahren Zentraler Meldebestand (ZMB) wurde im Rahmen eines Länder- Kooperations-Projektes für den automatisierten Meldedatenabruf gemäß Bundesmeldegesetz (BMG) für die Dataport-Trägerländer Hamburg, Sachsen-Anhalt und Schleswig-Holstein entwickelt. Es wird seit Januar 2016 insbesondere für automatisierte Behördenauskünfte, automatisierte einfache Melderegisterauskünfte, den vorausgefüllten Meldeschein, regelmäßige Datenübermittlungen an Dritte und für Auswertungen von Meldedaten eingesetzt. Gemeinsam mit den Datenschutz-Aufsichtsbehörden aus Sachsen-Anhalt und Schleswig-Holstein prüft der HmbBfDI dieses IT-Verfahren seit Herbst 2016. Den Schwerpunkt der Prüfung des Fachverfahrens ZMB bildet die Umsetzung der Datensicherheit, insbesondere die Gewährleistung der Vertraulichkeit und der Trennung der gespiegelten Meldedatenbestände der beteiligten Länder.

Die Meldedaten der drei beteiligten Länder werden im sogenannten Mehrländer-Meldedatenspiegel gespeichert. Die Trennung erfolgt einerseits, indem für jedes Land ein „Ländermandant“ eingerichtet wurde und für jeden dieser Mandanten eine eigene Datenbank für

die Verarbeitung genutzt wird. Innerhalb der „Ländermandanten“ kann eine weitere Trennung in Untermandanten erfolgen. Dies ist in Hamburg aufgrund des bestehenden gesetzlich geregelten zentralen Melderegisters und der Allzuständigkeit der hamburgischen Meldebehörden jedoch nicht erforderlich.

Neben den Meldedaten werden in den jeweiligen Datenbanken der „Ländermandanten“ auch die Protokolle der automatisierten Abrufe aus dem ZMB gespeichert. Rechtsgrundlage für die Protokollierung der Abrufe ist § 40 BMG, nach der grundsätzlich die Meldebehörden die automatisierten Abrufe protokollieren. Etwas anderes gilt jedoch, wenn die abrufende Stelle eine Sicherheits- oder Strafverfolgungsbehörde ist. Diese Behörden müssen die Protokollierung der automatisierten Abrufe selbst vornehmen.

Die drei ZMB-Länderverantwortlichen haben den IT-Dienstleister Dataport mit der Durchführung der Verarbeitung beauftragt. Im Zuge der Prüfung wurde bekannt, dass dieser Auftragsvertrag überraschenderweise auch die Protokollierung der automatisierten Abrufe der Sicherheits- und Strafverfolgungsbehörden gemäß § 40 Abs. 3 BMG umfasst. Eine rechtliche Grundlage für diese Beauftragung liegt weder für die hamburgischen noch für die externen Sicherheits- und Strafverfolgungsbehörden vor. Bezüglich der externen Behörden ist dies umso verwunderlicher, da ein automatisierter Abruf von Externen grundsätzlich nur möglich ist, wenn diese Stelle vorher einen entsprechenden Antrag für die Einrichtung eines Zugangs stellt. In diesem Antragsformular geben die hamburgischen Verantwortlichen für das ZMB den externen Sicherheits- und Strafverfolgungsbehörden folgenden Hinweis:

> ***Besonderheiten für Sicherheits- und Strafverfolgungsbehörden***
> *Sicherheits- und Strafverfolgungsbehörden sind verpflichtet, die Zugriffe selbst aus ihrer Behörde zu protokollieren (§ 40 (3) BMG) und diese Protokolle regelmäßig auszuwerten.*

Alle Protokolle der automatisierten Abrufe der Sicherheits- und Strafverfolgungsbehörden werden für ein Jahr gespeichert. Das Ausmaß dieser Speicherung der Protokollierung ist bei Redaktionsschluss noch nicht bekannt, da auch fast zwei Monaten nach Anforderung der Protokollierungen der IT-Dienstleister Dataport diese noch nicht zur Verfügung gestellt hat.

Die drei ZMB-Länderverantwortlichen haben erklärt, dass zukünftig die Protokollierung der Abrufe der Sicherheits- und Strafverfolgungsbehörden nach § 40 Abs. 3 BMG nicht mehr durch die Meldebehörden im ZMB erfolgen soll. Sie haben angekündigt, dass eine Protokollierung für die Sicherheits- und Strafverfolgungsbehörden im Wege der Auftragsverarbeitung stattfinden könne, sofern die für die jeweilige Protokollierung verantwortliche Sicherheits- bzw. Strafverfolgungsbehörde unmittelbar einen entsprechenden Auftragsvertrag mit dem IT-Dienstleister schließt. Die technischen und organisatorischen Details der Veränderung des Verfahrens werden derzeit von den ZMB-Verantwortlichen geplant und sind dem HmbBfDI bei Redaktionsschluss noch nicht bekannt. Der HmbBfDI wird sich in 2020 mit Nachdruck dafür einsetzen, dass eine vollständige Trennung der Protokolldaten der Sicherheits- und Strafverfolgungsbehörden vom IT-Verfahren ZMB sowohl organisatorisch als auch technisch gewährleistet wird.

Im Zuge der Prüfung wurden u.a. folgende weitere Mängel deutlich:

- Die vorhandenen Verträge, Dokumentationen und zugrundeliegenden Unterlagen wurden zum Teil nicht entsprechend den eigenen Vorgaben des IT-Dienstleisters regelmäßig aktualisiert und Anpassungen an die Veränderungen, die aufgrund der Datenschutz-Grundverordnung (DSGVO) hätten erfolgen müssen, wurden nicht fristgerecht durchgeführt.
- Die DSGVO sieht für ein Mehrländer-Verfahren vor, dass die gemeinsam Verantwortlichen eine Vereinbarung nach Art. 26 DSGVO schließen müssen, in der sie in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt. Obwohl die Datenschutz-Aufsichtsbehörden die

ZMB-Länderverantwortlichen bereits im November 2018 auf diesen Aspekt hingewiesen haben, sagten diese erst im September 2019 zu, eine solche Vereinbarung gemäß Artikel 26 DSGVO zu erstellen. Der Entwurf ist den Datenschutz-Aufsichtsbehörden kurz vor Redaktionsschluss zugegangen.

- Aufgrund des hohen Schutzbedarfs der Daten, die im ZMB verarbeitet werden, wurde 2015 zwar die Möglichkeit eines Penetrationstests zwischen den ZMB-Länderverantwortlichen und dem IT-Dienstleister erörtert, eine abschließende Prüfung und Entscheidung durch die Verantwortlichen blieb zum damaligen Zeitpunkt jedoch aus. Erst als dieser Aspekt auch in den Prüfbericht Eingang fand, haben die Verantwortlichen im Oktober 2019 einen Penetrationstest für das 1. Quartal 2020 angekündigt.
- Die Prüfung hat ergeben, dass über 50 Administratoren des IT-Dienstleisters Dataport für unterschiedliche administrative Aufgaben Zugriff auf das ZMB haben. Die erforderlichen Zugriffsrechte könnten aber auch zur Einsichtnahme und zum Abzug von Daten missbraucht werden. Die gesetzlichen Grundlagen sowohl zum Zeitpunkt des Beginns der Prüfung als auch seit Geltung der DSGVO fordern von den Verantwortlichen, die Vertraulichkeit und Revisionssicherheit des Verfahrens zu gewährleisten. Aufgrund des hohen Schutzbedarfs der verarbeiteten Daten kommt der präventiven Wirkung der Protokollierung hier eine besondere Bedeutung zu. Vor diesem Hintergrund ist es problematisch, dass die Tätigkeiten der Administratoren zwar mit einer Videoprotokollierung der Zugriffe, die über die Adminplattform erfolgen, aufgezeichnet werden, sich diese Protokolle jedoch nicht automatisiert auswerten lassen. Aus diesem Grund werden bisher diese Protokolle im Gegensatz zu anderen Protokollen keiner Stichprobenprüfung unterzogen. Es erfolgen im Bedarfsfall nur anlassbezogene Prüfungen, für die eine Eingrenzung auf einen sehr konkreten Zeitraum erforderlich ist. Das reduziert die präventive Wirkung der Protokollierung erheblich. Dataport hat angekündigt bis Ende 2019 einen Use Case zu erstellen, in dem eine verbesserte Auswertung dieser Videoprotokolle dargelegt werden soll.

- Auch der Entsorgungsprozess von Festplatten, auf denen die Daten des ZMB gespeichert sind, wurde kontrolliert. Dabei wurde festgestellt, dass weder dokumentiert wird, ob die defekten Festplatten, die dem Incidentmanagement gemeldet wurden, auch in den dafür vorgesehenen Sammelbehältern innerhalb des geschützten Rechenzentrums für die Vernichtung deponiert wurden, noch lückenlos dokumentiert wird, dass ebendiese Festplatten tatsächlich jene sind, die nach der vorgegebenen Sicherheitsstufe durch das beauftragte Entsorgungsunternehmen vernichtet werden sollten. Die Anforderungen an die Revisionsfähigkeit werden diesbezüglich nicht ausreichend erfüllt. Eine abschließende Antwort der Verantwortlichen bzw. des beauftragten IT-Dienstleisters Dataport steht noch aus.

Der HmbBfDI und die weiteren an der Prüfung beteiligten Datenschutz-Aufsichtsbehörden werden auch im Jahr 2020 die Beseitigung der festgestellten Mängel beharrlich weiter verfolgen, bis die datenschutzrechtlichen Anforderungen in ausreichendem Maße realisiert werden.

5. PROTOKOLLIERUNG LESENDER ZUGRIFFE INNERHALB EINES KIS

Wer in einem Krankenhaus behandelt wird, hat die berechtigte Erwartung, dass seine dort verarbeiteten sensiblen personenbezogenen Daten grundsätzlich nur von den für seine Behandlung und Pflege zuständigen Personen zur Kenntnis genommen und genutzt werden. Um dieser mit dem Datenschutzgrundsatz der Vertraulichkeit hinterlegten Erwartungshaltung zu genügen, müssen in sog. Krankenhausinformationssystemen nicht nur schreibende, sondern auch lesende Zugriffe auf die dort verarbeiteten personenbezogenen Daten protokolliert und geeignete Möglichkeiten zur Auswertung vorgehalten werden.

Krankenhausinformationssysteme (KIS) zählen aufgrund ihrer Komplexität, der enormen Menge in ihnen verarbeiteter Gesundheitsdaten, der Vielzahl unterschiedlicher Benutzer und der existenziellen Relevanz ihrer Performanz sowie der Verfügbarkeit und Richtigkeit der Daten zu den hoch risikobehafteten Datenverarbeitungssystemen. Dem bestehenden hohen Risiko ist mit umfassenden technischen und organisatorischen Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus zu begegnen. In technischer Hinsicht schließt dies ein geeignetes Instrumentarium ein, um die Nutzung des KIS zur Verarbeitung personenbezogener Daten nachvollziehen zu können. Grundlage dafür ist eine aussagefähige Protokollierung einschließlich geeigneter Auswertungsmöglichkeiten.

Bereits der Orientierungshilfe Krankenhausinformationssysteme der DSK-Arbeitskreise Gesundheit und Soziales sowie Technik in ihrer 2. Fassung (März 2014) war diesbezüglich zu entnehmen, dass von den Datenschutzaufsichtsbehörden des Bundes und der Länder neben der Eingabenkontrolle im engeren Sinne auch eine Protokollierung der lesenden Zugriffe auf personenbezogene Datensätze im KIS für notwendig gehalten wird. Auch unter Geltung der DSGVO ist die Zugriffsprotokollierung als geeignete und erforderliche technische Maßnahme anzusehen, um ein den Vorgaben aus Art. 5 Abs. 1 lit. f und Abs. 2, 24 Abs. 1 und 32 Abs. 1 lit. b DSGVO entsprechendes Schutzniveau zu gewährleisten. Die fehlende ausdrückliche Erwähnung der Protokollierung lesender Zugriffe als Regelbeispiel in § 22 Abs. 2 BDSG steht dem nicht entgegen. Der Katalog des § 22 Abs. 2 BDSG ist weder abschließend noch für Verarbeitungen auf der Grundlage von Art. 9 Abs. 2 lit. h DSGVO unmittelbar einschlägig. § 22 Abs. 2 BDSG nennt lediglich beispielhaft in Betracht kommende angemessene und spezifische Maßnahmen und deckt bei weitem nicht das gesamt mögliche und unter Umständen nötige Bündel technisch-organisatorischer Maßnahmen zum Schutz besonderer Kategorien personenbezogener Daten ab. Ein genereller Verzicht auf die Protokollierung lesender Zugriffe ist auch bei Vorhalt eines differenzierten Rollen- und Berechtigungskonzepts angesichts von

Notfallzugriffsberechtigungen des ärztlichen Personals, stationsübergreifenden Zugriffsberechtigungen von medizinischem Personal mit klinikübergreifenden Querschnitts- oder Spezialaufgaben und technisch-administrativen Zugriffsmöglichkeiten auf das KIS nicht gerechtfertigt. Der Protokollierung kommt insoweit eine Doppelfunktion als vorbeugende Maßnahme der Zugriffskontrolle einerseits und Maßnahme zur Nachweisbarkeit von Verarbeitungsvorgängen andererseits zu.

Der HmbBfDI hat sich daher anlässlich der Feststellung von Protokollierungsdefiziten im Zusammenhang mit einem vermuteten unbefugten KIS-Zugriff auf Patientendaten in einem Hamburger Krankenhaus zu breit angelegten Sensibilisierungs- und Prüfungsaktivitäten veranlasst gesehen. Dazu sind die Träger sämtlicher durch den HmbBfDI beaufsichtigter Krankenhäuser in einem ersten Schritt auf das Erfordernis einer revisionsfesten Protokollierung schreibender und lesender Zugriffe innerhalb eines KIS einschließlich geeigneter Auswertungsmöglichkeiten als Rahmenbedingung für den datenschutzkonformen Einsatz des KIS hingewiesen worden. In einem zweiten Schritt wurden die Träger für den Fall des Betriebs eines KIS zur Vorlage Ihres diesbezüglichen Protokollierungs- und Auswertungskonzepts aufgefordert. Der HmbBfDI wird die eingehenden Unterlagen einer technischen und rechtlichen Prüfung unterziehen, um sich so über die Gewährleistung eines angemessenen Schutzniveaus beim Einsatz eines KIS zu vergewissern und im Falle von Unzulänglichkeiten geeignete Abhilfemaßnahmen ergreifen zu können.

In dem Fall, welcher Anlass für die flächendeckende Prüfung gegeben hat, ist aufgrund festgestellter Protokollierungsdefizite ein Bußgeldverfahren eingeleitet worden.

6. Hochaufgelöste Luftbilder im Geoinformationsportal

Der Landesbetrieb Geoinformation und Vermessung wurde wegen der unbeabsichtigten Veröffentlichung detaillierter Bilder des gesamten Stadtgebietes verwarnt.

Zu stadtplanerischen Zwecken verfügt der Landesbetrieb Geoinformation und Vermessung (LGV) über umfangreiches Kartenmaterial sowie Luftbildaufnahmen. Die Daten dienen primär dazu, die Aufgabenerfüllung der Hamburgischen Behörden zu unterstützen. Teilweise stehen sie auch der Öffentlichkeit zur Verfügung, indem sie über das Internetportal Geo-Online abgerufen werden können. Zu den schon länger online verfügbaren Ablichtungen aus der Vogelperspektive sind im Dezember 2018 Schrägluftbildaufnahmen hinzugekommen. Diese bilden Grundstücke nicht senkrecht von oben ab, sondern aus einem leichten Winkel, sodass auch Fassaden erkennbar sind. Die Schrägluftbildaufnahmen können aus vier Himmelsrichtungen abgerufen werden.

Für die Zulässigkeit der Veröffentlichung von Luftbildern ist ein Grenzwert von 20 cm pro Pixel entscheidend. Liegt die Auflösung darunter, geht man davon aus, dass es sich bei den Bildern um personenbezogene Daten der Bewohner, Besucher und Eigentümer der abgebildeten Grundstücke handelt. Dementsprechend darf der LGV höher aufgelöste Bilder, die er aufgrund seines gesetzlichen Auftrags erheben und speichern darf, nur in einer niedriger aufgelösten Variante öffentlich verfügbar machen. Daher hatten der LGV und der HmbBfDI sich im Jahr 2012 darauf verständigt, dass nur Bilder mit einer Auflösung von mindestens 20 cm pro Pixel im Portal Geo-Online veröffentlicht werden sollten.

Nach der Veröffentlichung der Schrägluftbildaufnahmen fiel dem HmbBfDI deren hoher Detailgrad auf. Auf seine Nachfrage hin räumte der LGV ein, dass er unbeabsichtigt Schrägluftbilder der Stadt Hamburg mit einer Auflösung von 7 cm pro Pixel am unteren Bild-

rand und 11 cm pro Pixel am oberen Bildrand veröffentlicht hatte. Dies geschah aufgrund eines Konfigurationsfehlers, der zu einer Verlinkung auf einen falschen Bildordner geführt hatte. Nachdem wir den LGV auf den hohen Detailgrad aufmerksam gemacht hatten, schaltete dieser unverzüglich die Darstellung der Bilder im Geo-Online-Portal ab. Nach Behebung des Fehlers sind die Bilder nun wieder in einer zulässigen, niedrigen Auflösung abrufbar. Der HmbBfDI hat den LGV wegen der unzulässigen Veröffentlichung personenbezogener Daten verwarnt. Zudem hat er darauf hingewirkt, dass der LGV die Öffentlichkeit über den Vorfall informiert hat.

Die Speicherung von Luftbildern mit Personenbezug hat auch Auswirkungen auch die Rechte der Betroffenen. Dem HmbBfDI lag eine Beschwerde eines Bürgers vor, der Auskunft über die beim LGV zu seiner Person gespeicherten Daten verlangt hatte. Die Antwort des LGV beschränkte sich im Wesentlichen auf einen Grundbuchauszug. Auf das Hinwirken des HmbBfDI hin wurden dem Betroffenen nun die hochaufgelösten Lichtbilder seiner Immobilie zugeschickt.

7. PERSONALVERWALTUNGSSOFTWARE KOPERS

Die vom HmbBfDI über viele Jahre begleitete Entwicklung und Einführung der Personalverwaltungssoftware für Bedienstete des öffentlichen Dienstes ist nun abgeschlossen.

In seinem Tätigkeitsbericht 2008/2009 hat der HmbBfDI angekündigt, dass die Freie und Hansestadt Hamburg eine umfassende Digitalisierung seiner internen Personalverwaltung anstrebte und dafür in Kooperation mit Schleswig-Holstein die Personalplanungs- und Verwaltungssoftware KoPers entwickeln wollte. Im jetzigen Berichtszeitraum konnten nun die entsprechenden Verfahren in nahezu allen Behörden eingeführt werden. Der besonders große Umfang

der Beschäftigtendaten sowie die zum Teil hohe Sensibilität machten eine enge datenschutzrechtliche Begleitung erforderlich. Der HmbBfDI war von Anfang an in der Lenkungsgruppe und zahlreichen Arbeitsgruppen beteiligt und hat dadurch im Detail an einer datenschutzgerechten Gestaltung mitgewirkt.

Der problematischste Punkt war das Bedürfnis einzelner Behörden, auf die Rohdaten zuzugreifen. Um behördenspezifische Planungen durchzuführen oder z.B. Bürgerschaftsanfragen zu beantworten, besteht neben dem Zugriff über die KoPers-Oberfläche die Möglichkeit, im Einzelfall über das Modul HRBC direkt auf die Daten der Beschäftigten zuzugreifen. Während bei den regulären Datenabfragen über die Software KoPers die Abfragefunktionen am Grundsatz der Datenminimierung orientiert sind, sind bei der Nutzung der Rohdaten aus technischer Sicht beliebige Abfragen möglich. Um eine Umgehung der hohen Datenschutzstandards von KoPers zu verhindern, hat der HmbBfDI sich erfolgreich für eine Klausel in der entsprechenden landesweiten Dienstvereinbarung nach § 93 HmbPersVG eingesetzt. Danach dürfen solche Abfragen in der Regel nur erfolgen, wenn der jeweilige Personalrat der betreffenden Behörde zuvor zugestimmt hat. Die Zustimmung des Personalrats wirkt wie eine Einwilligung, die stellvertretend für die Beschäftigten abgegeben wird. Aufgrund der unabhängigen Stellung des Personalrats besteht das im Beschäftigtendatenschutz häufig auftretende Problem der fehlenden Freiwilligkeit hier nicht. Wegen der weitreichenden technischen Möglichkeiten des Direktzugriffs sind die Personalräte angehalten, entsprechende Anträge der Dienststellen kritisch zu hinterfragen und nur im zwingend erforderlichen Umfang zuzulassen.

In der Schlussphase des Projektes galt es vor allem, die notwendigen Anpassungen an die zwischenzeitlich wirksam gewordene DSGVO vorzunehmen. Hier war der HmbBfDI insbesondere bei der Abfassung der Datenschutz-Folgenabschätzung beratend involviert.

Für eine wesentliche Erweiterung ist bereits das Folgeprojekt HR Self-Services gestartet. Dieses hat zum Ziel, den Beschäftigten

eigenen Zugriff auf ihre in KoPers gespeicherten Daten zu ermöglichen, ausgewählte Daten selbst zu verändern und perspektivisch auch die Bezügemitteilung auf elektronischem Weg zu erhalten. Der HmbBfDI ist in dem Projekt ebenfalls in der Lenkungsgruppe und der Expertengruppe Datenschutz involviert. Die für ihn zentrale Problematik wird hier die Schaffung einer für den Schutzbedarf der abrufbaren Daten angemessenen sicheren Authentisierung sein. Parallel setzt sich der HmbBfDI im Projekt ePA für hohe Datenschutzstandards bei der Digitalisierung der Personalakten ein.

8. FEUERWEHR HAMBURG – NOCH IMMER KEIN SCHUTZ DER FUNKDATEN BEI DER NOTFALLALARMIERUNG

Auch drei Jahre nach Bekanntwerden des Mangels bei der Übertragung von Meldungen der Notfallalarmierung der Feuerwahr Hamburg ist der Mangel immer noch nicht behoben.

Bereits im Herbst 2016 hat der HmbBfDI erfahren, dass die Notfallalarmierungen der Feuerwehr Hamburg, die unverschlüsselt per Funk an die Einsatzkräfte übertragen werden, von Unbekannten illegal abgehört wurden. Die sensiblen personenbezogenen Daten wurden ins Internet gestellt. Als erste kurzfristige Maßnahme wurden die übertragenen Daten zwar reduziert. Aber auch dieser reduzierte Datensatz enthält immer noch sensible Daten, die nur verschlüsselt übertragen werden dürfen. Sowohl im 26. TB II. 3 des HmbBfDI als auch im 27. TB II. 1 sind Berichte über diesen Mangel.

CHRONIK 2019

Zum **Jahresende 2018** kündigt die Feuerwehr Hamburg im Unterausschuss Datenschutz der Hamburgischen Bürgerschaft an, dass einerseits der bekanntgewordene Mangel durch die Einführung einer Verschlüsselung der Notfallalarmierungen während der Übertragung

zum Ende des 1. Quartals 2019 beseitigt werden soll. Dabei setzt die Feuerwahr Hamburg auf den Einsatz einer App, die auf den privaten Smartphones der Einsatzkräfte genutzt werden soll. Diese Lösung stellt ein Dienstleister Out of the Box zur Verfügung. Andererseits soll parallel zu diesem Verfahren auch der TETRA-BOS-Digitalfunk so ertüchtigt werden, dass darüber diese Notfallalarmierungen u.a. an die Freiwillige Feuerwehr versendet werden. Die Feuerwehr sieht diesen Übertragungsweg als den wichtigsten an. Die Feuerwehr Hamburg setzt aufgrund der erforderlichen Ausfallsicherheit auf zwei unabhängige Übertragungstechnologien.

Ende Januar 2019 wird eine Verständigung zwischen der Feuerwehr Hamburg und dem HmbBfDI erzielt, die auch die erforderlichen technischen und organisatorischen Maßnahmen umfasst, mit denen die sensiblen personenbezogenen Daten nicht nur auf dem Übertragungsweg sondern auch bezüglich der Verarbeitung auf den privaten Geräten geschützt werden. Dazu gehört, dass nur dezidiert zugelassene private Geräte an der Notfallalarmierung beteiligt sind, dass der Zugang zur App mit einer gesonderten PIN geschützt wird und dass die Notfalldaten eine Stunde nach der Übertragung automatisiert in der App gelöscht werden. Die Datenschutz-Folgenabschätzung und die Dokumentation des Verfahrens soll dem HmbBfDI zugesendet werden.

Ende Februar 2019 wird auf Nachfrage bekannt, dass bis Ende März zwar die App zur Verfügung gestellt wird, gleichzeitig jedoch neue technische Schwierigkeiten bei der Datenausleitung der Notfalldaten aus dem IT-Verfahren HELS bekannt geworden sind, die zunächst geklärt werden müssen. Diese Situation stellt den geplanten Produktivsetzungstermin Ende März 2019 zunächst in Frage, sodass die Feuerwehr Hamburg diesen Termin verschiebt.

In seiner Stellungnahme zum 27. Tätigkeitsbericht des HmbBfDI bestätigt der Senat im Mai 2019 die Darstellung des HmbBfDI und kündigt an, dass die Umsetzung des neuen Verfahrens erst im **2. Quartal 2019** erfolgen könne.

Auf Nachfrage wird im **Juni 2019** bekannt, dass die Datenschutz-Folgenabschätzung und die Dokumentation des Verfahrens nach wie vor noch nicht erstellt wurden. Diese erforderlichen Unterlagen werden dem HmbBfDI nunmehr für den **September 2019** angekündigt.

Anfang August 2019 teilt die Feuerwehr Hamburg dem HmbBfDI auf Nachfrage mit, dass der Einführungstermin sich auf den **01.10.2019** verschiebt. Der HmbBfDI bittet den Oberbranddirektor nachdrücklich darum, zumindest diesen Termin nun zu halten.

In der Datenschutz-Folgenabschätzung und der weiteren Unterlagen dokumentiert die Feuerwehr Hamburg im September 2019, dass die von ihr beauftragte Anpassung der App nicht alle erforderlichen Schutzmaßnahmen enthält. Insbesondere der Zugriffsschutz zur App, für den eine separate PIN eingegeben werden soll, wurde nicht beauftragt. Ein solcher Schutz ist gerade bei der Verarbeitung der sensiblen Daten auf privaten Geräten erforderlich, weil diese Geräte im Freundes- und Familienkreis auch anderen Personen zeitweilig überlassen werden. Auch in solchen Situation müssen die Daten vor einer unberechtigten Einsichtnahme geschützt werden.

Im Oktober 2019 erfährt der HmbBfDI wieder auf Nachfrage, dass die produktive Nutzung der App zur Notfallalarmierung nunmehr auf den **15.11.2019** verschoben wird. Die Feuerwehr Hamburg kündigt an, dass die erforderlichen Unterlagen entsprechend der Anmerkungen des HmbBfDI fortgeschrieben werden sollen.

Trotz mehrfacher Nachfragen des HmbBfDI verstreicht auch der 15.11.2019, ohne dass eine Produktivsetzung erfolgt ist. Gleichzeitig wird beim Rollout der App für die erste Wehr deutlich, dass ein gravierender Programmfehler im Freigabetest nicht erkannt wurde und vor dem weiteren Rollout-Prozess beseitigt werden muss. Die Feuerwehr teilt als neuen Produktivsetzungstermin Anfang **Januar 2020** mit. Die fortgeschriebenen Unterlagen und eine abschließende Aussage zum Zugriffsschutz zur App liegen dem HmbBfDI noch immer nicht vor.

Und was macht der Stand der seitens der Feuerwehr Hamburg als wichtigsten Übertragungsweg bezeichneten Nutzung des TETRA-BOS-Digitalfunks für die Notfallalarmierung? Trotz mehrfacher Nachfragen wurde dem HmbBfDI die erbetene Information zum Stand und der detaillierte Projektplanung erst im Dezember 2019 übersandt. Diese Planung konkretisiert die Mitteilung der Feuerwehr Hamburg im Unterausschuss Datenschutz und Informationsfreiheit der Bürgerschaft, dass der Termin der Einführung für das Jahr 2021 geplant ist. Der HmbBfDI wird auch diese Entwicklung eines sicheren Übertragungsweges für die Notfallalarmierung kontinuierlich begleiten.

Dieser Fall zeigt exemplarisch: Datenschutz und Datensicherheit sind immer abhängig vom Willen der zuständigen Behörde, die Rechte und Freiheiten der Betroffenen auch tatsächlich zu schützen und die Realisierung der erforderlichen technischen und organisatorischen Maßnahmen entsprechend zu priorisieren. Leider wird gerade dort, wo Behörden die Aufgaben haben, die öffentliche Sicherheit und die Gesundheit der Bürgerinnen und Bürger zu gewährleisten, der Datenschutz mitunter gegen diese Zielsetzung ausgespielt. Die Maßnahmen, die den Aufsichtsbehörden zur Verfügung stehen, um eine rechtmäßige Verarbeitung der Daten durchzusetzen, sind hier gerade mit Blick auf die zentrale Bedeutung der Aufgabenerfüllung begrenzt. Hier wäre daher die Möglichkeit sinnvoll, im Falle wiederholter Verstöße Bußgelder gegen die verantwortlichen Behörden zu verhängen. Dies wäre nach der Datenschutz-Grundverordnung möglich, wurde aber vom nationalen Gesetzgeber in Deutschland nicht vorgesehen.

9. Prüfung Microsoft Windows 10

Der HmbBfDI hat erneut die eingesetzte Konfiguration von Windows 10 für den Behördeneinsatz datenschutztechnisch untersucht.

In Anlehnung an die Überprüfung von Windows 10 Enterprise zur Einführung in der FHH im Jahr 2018 führte der HmbBfDI in diesem Jahr eine erneute Überprüfung durch. Hauptsächlich sollte wieder die Frage beantwortet werden, inwieweit ein Tracking durch Microsoft, mit dem eine einzelne Nutzerin oder Nutzer oder ein bestimmtes Gerät identifiziert werden können, vermieden werden kann, soweit dies nicht unbedingt für den Betrieb notwendig ist.

Windows 10 steht weiterhin in der Kritik von Datenschützern und IT-Fachleuten, da es umfangreiche Nutzungstelemetrie, Benutzertracking und auch Analysen aus Werbung an Microsoft sendet und somit einzelne Installationen oder Nutzerinnen und Nutzer wiedererkannt werden können. Diese Funktionalitäten stehen einem datenschutzgerechten Einsatz im Weg und werden daher regelmäßig von Stellen der öffentlichen Verwaltung und auch anderen Stellen im Bereich der IT-Sicherheit untersucht.
Microsoft änderte in der Vergangenheit häufig sowohl die Bezeichnung als auch die Funktionalität einzelner Einstellungsparameter (sog. Gruppenrichtlinien, GPO), was teilweise nach Aktualisierungen auf die neueste Version zu einem unerwarteten Verhalten des Systems oder ein Zurücksetzen der vorherigen Einstellungen führte. Im Berichtszeitraum wurde daher der letztjährige Test mit den aktuellsten Betriebssystem-Versionen von Windows 10 Enterprise wiederholt und der verbleibende Netzwerkverkehr analysiert.

Hierzu hat der HmbBfDI erneut in Kooperation mit Dataport als IT-Dienstleister der Stadt Hamburg ein Test-Aufbau entwickelt und die Änderungen zum letzten Jahr eingepflegt. Die Analyse basiert auf einer virtualisierten Windows Server- sowie Client-Instanz, die mittels eines sog. Man-in-the-Middle-Proxy sämtlichen Netzwerkverkehr protokollierte. Der Laboraufbau wurde so umgesetzt, dass

der Windows 10-Client über mehrere Tage normal genutzt wurde. Ein Großteil der Standardprogramme und Dienste wurde dabei durch die Gruppenrichtlinien vollständig deaktiviert oder gelöscht. Es konnte diagnostiziert werden, dass die Vorarbeiten von Dataport weniger Netzwerkverbindungen im Gegensatz zum letztjährigen Test zur Folge hatten. Es konnten jedoch dennoch einige Verbindungen beobachtet werden, die bei genauerer Inspektion auch personenbezogene, zumindest personenbeziehbare, Daten enthielten, die eine Installation von Windows individuell wiedererkennbar machen. Microsoft dokumentiert einige Verbindungen auf der eigenen Hilfe-Seite als erforderlich und weist darauf hin, dass ein manuelles Blockieren der Netzwerkverbindungen zu Instabilitäten des Systems führen könnte. Diese Instabilitäten konnte der HmbBfDI nach einer händischen Firewall-Blockade nicht feststellen und hat Dataport daher das Blockieren der besagten Verbindungen empfohlen. Der weiterhin verbleibende Datenverkehr nach diesen Anpassungen ist nach bisherigem Kenntnisstand frei von Benutzer- und Maschinentracking und teilweise für den sicheren Betrieb von Windows erforderlich.
Diese Tests von Windows 10 Enterprise sollen nach Aussage Dataports ein fester Bestandteil des Rollout-Prozesses in der FHH werden. Eine endgültige Aussage, wann diese Analysen in das dortige Qualitätsmanagement mit aufgenommen werden steht zum Redaktionsschluss noch aus. Aufgrund der halbjährlichen Aktualisierungen seitens Microsoft und dem dadurch mindestens jährlich erzwungenen Update auf die nächste Version innerhalb der FHH, bedarf es einer intensiven Kontrolle dieser potentiell verbleibenden Datenflüsse.

Der HmbBfDI stellte im gesamten Prozess der Einführung von Windows 10 in der FHH fest, dass die einseitige Abhängigkeit der öffentlichen Verwaltung von Microsoft-Produkten immer wieder in Situationen führt, in denen die Betreiber und Verantwortlichen zusätzliche Maßnahmen zum Schutz personenbezogener Daten ergreifen müssen, da der Hersteller dies ansonsten nicht beabsichtigt. Der HmbBfDI befürwortet daher weiterhin jeden Versuch, diese Abhängigkeiten zu durchbrechen und souveräner in der Wahl und Einsatz von Software zu werden (siehe dazu auch III 4 Digitale Souveränität).

10. Datenpanne eines Kreditinstituts

Bei meldepflichtigen Datenpannen sind die Betroffenen stets zu informieren, wenn ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Je mehr Daten von einer Person von einer Datenpanne betroffen sind, desto wahrscheinlicher liegt ein hohes Risiko vor.

Artikel 33 Abs. 1 Datenschutz-Grundverordnung (DSGVO) sieht vor, dass im Falle einer Verletzung des Schutzes personenbezogener Daten der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nachdem ihm die Verletzung bekannt wurde, diese der gemäß Art. 55 zuständigen Aufsichtsbehörde meldet, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, sieht Artikel 34 Absatz 1 DSGVO zudem vor, dass der Verantwortliche die betroffene Person unverzüglich über die Verletzung benachrichtigt.

Sinn und Zweck dieser Vorschriften ist, dass mit den Pflichten aus Art. 33, 34 insbesondere Transparenz über stattgefundene Datenschutzverletzungen geschaffen werden und es den Datenschutzbehörden und betroffenen Personen erleichtert werden soll, aus der Datenschutzverletzung resultierende Folgeschäden zu vermeiden bzw. minimieren. Gemäß Erwägungsgrund (EG) 85 der DSGVO kann eine Verletzung des Schutzes personenbezogener Daten – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefug-

te Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile. Durch die Verpflichtung, die Datenschutzpanne nach außen transparent zu machen, soll die betroffene Person in die Lage versetzt werden, durch rechtzeitige und angemessene Reaktion Schaden von sich abzuwenden. Es soll ihr ermöglicht werden, die erforderlichen Vorkehrungen zu treffen (EG 86), also z.B. Passwörter zu ändern oder das Konto auf unbefugte Abbuchungen hin zu kontrollieren.

Häufig ist von keinem hohen Risiko auszugehen, wenn einzelne Daten für sich genommen von einer Datenpanne betroffen sind, wie z.B. nur die Grunddaten oder nur die Kontonummer der betroffenen Personen. Je mehr Daten aber von einer Person von einer Datenpanne betroffen sind, wie z.B. die Grunddaten, Geburtsdaten und Kontodaten, desto wahrscheinlicher liegt ein hohes Risiko vor. Dies wird bei dem nachfolgenden Fall deutlich.

Im Sommer 2018 meldete ein Kreditinstitut schriftlich einen Data Breach gem. Artikel 33 Absatz 1 DSGVO. Einige Tage später erreichte den HmbBfDI die Beschwerde einer Betroffenen, die mitteilte, dass sie bei einer zufälligen Recherche zu ihrem Namen im Internet auf ein unverschlüsseltes PDF-Dokument mit umfangreichen Angaben des Kreditinstituts zu Ihrem Konto und der Geschäftsverbindung gestoßen sei. Das Dokument sei über einen Link erreichbar und enthielte unter anderem Vorname, Nachname, Geburtsdatum, IBAN-Kontonummer, Adresse und Kassenart. Neben ihren eigenen Daten seien ähnliche Daten mehrerer Tausend weiterer Personen vorhanden. Nachdem die Betroffene den Vorfall noch am selben Tag dem Kreditinstitut meldete, wurde der Link, unter dem das Dokument abgerufen werden konnte, unverzüglich vom Netz genommen und war nicht mehr verfügbar.

Die Offenlegung der Grunddaten hätte in diesem Fall zwar zu einer Meldepflicht bei der Aufsichtsbehörde geführt, nicht jedoch zwingend eine Benachrichtigungspflicht gem. Art. 34 DSGVO gegenüber

der betroffenen Person. Grunddaten dürften in den allermeisten Fällen sogar einen geringeren Schutzbedarf haben, da sie oft entweder von den Betroffenen selbst frei verfügbar preisgegeben werden oder aber - sofern keine Meldesperre vorliegt - über eine einfache Melderegisterauskunft erhältlich sind. Erforderlich ist lediglich die Glaubhaftmachung des berechtigten Interesses wobei das "berechtigte Interesse" jedes als schutzwürdig anzuerkennende Interesse rechtlicher, wirtschaftlicher oder auch ideeller Art umfasst. Die Hürden sind daher nicht all zu hoch, um an die Grunddaten einer Person zu gelangen.

Anders hingegen sieht es aus, wenn neben den Grunddaten auch die Geburtsdaten und dazu auch die Kontodaten durch eine Datenpanne frei verfügbar sind. Diese Daten in der Kombination eignen sich z.B. optimal für einen Identitätsdiebstahl und für die Erstellung von Konten im Bereich des Online-Handels, die unter Umständen sogar zu einer positiven Abfrage bei Auskunfteien führen können. Ein naheliegendes Schadensrisiko ist hierbei also, dass Personen, die unberechtigt Kenntnis dieser Daten haben, versuchen können Waren zu bestellen oder direkt Geld abzubuchen. Die Offenlegung dieser Daten kann somit nicht nur zu einer hypothetischen Gefahr eines Identitätsdiebstahls, sondern auch zu einer Drohung eines finanziellen Verlustes führen.

Der HmbBfDI konnte dem Kreditinstitut das Vorliegen eines hohen Risikos erfolgreich darlegen, was dazu führte, dass die Betroffenen gem. Art. 34 DSGVO von der Datenpanne benachrichtigt wurden.

11. Webtracking im Online-Banking-Bereich und auf Hamburg.de

Banken und Sparkassen schrecken selbst im angemeldeten Online-Banking-Bereich nicht davor zurück, das Surfverhalten ihrer Kunden mit Tools wie Google Analytics zu erfassen und auszuwerten. Ebenso erfolgt ein massives Webtracking auf dem Stadtportal der Hansestadt Hamburg, auch unter Einsatz der Webanalyse von Google Analytics.

Der HmbBfDI hat im Berichtszeitraum vermehrt Beschwerden von Betroffenen über den Einsatz von Google Analytics sowohl auf den allgemein zugänglichen Webseiten der Banken und Sparkassen als auch im nur für Kunden nach Anmeldung zugänglichen Online-Banking-Bereich erhalten. Außerdem erhielt der HmbBfDI vermehrt Beschwerden von Betroffenen zum Stadtportal der Hansestadt Hamburg, das von Hamburg.de betrieben wird und ebenfalls den Dienst von Google Analytics einsetzt. Dies hat der HmbBfDI zum Anlass genommen, verschiedene Banken und Sparkassen sowie Hamburg.de aufzufordern, den rechtmäßigen Einsatz von Tracking-Tools nachzuweisen.

Aus den Datenschutzerklärungen der Geldhäuser sowie von Hamburg.de ließ sich nicht plausibel entnehmen, auf welche Erlaubnisnorm eine Datenverarbeitung im Rahmen des Einsatzes solcher Tracking-Tools gestützt wird. Zwar enthalten die Datenschutzerklärungen der verantwortlichen Unternehmen einen Hinweis auf ein berechtigtes Interesse nach Art. 6 Abs. 1 f) DGVO. Ein solches dürfte regelmäßig zwar vorliegen. Warum dieses Interesse allerdings den Schutz von Grundrechten und Grundfreiheiten betroffener Personen überwiegen soll, wie es für die Anwendung von Art. 6 Abs. 1 f) als Rechtsgrundlage erforderlich wäre, wird nicht deutlich. Der Hinweis auf das Anbieten einer nutzerfreundlichen und optimierten Webseite reicht für ein überwiegendes Interesse auf Seiten der Verantwortlichen Unternehmen nicht aus. Aus diesem Grund kann hier nur auf

die Einwilligung als Rechtsgrundlage zurückgegriffen werden (siehe auch V 4). Außerdem ergeben sich aus den Datenschutzhinweisen der Geldinstitute für die Betroffenen aus den Datenschutzerklärungen keine Hinweise darauf, dass der Einsatz von Google Analytics auch im eingeloggten Bereich erfolgt.

Bei einer überprüften Bank war der Datenschutzerklärung ein Anhaltspunkt zum Einsatz von Google Analytics überhaupt nicht zu entnehmen. Es erfolgte lediglich ein allgemeiner Hinweis im Rahmen eines eingesetzten Cookie-Banners, der wie folgt lautete:

> „Diese Website verwendet Cookies für Analysen, personalisierte Inhalte, Legitimationszwecke sowie aus Sicherheitsgründen. Durch einen Klick auf „OK" oder die weitere Nutzung dieser Webseite stimmen Sie der Verwendung von Cookies und Tracking-Tools zu. Die Verwendung von Cookies und Tracking-Tools können Sie hier deaktivieren."

Im letzten Satz war das Wort „hier" auf die Datenschutzhinweise des verantwortlichen Unternehmens verlinkt, die jedoch keinerlei Einstellungsmöglichkeiten vorhielten, mit denen Betroffene auf den Einsatz von Cookies einwirken konnten. Ohne explizite Zustimmung wurden bereits beim ersten Aufruf der Webseite Cookies von Google Analytics geladen. Eine auch unter Berücksichtigung der aktuellen europäischen Rechtsprechung (EuGH, Urteil v. 1.10.2019, Az: C-673/17 „Planet49") erforderliche Einwilligung der Betroffenen wurde nicht eingeholt.

Besonders problematisch ist dabei der Einsatz von Analyse-Tools im angemeldeten Online-Banking-Bereich. Nach Ansicht des HmbBfDI ist der Einsatz für die Betroffenen schon nicht von ihrem Erwartungshorizont gedeckt und wäre daher ggf. gesondert einwilligungsbedürftig. Die betroffenen Nutzer gehen vielmehr berechtigterweise davon aus, dass sie sich in einem geschützten Bereich befinden. Zum einen, weil sie sich explizit anmelden müssen, zum anderen, weil es sich bei Bankdaten um Daten handelt, die einen besonderen Vertrau-

ensschutz genießen. Die Sensibilität der Daten wird unterstrichen durch die kürzlich umgesetzte zweite EU-Zahlungsrichtlinie (PSD2), die durch technische Sicherheitsverschärfungen für mehr Sicherheit und Vertrauen im Online-Banking-Bereich sorgen soll. Hierzu zählt auch die sogenannte starke Kundenauthentisierung, wonach Kontozugriffe bzw. Finanzstatusanzeigen nur noch nach Eingabe von in Echtzeit generierten TAN-Nummern möglich sind.

Vor diesem Hintergrund werden betroffene Nutzer nicht erwarten, dass personenidentifizierbare Daten – erst recht nicht im Online-Banking-Bereich – erhoben und an ein amerikanisches Unternehmen auch zur Verfolgung von dessen eigenen Zwecken weitergeben werden, ohne dass hierfür eine explizite Einwilligung vorliegt.

Zudem war es auch auf mehrere Nachfragen des HmbBfDI hin, dem Stadtportal Hambrg.de nicht möglich, die näheren Umstände der Datenverarbeitung im Rahmen des Webtrackings darzulegen. Dies wäre jedoch Pflicht des Unternehmens im Rahmen des Art. 5 Abs. 2 DSGVO gewesen.

Die eingeleiteten aufsichtsrechtlichen Verfahren waren zum Redaktionsschluss noch nicht sämtlich abgeschlossen. Die Betreiber von Hamburg.de haben nach der Einleitung eines aufsichtsrechtlichen Verfahrens dahingehend Stellung genommen, dass Anpassungen im Bereich des Webtrackings, die datenschutzrechtliche Vorgaben berücksichtigen, vorgenommen werden sollen. Der HmbBfDI wird dies nachverfolgen und überprüfen.

12. AUFZEICHNUNG VON KUNDENGESPRÄCHEN IM BEREICH DER KREDITWIRTSCHAFT

Ein Erlaubnistatbestand ist bei Aufzeichnungen von Telefongesprächen auch in datenschutzrechtlicher Hinsicht erforderlich. Das betrifft sowohl die Beschäftigten als auch Kunden von Wertpapierdienstleistungsunternehmen.

Der HmbBfDI hat sich im Berichtszeitraum wiederholt der Frage gewidmet, ob und wann Aufzeichnungen von Kundengesprächen im Bereich der Kreditwirtschaft datenschutzrechtlich zulässig sind. Hintergrund hierfür waren Beschwerden von Betroffenen, die in der Servicehotline von einem Kreditunternehmen nicht bedient wurden, weil Sie die Einwilligung zur Telefonaufzeichnung nicht erteilten.

Das Aufzeichnen und Abhören von Telefongesprächen, soweit dies unbefugt ist, stellt eine Straftat im Sinne des § 201 Abs. 1 StGB dar. Vor diesem Hintergrund ist ein Erlaubnistatbestand bei Aufzeichnungen von Telefongesprächen auch in datenschutzrechtlicher Hinsicht erforderlich. Das betrifft sowohl die Beschäftigten als auch Kunden von Wertpapierdienstleistungsunternehmen.

Mit der Aufzeichnung von Telefongesprächen hatte sich noch vor Anwendbarkeit der DSGVO auch die die Datenschutzkonferenz (DSK) beschäftigt und beschlossen, dass die Aufzeichnung von Telefongesprächen datenschutzrechtlich in aller Regel nur mit Einwilligung im Sinne der DSGVO zulässig ist (Beschluss der DSK vom 23.03.2018 „Aufzeichnung von Telefongesprächen“, abzurufen unter https://www.datenschutzkonferenz-online.de/media/dskb/20180323_dskb_aufzeichnung_telefon.pdf).

Dieser Auffassung ist grundsätzlich zuzustimmen, wobei im Bereich der Kreditwirtschaft gemäß § 83 Abs. 3 Wertpapierhandelsgesetz (WpHG) auch eine Pflicht zur Telefonaufzeichnung bestehen kann und

somit keine Einwilligung der Betroffenen erforderlich ist. Zu differenzieren ist daher, ob die Aufzeichnung im Zusammenhang mit Wertpapierdienstleistungen erfolgt oder aber dann, wenn sich die Kunden bei Servicehotlines melden, weil sie sonstige Dienstleistungen wahrnehmen möchten, wie z.B. welche Unterlagen für einen Kreditantrag benötigt werden. Danach richten sich auch die Anforderungen an die Telefonaufzeichnung.

§ 83 Abs. 5 WpHG sieht beispielsweise vor, dass im Zusammenhang mit Wertpapierprodukten das Wertpapierdienstleistungsunternehmen die betroffene Person vorab in geeigneter Weise über die Aufzeichnung von Telefongesprächen zu informieren hat. Erfolgt dies nicht oder hat die betroffene Person einer Aufzeichnung widersprochen, darf das Wertpapierdienstleistungsunternehmen keine telefonisch veranlassten Wertpapierdienstleistungen erbringen, wenn sich diese auf die Annahme, Übermittlung und Ausführung von Kundenaufträgen beziehen. In beiden Fällen darf das Gespräch folglich abgebrochen werden, ohne dass dies datenschutzrechtlich zu beanstanden ist.

Die Telefonaufzeichnung im Kundensupport bzw. einer Servicehotline hingegen erfolgt in der Regel zur Qualitätskontrolle/-sicherung oder aber zu Dokumentations- und Schulungszwecken. Eine Pflicht zur Aufzeichnung besteht demnach nicht, so dass die Aufzeichnung ausschließlich auf Grundlage des Art. 6 Abs. 1 lit. a DSGVO durch Einholung einer Einwilligung der betroffenen Person in die Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke erfolgen kann.

Eine „Einwilligung" der betroffenen Person i.S.d. Art. 6 Abs. 1 lit. a DSGVO wird gem. Art. 4 Nr. 11 DSGVO definiert als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

Freiwilligkeit nach Erwägungsgrund (EG) 42 der DSGVO setzt voraus, dass die betroffene Person „eine echte oder freie Wahl haben“ und somit in der Lage sein muss, „die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“. Keine Nachteile entstehen, wenn der betroffenen Person eine anderweitige praktikablere Kontaktmöglichkeit, z.B. per Post oder E-Mail, aufgezeigt wird. Zu beachten sind ferner die übrigen Bedingungen für die Einwilligung gem. Art. 7 DSGVO. Die Schriftform ist nicht erforderlich; ausreichend ist vielmehr eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung, durch die die betroffene Person ihr Einverständnis zur Datenverarbeitung unmissverständlich erteilt. Aus EG 32 der DSGVO ist ersichtlich, dass Stillschweigen oder Untätigkeit der betroffenen Person keine Einwilligung darstellen. Ebenso wenig gilt dies nach Auffassung des Europäischen Datenschutzausschusses für die einfache Weiternutzung eines Services. Für die Erteilung von Einwilligungen ist vielmehr ein aktives Verhalten der betroffenen Person erforderlich.

Die betroffene Person kann die erteilte Einwilligung natürlich auch während des Telefongesprächs jederzeit und ohne Angabe von Gründen widerrufen (Art. 7 Abs. 3 DSGVO). Die bisherige Aufzeichnung bzw. das Mithören muss dann umgehend beendet werden. Auf die Möglichkeit eines Widerrufs ist die betroffene Person vor Abgabe der Einwilligung in Kenntnis zu setzen (Art. 7 Abs. 3 S. 2 DSGVO). Konsequenz einer widerrufenen Einwilligung ist nach geltendem Datenschutzrecht die Unzulässigkeit der weiteren Datenverarbeitung für die Zukunft (sog. Ex-nunc-Wirkung). Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung wird hingegen durch den Widerruf nicht berührt. Zu einer gewissen Ex-tunc-Wirkung (rückwirkenden Wirkung) des Widerrufs kommt es aber gleichwohl, weil die betroffene Person im Falle des Widerrufs gem. Art. 17 Abs. 1 lit. b das Recht hat, von dem für die Verarbeitung Verantwortlichen die Löschung der sie betreffenden Daten zu verlangen, und der für die Verarbeitung Verantwortliche verpflichtet ist, diese Daten ohne unangemessene Verzögerung zu löschen.

Eine Löschung ist jedoch ausgeschlossen, wenn die Speicherung der Telefonaufzeichnung auf eine andere Rechtsgrundlage gestützt werden kann. Eine solche ist im Falle einer Telefonaufzeichnung im Kundensupport zur Qualitätskontrolle/-sicherung oder aber zu Schulungszwecken jedoch nicht ersichtlich.

Beschäftigte von Wertpapierdienstleistungsunternehmen unterliegen denselben rechtlichen Anforderungen wie die Kunden. Da die notwendige Freiwilligkeit der Einwilligung aufgrund der wirtschaftlichen Abhängigkeit der Beschäftigten im Arbeitsverhältnis (sog. Über- / Unterordnungsverhältnis) nur schwierig sichergestellt werden kann, ist idealerweise eine Betriebsvereinbarung zu schließen, die Telefonaufzeichnungen regelt.

Der HmbBfDI hatte aufgrund der Beschwerden mehrere Testanrufe zu verschiedenen Zeiten vorgenommen, konnte jedoch keine Verstöße feststellen. Auch wenn nicht gänzlich ausgeschlossen werden kann, dass die Betroffenen mangels Einwilligung nicht beraten wurden, konnte dies nicht nachgewiesen werden. Hierüber wurden die Betroffenen informiert.

13. BODYCAM IM PRIVATEN BEREICH

Der Einsatz einer Bodycam auf der Großen Freiheit erfolgt durch Intervention des HmbBfDI nun datenschutzkonform.

Private Sicherheitsdienste setzen zunehmend auf den Einsatz von Bodycams um Beschäftigte vor Übergriffen zu schützen oder Beweismittel für zivilrechtliche Ansprüche zu beschaffen. Videokameras, auf der Schulter oder an der Brust befestigt, sollen abschrecken oder deeskalierend wirken. Aus Betroffenensicht ist dabei jedoch problematisch, dass die Geräte nicht auf einzelne Kamerawinkel beschränkt sind, so dass die Umgebung umfangreich erfasst wird. Indem beispielsweise direkt in Gesichter gefilmt wird, wird stark in

die Rechte der Betroffenen eingegriffen. Jeder Bürger hat das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne das sein Verhalten mit einer Kamera beobachtet und aufgezeichnet wird. Deshalb greift das Aufzeichnen von Bild und Ton mittels einer Bodycam in das Grundrecht auf informationelle Selbstbestimmung ein und ist nur im begründeten Ausnahmefall anlassbezogen denkbar.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) erhielt Hinweise auf einen solchen Sicherheitsdienst mit Bodycam mit dem Vorhalt, die Kamera nicht anlassbezogen, sondern permanent einzuschalten. Aufgrund dieser Hinweise nahm der HmbBfDI eine Vor-Ort-Prüfung in der Großen Freiheit während der Öffnungszeiten des betreffenden Tanzlokals vor. Dabei zeigte sich, dass die Kamera während des Observationszeitraums durchgehend ausgeschaltet war. Im anschließenden Gespräch wurde der Türsteher zu seiner Nutzungspraxis befragt und das Gerät in Augenschein genommen. Es zeigte sich, dass sich der Türsteher zuvor mit dem datenschutzgerechten Einsatz von Bodycams auf den Internetseiten und mit der von den Aufsichtsbehörden zur Verfügung gestellten Orientierungshilfe vertraut gemacht hatte (https://www.datenschutzkonferenz-online.de/media/oh/20190222_oh_bodycams.pdf). Nach den Feststellungen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) erfolgt eine Aufnahme nur punktuell, wenn eine konkrete Situation zu eskalieren droht. Vor dem Einschalten der Bodycam werden die Betroffenen auf die Aufnahme hingewiesen. Aktiviert wird die Aufnahme vom Türsteher nur, wenn die Situation durch den Hinweis noch nicht entschärft werden kann. Dabei zeigt ein optisches Signal („rote Lampe“) an, dass die Bodycam Daten erhebt. Im Falle von Aufnahmen werden diese nach Schichtende auf der nahegelegenen Davidwache zur Strafverfolgung übergeben.

Darüber hinaus wurde jedoch festgestellt, dass die Bodycam über eine unzulässige Funktion zur Anfertigung von Tonaufzeichnungen verfügt, die bisher nicht deaktiviert worden war.

Aufgrund der Intervention des HmbBfDI ist die Funktion zur Anfertigung von Tonaufzeichnungen mittlerweile technisch dauerhaft deaktiviert worden. Außerdem verwendet der Verantwortliche jetzt ergänzend zu der schon bestehenden Kennzeichnung an seiner Kleidung (Aufnäher mit Piktogramm einer Videokamera und Schriftzug Videoüberwachung) Informationsblätter, die den Betroffenen bei Bedarf ausgehändigt werden, um so den datenschutzrechtlichen Transparenzpflichten umfänglich zu genügen.

14. FACEBOOK MESSENGER UND „BE ON LOOKOUT"-LISTE

Seit den Vorfällen rund um Cambridge Analytica häuften sich zahlreiche Medienberichte zu erheblich bedenklichen Verarbeitungsvorgängen bei Facebook, die Anlass zur Sorge um deren Rechtmäßigkeit bieten.

Anfang des Jahres haben einige US-amerikanische Medien über die sogenannte „be on lookout"-Liste berichtet und damit den HmbBfDI veranlasst, dem Sachverhalt in eigener Zuständigkeit im Hinblick auf mögliche Betroffene in Deutschland nachzugehen. Den Berichten zufolge führt Facebook unter dem Begriff "be on lookout" (kurz „BOLO") eine Liste mit Daten zu Personen, die der Konzern als Sicherheitsrisiko für die Facebook-Mitarbeiter oder -Einrichtungen betrachtet.

In diesem Zusammenhang wurden die Facebook Inc. und die Facebook Germany GmbH vom HmbBfDI informatorisch befragt. Beide Unternehmen bestätigten die Existenz der BOLO-Liste, beantworteten jeweils die Fragen des HmbBfDI und übersandten je eine Liste mit Personen, die für den Standort Deutschland relevant seien. In ihren Antwortschreiben gaben beide an, dass die Facebook Inc. mit Hilfe ihres Security-Teams global für die gesamte Facebook-Gruppe agie-

re und eine umfassende BOLO-Liste für Facebook-Niederlassungen weltweit führe. Die jeweilige Facebook-Niederlassung erhält dabei den Lesezugriff auf solche Daten, die ihre Niederlassung betreffen, so auch die Facebook Germany GmbH. Die in diesem Zusammenhang möglicherweise bestehenden datenschutzrechtlichen Probleme, etwa in Hinblick auf die Information der Betroffenen sowie die Rechtslage für Erhebung und Weitergabe der Daten an den Mutterkonzern, die Facebook Inc., sind zum Redaktionsschluss noch Gegenstand laufender Verfahren.

Des Weiteren nahm der HmbBfDI etwa zeitgleich nach dem Bekanntwerden der unerlaubten Transkription bei zahlreichen Anbietern von Sprachassistenzsystemen (siehe II 17) Ermittlungen gegen Facebook auf, da nach Medienberichten bei der Nutzung des Facebook-Messengers aufgezeichnete und transkribierte Sprachmitschnitte von Mitarbeitern angehört und zur Qualitätskontrolle und –verbesserung individuell transkribiert wurden.

Der Facebook-Messenger-Dienst ermöglichte den Nutzern in den USA eine erhaltene Audionachricht in eine entsprechende Textnachricht umzuwandeln. Dieses Feature steht den europäischen Nutzern nicht zur Verfügung. Die Nutzer in den USA wurden darauf hingewiesen, dass auch bei persönlicher Deaktivierung dieses Features bei dem jeweiligen Empfänger einer eigenen Audionachricht eine Text-Umwandlung stattfinden könne, wenn jener diese Funktion nicht ebenfalls deaktiviert hat.

Nach anfänglicher Klärung der Zuständigkeitsfragen mit der irischen Aufsichtsbehörde IDPC erklärte die Facebook Ireland Ltd., für dieses Feature nicht verantwortlich zu sein.

Die Facebook Inc. teilte dem HmbBfDI mit, dieses Feature nur in bestimmten Ländern außerhalb der EU angeboten zu haben. Dabei ist der Umstand nicht berücksichtigt worden, dass Audionachrichten europäischer Nutzer, die an US-Nutzer versandt wurden, ebenfalls Gegenstand der Transkription und damit auch der Qualitäts-

kontrolle werden konnten. Das Unternehmen stellte für den gesamten EU-Raum eine Liste mit Betroffenen in den jeweiligen Mitgliedsstaaten auf. In Deutschland waren den Angaben von Facebook zufolge insgesamt 5 Personen von der Transkription ihrer Audionachrichten betroffen. Die Facebook Inc. vertritt im Übrigen die Auffassung, nicht unter die Anwendung der DSGVO zu fallen.

Die informatorische Befragung der Facebook Inc. zum Messenger wurde im Rahmen des Austauschs in den Fachgremien des EDSA von anderen europäischen Aufsichtsbehörden zum Anlass genommen, ebenfalls an die Facebook Inc. heranzutreten. Nach der Auswertung der Ergebnisse der Befragung ist eine koordinierte Vorgehensweise der europäischen Aufsichtsbehörden geplant.

15. TRACKING AUF MOBILEN ENDGERÄTEN

Eine Häufung an Beschwerden über vermeintliches Tracking durch die Mikrofone von Smartphones oder digitalen Assistenten führt zur Einführung neuer Methoden beim HmbBfDI.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit nimmt in den letzten Jahren eine Häufung an Beschwerden über eine angebliche Auswertung des gesprochenen Wortes durch im Raum oder in der Nähe befindliche Mobiltelefone wahr. Auch in der Presse wird immer wieder von derartigen oder ähnlich gearteten Fällen berichtet.

Betroffene Personen geben an, dass Werbung, die sie im Internet sehen oder direkt als persönliche Werbung per E-Mail erhalten, Bezug auf Inhalte aus persönlichen Gesprächen nimmt, etwa in Hinblick auf dabei genannte Produkte oder Themenfelder.

Um diesen Fällen nachgehen zu können, hat der HmbBfDI Anfang 2019 ein Labor eingerichtet, in dem konkrete Verdachtsfälle nachgestellt und das Verhalten von Apps analysiert werden kann. Dieses Labor kommt seither auch immer häufiger in der Bearbeitung von anderen Beschwerden über Apps und der Beantwortung von Presseanfragen zum Einsatz.

Der HmbBfDI ist dadurch in der Lage, mobile Apps nicht nur aus der Perspektive der Nutzenden zu beurteilen, sondern die Kommunikation in einem Laboraufbau zu analysieren. Es kann festgestellt werden, mit welchen Dritten welche Informationen geteilt werden und, abhängig von der App, auch die Datenverarbeitung auf dem Gerät betrachtet werden. Durch eigene Entwicklungen kann außerdem die Nutzung von Systemressourcen oder das Verhalten von 3rd-Party Bibliotheken überwacht und analysiert werden. Mit den hier angewandten Methoden werden auch digitale Assistenten (siehe auch II 16) evaluiert, die jedoch aufgrund ihrer geschlossenen Plattform weniger Einblicke in ihre inneren Abläufe zulassen.

Im Rahmen mehrerer kurzer Projektsprints hat der HmbBfDI eine Liste von Apps innerhalb der eigenen Zuständigkeit auf Auffälligkeiten hin überprüft und nach Anzeichen für eine Übertragung von Audioinhalten ins Internet gesucht.

Bislang konnte weder im Rahmen keiner Beschwerde noch in den Projektsprints ein Fall von unautorisierter Nutzung eines Gerätemikrofons nachgewiesen werden. Der HmbBfDI bleibt weiter an diesem Thema dran und wird seine Fähigkeiten in diesem Bereich weiter ausbauen.

16. SPRACHASSISTENTEN

Digitale Sprachassistenten finden zunehmend Verbreitung. Nutzer gehen hierbei zahlreiche Risiken ein, denn die Zahl von Problemen und Missbräuchen steigt.

Bereits im 26. Tätigkeitsbericht hat der HmbBfDI die Nutzung digitaler Sprachassistenten kritisch beleuchtet (vgl. 26. TB, III 6). Seither haben sich derartige Geräte bzw. Dienste bei Bürgern und Verbrauchern weiter verbreitet und etabliert.
In immer mehr Wohnungen, Büros, Kraftfahrzeugen und neuerdings auch Hotels (siehe https://www.amazon.com/alexahospitality) befinden sich Geräte, die permanent alle Geräusche erfassen und nach Erkennen von Aktivierungsworten wie „Hey Alexa" oder „OK Google" die akustischen Signale über das Internet an die Server ihrer Anbieter übermitteln. Dort erfolgt dann die eigentliche Sprach- und Befehlserkennung und das Ergebnis eines Befehls oder einer Suchanfrage wird an das Gerät zurückgeschickt.

Die Nutzung solcher Angebote hat Risiken für die Privatsphäre der Betroffenen. Dies sind nicht nur diejenigen Personen, die den Sprachassistenten betreiben, sondern potentiell alle, die sich in den entsprechenden Räumen aufhalten und deren Stimmen erfasst werden. Beispielweise Familienmitglieder, Mitbewohner, Arbeitskollegen oder Besucher. Auch ist nicht ausgeschlossen, dass Gerätebetreiber wirtschaftlichen Schaden erleiden. Denn wird ein Gerät Ziel von Missbrauch durch Dritte, können diese u.U. nicht autorisierte Online-Einkäufe auf Kosten des Gerätebesitzers tätigen oder vernetzte Türschlösser, Garagentore oder Rollläden öffnen, um leichteren Zugang für Einbruch und Diebstahl zu erlangen.

Zur unberechtigten Nutzung eines Sprachassistenten muss ein Angreifer sich nicht einmal im gleichen Raum aufhalten. So können Befehle z.B. durch eine geschlossene Wohnungstür gerufen oder per Anruf an einen im Raum stehenden Anrufbeantworter übermittelt

werden. Ein erstaunliches Angriffsszenario publizierten Forscher im November 2019. Ihnen war es gelungen, Geräte alleine mit Laserstahlen zur Ausführung von Befehlen zu bringen, sogar auf Distanzen über 100 Meter (siehe https://lightcommands.com). Sie nutzten dabei den Umstand aus, dass bei den Mikrofonen der Sprachassistenten durch „Beschuss" mit Laserstrahlung in unterschiedlicher Intensität unhörbare akustische Befehle ausgelöst werden können. Damit kann die unberechtigte Nutzung eines Gerätes sogar durch das Fenster von einem benachbarten Gebäude aus durchgeführt werden.

Neben den Risiken durch Dritte offenbarten sich im Juli 2019 auch Probleme bei den Anbietern der Sprachassistenzdienste selbst, konkret beim Umgang mit den erhobenen Nutzerdaten. Über Mitschnitte, die ein Whistleblower einem belgischen Mediennetzwerk zugespielt hatte, wurde publik, dass Google die Spracherkennung keineswegs nur maschinell vornimmt, sondern einen gewissen Anteil der Audioaufnahmen von Menschen auswerten lässt, um die Spracherkennungsfähigkeit des Google Assistant zu optimieren. Hierbei hören Mitarbeiter von Google bzw. von beauftragten Firmen die Aufzeichnungen ab und transkribieren diese, um bewerten zu können, ob die aufgenommenen akustischen Informationen von dem automatisierten Spracherkennungssystem korrekt verarbeitet wurden. Den Mitschnitten des Whistleblowers ließen sich zum Teil sensible personenbezogene Informationen aus der Privat- und Intimsphäre der Betroffenen durch die von Google beauftragten Mitarbeiter entnehmen. Des Weiteren zeigte sich, dass ein nicht unerheblicher Teil der Aufnahmen aufgrund fehlerhafter Aktivierung erfolgte.

Der HmbBfDI hat daraufhin ein Verwaltungsverfahren gegen Google eröffnet und Auswertungen durch Mitarbeiter oder Dritte für den Zeitraum von drei Monaten untersagt. Dem ist das Unternehmen auch nachgekommen. Eine Wiederaufnahme der bisherigen Auswertungspraxis beim Google Assistant ist aus Sicht des HmbBfDI nur zulässig, wenn für die Speicherung der Audioaufnahmen eine aktive Einwilligung (Opt-in) der Nutzer eingeholt wird. Zusätzlich müssen

diese über das Risiko von Fehlauslösungen und unbemerkte Aufzeichnungen aufgeklärt werden.

Um für Dienste im Bereich Sprachassistenz und -steuerung europaweit Klarheit zu schaffen, hat der Europäische Datenschutzausschuss (EDSA bzw. EDPB, European Data Protection Board) vereinbart, Leitlinien zu erarbeiten, die aufzeigen sollen, welche Datenverarbeitungsprozesse zulässig sind, welche Anforderungen hierfür bestehen und wie die Verantwortlichkeiten zu regeln sind. Der HmbBfDI wird sich an der Erarbeitung dieser Leitlinien beteiligen.

BERICHTE III.

1. Bromium

Die Einführung einer Lösung zum sicheren Browsen im Internet geht auf die Zielgerade.

Eines der größten Einfallstore für Schadsoftware bei Endgeräten sind Internet-Browser. Wie im 27. Tätigkeitsbericht unter Ziffer III.4.berichtet, begegnete die Stadt Hamburg diesem potentiellen Risiko bisher an Arbeitsplätzen mit hohem Schutzbedarf mit einem sogenannten Windows-Terminalserver (WTS). Dieser WTS sorgt dafür, dass lediglich ein Videostream des Browserfensters auf dem lokalen Computer des Anwenders angezeigt wird. Der eigentliche Prozess läuft auf abgesicherten Servern im Rechenzentrum des IT-Dienstleisters Dataport. Dieser Umstand bringt Vorteile, aber auch diverse Nachteile mit sich. Vorteile auf Anwenderseite sind insbesondere die Möglichkeit, sämtlichen Netzwerkverkehr über diese WTS zu leiten und den lokalen Computer strikt vom öffentlichen Netz zu trennen. Die wesentlichen Nachteile lagen in der geringeren Leistungsfähigkeit und im fehlenden Komfort beim Datentransfer dieser Lösung. So konnten in Spitzenlastzeiten die Reaktionszeiten des WTS erhebliche Ausmaße annehmen; teilweise waren die Server auch vollständig unerreichbar. Ferner gab es Einschränkungen in Bezug auf heruntergeladene oder hochzuladende Dateien, die erst mit Ablage in Netzlaufwerken für den WTS nutzbar waren.

Um eine zeitgemäße Lösung für die Anwendung des sicheren Browsens zu finden, führte die Senatskanzlei nach intensiver Erörterung mit dem HmbBfDI und einzelnen Behörden, u.a. der Polizei Hamburg, gemeinsam mit Dataport eine öffentliche Ausschreibung für eine Alternative zu WTS durch. In dieser Ausschreibung setzte sich die Bromium Secure Platform (Bromium) durch. Die ersten Tests mit Bromium wurden bereits vor der Ausschreibung Anfang 2018 vom HmbBfDI mitbegleitet und zeigten, dass die Software grundsätzlich als Ablösung des WTS geeignet ist. Technisch ist Bromium eine Hardware-isolierte Micro-Virtualisierung (Micro-VM). Diese Micro-VM sorgen dafür, dass alle riskanten Anwenderaktivitäten, dies sind

in der Regel alle Daten aus fremden Quellen, gekapselt und isoliert werden. Jeder Browser und jede einzelne Webseite wird in einer eigenen Micro-VM ausgeführt. Dadurch kann sich Schadsoftware höchstens innerhalb dieser Micro-VM ausbreiten und den Computer selbst nicht befallen. Nach Beendigung der jeweiligen Aktivität wird die Micro-VM gelöscht; mitsamt der Schadsoftware. Das Endgerät und das Behördennetz sind somit weiterhin sicher.

Neben Lösungen zum sicheren Browsen bietet Bromium zusätzlich an, E-Mail-Anwendungen und einige gängige Standardsoftware zu virtualisieren. Die Risiken durch weiter Angriffsvektoren könnten so deutlich reduziert werden. Dieser zusätzliche Schutz des Endgeräts wird auf absehbare Zeit nach Aussagen der Senatskanzlei (SK) nicht in der FHH zur Verfügung stehen. Demgegenüber fordert der HmbBfDI seit Beginn der ersten Tests die Einführung Bromiums in der Stadt Hamburg nicht nur auf das Browsen im Internet zu beschränken. Ein ganzheitlicher Schutz der Endgeräte kann nur gewährleistet werden, wenn sämtliche potentielle Schwachstellen der Systeme betrachtet werden. Erfahrungsgemäß liegt das Hauptaugenmerk von Angreifern dabei auch im Mailverkehr. Phishing-Versuche und automatisch ausführbare Scripte in Office-Macros beginnen für die Betroffenen häufig im Mail-Client und breiten sich dann über die Office-Software des Anwenders auf den Systemen aus. Daher sieht der HmbBfDI den Bedarf der Virtualisierung sämtlicher Software innerhalb der gesamten FHH und insbesondere in Bereichen, in denen ein hoher Schutzbedarf herrscht. Angriffe über Office-Macros würden gekapselt im jeweiligen Dokument versanden; das Endgerät selbst wäre nicht betroffen. Bromium bietet diese Lösungen von Haus aus an. Leider erfolgte die bisherige Lizenzbeschaffung lediglich für die Komponente des sicheren Browsens und steht der FHH daher nicht einmal optional für einzelne Behörden und Ämter zur Verfügung. Der HmbBfDI wird die Forderung nach einer vollständigen virtualisierten Umgebung weiter aufrechterhalten zumal auch eine aktuelle Studie des Bundesamtes für Informationssicherheit (BSI) diese Auffassung mit Nachdruck stärkt. Diese Studie bestätigt auch die Auffassung des HmbBfDI, dass Bromium an allen Arbeitsplätzen der Verwaltung

mit Internetzugang eingesetzt werden sollte. Das Roll-out zunächst nur auf Arbeitsplätze zu beschränken, an denen sehr sensible personenbezogene Daten mit hohem Schutzbedarf verarbeitet werden, kann aus Sicht des HmbBfDI nur ein erster Zwischenschritt sein.

Ein weiterer Aspekt, der auch im Zuge der Einführung von Bromium festzustellen ist, liegt darin, dass gemäß Art. 35 DSGVO „der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge" durchführen muss, sofern die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Da in der FHH das Browsen auch für private Zwecke gestattet ist und da eine umfangreiche Auswertung der besuchten Webseiten mittels Analyse der Protokolle vom Bromium durchgeführt werden könnte, nimmt die SK folgerichtig ein hohes Risiko an. Die deshalb notwendige Datenschutzfolgenabschätzung wurde im Zuge der Einführung Bromiums beim HmbBfDI von der SK angefordert. Leider musste der HmbBfDI feststellen, dass weder die SK noch Dataport diese Dokumentation zum Zeitpunkt der Anfrage unmittelbar mitteilen konnte, obwohl der Roll-Out-Prozess bereits schon weit fortgeschritten war. Vielmehr startete mit der ersten Nachfrage ein Prozess, in dem der HmbBfDI mehrmals die Anforderungen nach Art. 35 DSGVO aufzeigte und die SK diese erst mit Verspätung aufgriff. Der geschilderte Prozess dauert seit März 2019 an und scheint mit Redaktionsschluss ein Ende zu finden, nachdem nochmals die konkreten Anforderungen kommuniziert wurden. Der HmbBfDI wartet bis zum Vorliegen dieser Dokumentation die Einführung Bromiums ab; obgleich aus technischer Sicht zum aktuellen Stand keine Bedenken gegen diese Lösung existieren. Der HmbBfDI fordert, dass die SK ihrer Rolle als zuständige Behörde für die Bereitstellung einer datenschutzgerechten Infrastruktur für die Verwaltung gerecht wird.

2. Sichere Kommunikation der Jugendämter und externen Stellen

Kommunikation der Jugendämter mit externen Stellen weiterhin unverschlüsselt.

Die Kommunikation zwischen Allgemeinem Sozialen Dienst (ASD) und den externen Stellen läuft weiterhin ohne Inhaltsverschlüsselung der teilweise hochsensiblen Daten der betreuten Kinder und Jugendlichen. Obwohl die zuständige Behörde für Arbeit, Soziales, Familie und Integration (BASFI) bereits Ende 2018 im Unterausschuss „Datenschutz und Informationsfreiheit" zusicherte, dass die notwendigen Änderungen in der Kommunikation per Mail nach einer „Pilotierung im Januar (Anm. 2019) flächendeckend umgesetzt" werden, hat bis zum Redaktionsschluss dieses Berichts noch keine Anpassung stattgefunden. Der Workshop zur Erprobung notwendiger technischen Anpassungen fand im Januar 2019 statt und wurde mit Nutzerinnen und Nutzern in den Bezirken erfolgreich durchgeführt, allerdings blieb es nach unserer Kenntnis bei diesem einmaligen Pilotbetrieb.

Trotz wiederholter Nachfragen und kontinuierlichen Bemühungen um eine konstruktive Zusammenarbeit liegen dem HmbBfDI bis dato keine verbindlichen Aussagen über den Stand der Projektierung und Einführung des sog. Governikus MultiMessenger (GMM) vor. Angesichts der auch von der BASFI grundsätzlich nicht bestrittenen Datenschutzwidrigkeit einer generell unverschlüsselten E-Mail-Kommunikation des ASD mit externen Stellen kommt der HmbBfDI daher zu dem unbefriedigenden Ergebnis, dass die verantwortliche Stelle die Vertraulichkeit sensibler Sozialdaten, insbesondere von Kindern, über einen längeren Zeitraum nicht ausreichend abgesichert hat, obwohl die rechtliche Erforderlichkeit bekannt war.

Dieser Umstand ist auch unter dem Gesichtspunkt bedenklich, dass die Senatskanzlei (SK) eine nutzbare Lösung für solche Bedarfe

anbietet. Wie im 27. Tätigkeitsbericht in Kapitel III 3 geschildert, werden dadurch alle gängigen Standards zur Inhaltsverschlüsselung angenommen und diese auf einem sicheren Kanal weitergeleitet. Der umgekehrte Weg zu den Trägern erfolgt ebenfalls ab dem GMM Ende-zu-Ende-verschlüsselt. Bereits Ende 2018 hat der HmbBfDI gemeinsam mit der BASFI diesen Lösungsweg abgestimmt, ohne dass sich an der unbefriedigenden Situation etwas geändert hätte.

Aufgrund der Untätigkeit der BASFI hat der HmbBfDI am 06.12.2019 die Behördenleitung aufgefordert, kurzfristig einen belastbaren Zeitplan für die Umsetzung der für einen datenschutzkonformen Betrieb erforderlichen technischen Maßnahmen vorzulegen. Bis zum Redaktionsschluss dieses Berichts hat der HmbBfDI hierauf noch keine schriftliche Antwort erhalten. Vor dem Hintergrund der möglichen aufsichtsbehördlichen Abhilfemaßnahmen konnte allerdings vor Redaktionsschluss für Mitte Januar ein Gespräch des HmbBfDI mit der Behördenleitung der BASFI vereinbart werden. Der HmbBfDI wird sich weiter dafür einsetzen, dass eine flächendeckende Nutzung schnellstmöglich erfolgt.

3. DIGITAL FIRST: CHANCEN NUTZEN UND GLEICHZEITIG RISIKEN ERKENNEN UND BEGRENZEN

Datenschutz-Folgenabschätzungen müssen rechtzeitig erstellt und von den Verantwortlichen genutzt werden, um Risiken transparent zu machen und um diese in ausreichendem Maße zu begrenzen.

Mit dem Programm Digital First verfolgt Hamburg das Ziel, Prozesse in der Verwaltung vom Nutzer aus neu zu denken, und zwar vollständig: Von der verständlichen Benutzeroberfläche bis hin zu den dahinter liegenden Verwaltungsabläufen soll der gesamte Prozess

digital neu gestaltet werden. Dabei werden vier Leitlinien verfolgt: (1) Die Kommunikation mit der Verwaltung erfolgt vorrangig digital. (2) Proaktives Verwaltungshandeln soll Dienstleistungen ohne Antrags- oder sonstige Mitwirkungserfordernisse ermöglichen. (3) Eine weitgehende Automatisierung soll darüber hinaus die Mitarbeiterinnen und Mitarbeiter entlasten und die Effizienz der Verwaltung stärken. (4) Durch die Reduzierung von Dateneingaben sollen die Kunden der Verwaltung Informationen, die sie in einem Kontakt mit Behörden bereits angegeben haben, bei einem weiteren Verfahren nicht erneut angeben müssen (Once-Only-Prinzip). Der HmbBfDI hat in den beiden vorangegangenen Tätigkeitsberichten über dieses Programm bereits berichtet (vgl. 26. TB, V 2.2 und 27. TB, V 1.).

Keine Wartezeiten mehr im Kundenzentrum, nicht immer wieder dieselben Daten angeben müssen, die Prüfung auf Vollständigkeit der Unterlagen gleich bei der Antragstellung, nicht mehr begrenzte Öffnungszeiten beachten müssen und eine schnelle Reaktion der Verwaltung sind nur einige Beispiele, wie Bürgerinnen und Bürger durch Online-Zugänge zur Verwaltung profitieren können. Das sind lohnenswerte benutzungsorientierte Ziele.

Gerade wenn Verwaltungsprozesse so radikal neu gedacht werden sollen, ist es wichtig, dass bereits im Planungsprozess insbesondere bei der Verarbeitung sensibler personenbezogener Daten die Vertraulichkeit und Integrität gewährleistet wird.

Zu berücksichtigen ist auch, dass bestimmte, die Betroffenen einbeziehenden Verfahrensschritte des analogen Verfahrens in der digitalen Welt durch automatisierte Prozesse substituiert werden können, die ohne Beteiligung des Betroffenen stattfinden. Während beispielsweise zum Nachweis einer Hamburger Meldeanschrift bei Antragstellung vor Ort der Personalausweis vorgelegt werden kann, besteht im digitalen Verfahren die Möglichkeit, die Anschriften aller Bürgerinnen und Bürger automatisiert im Zentralen Meldebestand abzufragen. Dies soll für die Optimierung des Verfahrens zur Kita-Inanspruchnahme genutzt werden: Dort erfolgt bisher die

Prüfung der Meldeanschrift als Voraussetzung der örtlichen Zuständigkeit anlassbezogen bei Erstantragstellung und bei den jährlichen Folgeanträgen. Darüber hinaus sind die Antragsteller verpflichtet, Adressänderungen der zuständigen bezirklichen Abteilung Kindertagesbetreuung mitzuteilen, die dann anlassbezogen die Konsequenzen für die laufende Bewilligung prüft. Im neuen Online-Verfahren ist geplant, durch Verlängerung des Bewilligungszeitraums Folgeanträge entbehrlich zu machen. Weil jedoch die Verwaltung erfahrungsgestützt davon ausgeht, dass nicht alle Adressänderungen den bezirklichen Abteilungen Kindertagesbetreuung von den Betroffenen mitgeteilt werden, soll zukünftig ohne Beteiligung der Betroffenen eine regelhafte Prüfung stattfinden, ob sich Veränderungen bezüglich der Meldeadresse ergeben haben, die Auswirkungen auf die örtliche Zuständigkeit der FHH und damit die Bewilligung der Leistung haben. Der aktuelle Planungsstand sieht dabei vor, dass diese Prüfung im Hintergrund nicht nur jährlich, sondern alle drei Monate erfolgt. Daran wird deutlich, dass einmal eingerichtete automatisierte Prozesse nicht nur die Substitution bisher manuell erfolgender Verarbeitungen ermöglichen, sondern auch zur Intensivierung von Kontrollen genutzt werden können, ohne dass ein individueller Grund für eine häufigere Überprüfung besteht. Bezogen auf den hier beispielhaft dargestellten Aspekt begrüßt der HmbBfDI die erklärte Absicht, Rechtsgrundlagen für die anlasslose Prüfung der Adressdaten des Kindes und des gesetzlichen Vertreters während des Bewilligungszeitraums zu schaffen. Die inhaltliche Erörterung dazu ist noch nicht abgeschlossen.

Ein anderes Beispiel: Datenbestände können viel intensiver dahingehend durchleuchtet werden, ob Unregelmäßigkeiten vorliegen. Das soll zum Beispiel das Ziel eines Verfahrens für die Beihilfe sein: Um Betrugsfälle aufzudecken, sollen die pseudonymisierten Daten der letzten Jahre und dann regelmäßig von einem privaten IT-Dienstleister analysiert werden, um potentiellen Missbrauch anzuzeigen. Hier liegen Erfahrungen aus einer anderen Großstadt-Verwaltung vor, wo bislang nur sehr wenig mögliche Verdachtsfälle Anlass zu Nachfragen gegeben haben.

Diese Beispiele sollen nicht dahingehend missverstanden werden, dass die Chancen einer Digitalisierung nicht genutzt werden sollten und schon gar nicht soll damit ein Missbrauch von Leistungen verharmlost oder gar gerechtfertigt werden. Es gilt deutlich zu machen, dass mit der Digitalisierung auch u.a. die Risiken einer wesentlich stärkeren anlasslosen Kontrolle bis hin zur Überwachung verbunden sein können. Diese Risiken gilt es für Online-Projekt bereits in der Konzeptphase explizit herauszuarbeiten. In der Datenschutz-Grundverordnung wurde daher auch in Art. 35 festgeschrieben, dass die Verantwortlichen mit einer Datenschutz-Folgenabschätzung die Risiken einer Verarbeitung für die Rechte und Freiheiten natürlicher Personen vorab untersuchen müssen und die erforderlichen technischen und organisatorischen Maßnahmen zu treffen haben, um ein angemessenes Schutzniveau zu gewährleisten. Dies bedeutet auch, dass immer eine Rechtsgrundlage für eine Verarbeitung bestehen bzw. rechtzeitig vor dem Beginn der Verarbeitung neu geschaffen werden muss. Auch muss es im Zuge der Datenschutz-Folgenabschätzung immer eine Abwägung geben, ob die verfolgten Ziele nicht mit datensparsameren Verfahren oder mit weniger Risiken für die Betroffenen erreicht werden können. So kann u.a. eine Stichprobenprüfung statt einer Vollkontrolle ein adäquates Mittel sein.

Die Senatskanzlei hat zur Durchführung einer Datenschutz-Folgenabschätzung eine Arbeitshilfe zur Verfügung gestellt. Erste Datenschutz-Folgenabschätzungen, die dem HmbBfDI zur Beratung übermittelt wurden, zeigen, dass die Datenschutz-Folgenabschätzung noch zu wenig genutzt wird, auf der Grundlage einer systematischen Beschreibung der geplanten technischen Prozesse gerade das völlig Neue herauszuarbeiten, das mit einer Verarbeitungstätigkeit verbunden ist, und unter dem Blickwinkel des Datenschutzes insbesondere die mit der Verarbeitungstätigkeit verbundenen neuen Risiken zu betrachten.

Bemerkenswert ist auch, dass die Datenschutz-Folgenabschätzungen häufig erst erstellt werden, wenn die Produktivsetzung eines

Verfahrens unmittelbar bevorsteht oder bereits erfolgt ist. So geschehen etwa im Fall der Online-Service-Infrastruktur (OSI), deren Nutzungsbeginn im Berichtszeitraum des vorliegenden Tätigkeitsberichts liegt. Mit der OSI können Hamburgs Bürgerinnen, Bürger und Unternehmen einen zentralen Zugang zu allen Online-Diensten der Hamburger Verwaltung und zukünftig auch zu Online-Diensten des Bundes und anderer Länder erhalten. Damit ist diese Infrastruktur eine wesentliche technische Grundlage für die Umsetzung aller Online-Verwaltungsdienste im Rahmen des Onlinezugangsgesetzes und auch für das Programm Digital First. Technisch soll mit der OSI-Plattform eine sichere Verbindung zwischen dem Nutzer und dem Online-Dienst sowie den Fachverfahren im Netz der Hamburger Verwaltung hergestellt werden. Dazu gehören auch das Servicekonto einschließlich der dafür bereitgestellten Postfächer für eine sichere Kommunikation zwischen Nutzer und Verwaltung und weitere Module wie das ePayment.

Der HmbBfDI begrüßt es ausdrücklich, dass mit solch einer zentralen Komponente der Ansatz verfolgt wird, den Aufwand für die Umsetzung technischer Sicherheitsmaßnahmen an dieser Zugangsplattform zu konzentrieren, statt zahlreiche unterschiedliche Zugänge für die über 500 Verwaltungsvorgänge zu schaffen, die bis 2022 nach dem Onlinezugangsgesetz einen Onlinezugang erhalten sollen. Der Anspruch des Senats an die Sicherheit dieser Plattform ist hoch, wie er in den Senatsdrucksachen dazu immer wieder betont. Dennoch wurden dem HmbBfDI die Datenschutz-Folgenabschätzung und die Dokumentation der technischen und organisatorischen Maßnahmen, mit denen die Risiken für die Betroffenen begrenzt werden sollen, trotz wiederholter Nachfragen erst ein Jahr nach der Produktivsetzung übersandt. Das wird weder der Bedeutung des Projektes noch den gesetzlichen Anforderung gerecht.

4. Digitale Souveränität

Freie und selbstbestimmte Entscheidungen im Umgang mit den eigenen personenbezogenen Daten können nur funktionieren, wenn grundlegende Rahmenbedingungen bei der Wahl von Software, Hardware und Dienstleistungen zur Verfügungen stehen.

Digitale Souveränität wird als Schlagwort oft genutzt, wenn es auf politischer Ebene um richtungsweisende Entscheidungen der Sicherheit und Vertrauenswürdigkeit von Informationstechnologien geht. Im Herbst diesen Jahres wurde die Digitale Souveränität betrachtet, um Abhängigkeiten und gefühlten Bedrohungen von ausländischen Herstellerfirmen bei der Errichtung von 5G-Technologien zu begegnen. Diese Souveränität richtet sich an Staaten. Je nach Diskussionsgegenstand wird dieser Begriff vielfältig verwendet.
Insbesondere aus Sicht von natürlichen Personen im Kontext der informationellen Selbstbestimmung setzt die Digitale Souveränität aber weit vor einzelnen Herstellern oder anderen Marktteilnehmern an. So setzt Digitale Souveränität voraus, dass Nutzer grundsätzlich selbst über Mittel und Wege der Verarbeitung ihrer Daten entscheiden, diese nachvollziehen und kontrollieren können. Somit betrifft es neben der reinen Hard- oder Software auch technische Details wie Schnittstellen und Weitergaben, Datenformate, die Auswahl von Dienstleistern bis hin auf die Ebene des Quellcodes, die fachkundigen Nutzern Transparenz und somit Souveränität bringen soll. Produkte und Dienstleistungen sind immer stärker miteinander verbunden. Die Wahl des Betriebssystems führt bereits zu einer Einschränkung in der Wahl von Software und Diensten, die der Betriebssystemhersteller überhaupt für seine Plattform zulässt. Ein bestimmtes Software-Ökosystem bedingt gleichzeitig eine Festlegung auf die zugehörigen Clouddienste des Herstellers und wiederum implizit die anzuwendende Rechtsgrundlage; beispielsweise bei Zugriffsmöglichkeiten von Nachrichtendiensten. Diese zunehmend zentralisierte Bereitstellung von Diensten und Produkten führt zu starken Abhängigkeiten, die nur schwer zu durchbrechen und noch schwerer vollständig für den Normalanwender zu verstehen sind.

Die grundlegenden Anforderungen des Datenschutzes durch Technikgestaltung, der Gewährleistung von Informationssicherheit und Datenschutzfunktionalitäten sowie Rechenschaftspflichten von Verantwortlichen tragen alle einen Teil zur Digitalen Souveränität der Betroffenen und Nutzerinnen bei. Aus diesem Grunde unterstützt der HmbBfDI ausdrücklich Bestrebungen der Datenschutzkonferenz (DSK), ein Positionspapier im Kreise der deutschen Aufsichtsbehörden zu veröffentlichen, welches klare Forderungen stellt, um den o.g. Anforderungen gerecht zu werden. Im Kern sieht der HmbBfDI folgende wesentliche Punkt als besonders wichtig an:

1. Überprüfbarkeit und Möglichkeiten zur Kontrolle der Produkte und Dienstleistungen, sowohl bei der Auswahl als auch im Betrieb. Verantwortliche und Nutzer können aufgrund komplexer Funktionsweisen häufig nicht beurteilen, ob die zur Auswahl stehende Informationstechnik für die Aufgabe geeignet und optimal ist. Für solche Beurteilungen erscheinen u.a. Zertifizierungen nach klaren Kriterien geeignet.
2. Nutzung offener Standards, um tatsächlich Interoperabilitäten zu gewährleisten und Anbieter wechseln zu können. Zudem fördern offene Standards unmittelbar die Transparenz und erleichtern somit die Überprüfbarkeit und Kontrolle. Offene Standards sind bereits heute auf weitestgehend allen Ebenen der Informationstechnik nutzbar, aber nicht überall die Regel.
3. Möglichkeiten zur Steuerung des Zugriffs auf Daten und der Konfiguration von Systemen. Verantwortliche müssen bei der Nutzung von Dienstleistungen über Steuerungsmöglichkeiten verfügen. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil einer jeden Dienstleistung werden. Betroffene sollten über Möglichkeiten verfügen, die von ihnen bereitgestellten Daten verwalten zu können.
4. Zudem müssen Betroffene in die Lage versetzt werden, freiwillig, selbstbestimmt und in Kenntnis der Auswirkungen über die Verarbeitung ihrer Daten zu entscheiden. Hierzu müssen auch Verantwortliche die notwendigen Informationen bereitstellen. Angesichts komplexer technischer Lösungen bedarf es unab-

hängiger Bewertungen, auch wenn der Verantwortliche von externen Kompetenzen beraten wird.

Neben den technischen Anforderungen müssen für eine objektive Bewertung Digitaler Souveränität darüber hinaus auch rechtliche Rahmenbedingungen und politische Entwicklungen beachtet werden. In den letzten Jahren haben bereits viele Verantwortliche erkannt, dass neben Privatpersonen, sondern zunehmend in besonderem Maße Unternehmen und staatliche Institutionen riskieren, die Kontrolle über die von ihnen generierten Daten zu verlieren. Zentralisierungen bei der Erbringung von IT-Dienstleistungen, annähernd monopolistische Datenkonzerne sowie politische Entscheidungen, die erst nachgelagert auf Grundrechte wie das Recht auf informationelle Selbstbestimmung eingehen, erschweren die Beschreitung auf dem Weg zu einer tatsächlichen digitalen Souveränität. Die DS-GVO schafft einen grundsätzlichen Rahmen für alle Beteiligten und ermöglicht es Bürgerinnen und Bürgern die Nutzung ihrer Daten zu kontrollieren und somit tatsächlich zum Souverän zu werden. Der HmbBfDI wird sich weiter dafür einsetzen, dass diese Entwicklungen weiter im Sinne der Wahrung von Grundrechten erfolgt und somit jedes Individuum frei und ohne Einschränkungen über die eigene Datenverarbeitung bestimmen kann.

5. KRANKSCHREIBUNG VIA HANDY

Lockerungen des Fernbehandlungsverbots in den Berufsordnungen der meisten Landesärztekammern schaffen die Grundlage für neue telemedizinische Angebote. Neben der berufsrechtlichen Zulässigkeit setzt die rechtskonforme Beratung und Behandlung über Kommunikationsmedien aber auch ein besonderes Augenmerk auf Datenschutz und Datensicherheit voraus.

Zum einen können Anbieter von Telemedizin-Plattformen, die nicht selbst Behandler sind, die Verarbeitung von Gesundheitsdaten nicht auf Art. 9 Abs. 2 lit. h DSGVO als Rechtsgrundlage stützen. Vielmehr müssen sie für die Gesundheitsdatenverarbeitung zwingend eine wirksame Einwilligung der Betroffenen einholen. Zum anderen muss auch die Einbindung externer (technischer) Dienstleister etwa für die Audio- und Videotelefonie, zur Identitätsfeststellung oder zur Nutzungsanalyse den datenschutzrechtlichen Anforderungen genügen. Dies ist insbesondere dann problematisch, wenn die externen Dienstleister personenbezogene Daten auch für eigene Zwecke nutzen.

Dies hat ein in Hamburg ansässiges Unternehmen, das seinen Kunden Krankschreibungen ohne Arztbesuch anbietet, zunächst verkannt und ein Einschreiten des HmbBfDI im Berichtszeitraum erforderlich gemacht.

Anfang Januar 2019 ist der HmbBfDI durch intensive Presseberichterstattung auf das Angebot eines Hamburger Start-Ups aufmerksam geworden, Krankschreibungen per WhatsApp zu vermitteln. Für das Angebot stellt das Unternehmen eine Website zur Verfügung, auf der Patientinnen und Patienten online einen Fragebogen zu ihren Symptomen ausfüllen können, um dann unter Angabe personenbezogener Daten eine diesbezügliche Krankschreibung zu bestellen. Die Zusendung der Krankschreibung ebenso wie die Kommunikation zwischen Arzt und Patienten fand beim Start des Dienstes Ende 2018 über den Messaging-Dienst WhatsApp statt.

Aufgrund von Unklarheiten bezüglich der tatsächlichen Datenflüsse zwischen dem Unternehmen und dessen Honorarärzten sowie der diesbezüglichen Rechtsgrundlagen und wegen grundsätzlicher Bedenken des HmbBfDI gegen die Übermittlung von Gesundheitsdaten via WhatsApp hat der HmbBfDI bereits Mitte Januar 2019 eine aufsichtsbehördliche Prüfung des Angebots eingeleitet. Das Unternehmen teilte daraufhin in seiner ersten Stellungnahme mit, das Angebot bereits in Teilen von WhatsApp gelöst zu haben und mit dem nächsten Release vollständig auf den Messaging-Dienst verzichten zu wollen. Zum Zeitpunkt der ersten Stellungnahme wurde nur noch der zufällige erstellte Schlüssel, mit welchem die vom Patienten auf der Website eingegebenen Daten vor Speicherung auf dem deutschen Server des Unternehmens clientseitig verschlüsselt wurden, per WhatsApp an den Arzt übertragen, damit dieser den Datensatz nach Abholung vom Server für die Diagnose und Krankschreibung entschlüsseln konnte. Der daneben ebenfalls über WhatsApp abgewickelte digitale Versand der Krankschreibung erfolgte in der Verantwortung des jeweils attestierenden Arztes als eigenständigem Verantwortlichen und nicht durch das Unternehmen. Seit Mitte vergangenen Jahres kommt die Krankschreibung via Handy vollständig ohne Einbindung von WhatsApp aus. Der Patient erhält eine Bestellnummer per Mail und einen Code per SMS. Damit lässt sich die Krankschreibung auf der Website des Unternehmens herunterladen und entschlüsseln.

Allerdings ergab die Prüfung der Datenschutzdokumentation des Unternehmens andere, schwerwiegende Mängel. So stellte sich das Unternehmen zunächst zum einen auf den Standpunkt, für die Verarbeitung der Gesundheitsdaten seiner Kunden (Symptome, etwaige Risikoumstände) zwecks Bereitstellung und Abrechnung des Services keine Einwilligung der Betroffenen einholen zu müssen bzw. durch das erforderliche Setzen eines Hakens zum Akzeptieren der AGB und zur Bestätigung der Datenschutzerklärung und der Widerrufsbelehrung hinreichend abgesichert zu sein. Zum anderen hatte es das Unternehmen versäumt, für den im Auftrag der attestierenden Ärzte durch das Unternehmen erfolgenden postalischen

Versand der Arbeitsunfähigkeitsbescheinigung mit den Ärzten einen Auftragsverarbeitungsvertrag abzuschließen.

Aufgrund dessen machte der HmbBfDI Anfang März 2019 von der förmlichen Abhilfemaßnahme des Art. 58 Abs. 2 lit. d DSGVO Gebrauch und wies das Unternehmen unter Anordnung der sofortigen Vollziehung an, a) Gesundheitsdaten seiner Kunden für die oben genannten Zwecke nur bei Vorliegen einer wirksamen Einwilligung und b) personenbezogene Daten im Auftrag der mit dem Unternehmen kooperierenden Ärzte nur bei Vorliegen eines Auftragsverarbeitungsvertrages zu verarbeiten. Gegen die Anweisung wurde kein Rechtsbehelf eingelegt. Vielmehr hat das Unternehmen seine zuvor vertretene Rechtsaufassung aufgegeben und der Anweisung innerhalb der hierfür gesetzten Frist Rechnung getragen. Es holt nunmehr vor Abschluss des Bestellvorgangs und der damit verbundenen Speicherung von Gesundheitsdaten eine ausdrückliche Einwilligung seiner Kunden in die Verarbeitung der Gesundheitsdaten ein. Zudem hat es die erforderlichen Auftragsverarbeitungsverträge abgeschlossen und dem HmbBfDI vorgelegt.

Hinsichtlich der zuvor mangels Einwilligung rechtswidrigen Verarbeitung von Gesundheitsdaten und des anfänglichen Verstoßes gegen Art. 28 Abs. 3 DSGVO prüft der HmbBfDI auch Maßnahmen nach Art. 58 Abs. 2 lit. i DSGVO. Zudem wirft auch die gegenwärtige Ausgestaltung des Angebots noch datenschutzrechtliche Fragen auf, die aktuell einer Klärung zugeführt werden.

6. Sicherheit von Gesundheitsdaten bei nicht-ärztlichen Behandlern

Überall dort, wo medizinische Behandlungen stattfinden, sind Behandler gemäß § 630f des Bürgerlichen Gesetzbuchs zur Dokumentation in Gestalt einer Patientenakte verpflichtet und findet daher eine Verarbeitung personenbezogener Gesundheitsdaten statt. Gesundheitsdatenschutz ist also keineswegs nur ein Thema für Krankenhäuser, Arztpraxen und Psychotherapeuten, sondern auch für Heilpraktiker, Hebammen, Masseure, medizinische Bademeister, Podologen, Osteopathen, Ergotherapeuten und viele mehr. Nicht alle behandelnden Professionen scheinen aber ausreichend auf die hohen datenschutzrechtlichen Anforderungen im Umgang mit Gesundheitsdaten eingestellt, wie der HmbBfDI im vergangenen Jahr anlässlich verschiedener Eingaben feststellen musste.

Offen herumliegende Kundenkarteien mit sensiblen Anamnesedaten im Publikumsbereich von Kosmetikstudios, unzureichend akustisch abgekoppelte Behandlungsbereiche in Gemeinschaftsräumlichkeiten verschiedener Therapeuten, Trainern und Coaches, die Aufbewahrung von Behandlungsdokumentationen auf einem unverschlossenen privaten Dachboden, eine offene Lagerung zu entsorgender Unterlagen vor der vollen Papiertonne eines Mehrparteienhauses oder die (unvollständige) Verbrennung von Patientenakten auf einem öffentlich zugänglichen Grundstück – die den HmbBfDI erreichenden Beschwerden und Anzeigen aus dem Bereich der nicht-ärztlichen Gesundheitsdatenverarbeitung betreffen den gesamten Verarbeitungszyklus von Gesundheitsdaten durch medizinische Behandler. Um den gegebenen Missständen abzuhelfen, war der HmbBfDI im vergangenen Jahr mit einer großen Bandbreite seines Untersuchungs- und Abhilfespektrums gefordert. In einigen Fällen ist dabei nur eine telefonische Beratung der Betroffenen erfolgt, da die Betroffenen aus Sorge vor einer Beschädigung des Behandlungsverhältnisses keine unmittelbare Einschaltung des HmbBfDI wünschten. Anderen Fällen vermuteter Missstände konnte mittels Hinweis nach

Art. 58 Abs. 1 lit. d DSGVO abgeholfen werden. In einem Fall waren aber auch Gefahrenabwehrmaßnahmen im Wege der unmittelbaren Ausführung zu treffen. Zudem sind Abgaben an die Staatsanwaltschaft wegen bestehenden Anfangsverdachts von Straftaten erfolgt.

Vor diesem Hintergrund appelliert der HmbBfDI nachdrücklich an die oben genannten Berufsgruppen, sich – auch und gerade bei fehlender Pflicht zur Benennung eines Datenschutzbeauftragten – selbst mit den einschlägigen Sicherheitsvorgaben für die Aufbewahrung und spätere Löschung bzw. Vernichtung von Gesundheitsdaten vertraut zu machen und entsprechend zu handeln. Insbesondere müssen von den Verantwortlichen geeignete technische und organisatorische Maßnahmen ergriffen werden, um den Zugang, Zutritt und Zugriff Unbefugter auf Patientenakten zu verhindern. Weiter ist während der Aufbewahrungs- bzw. Speicherdauer die Verfügbarkeit der Daten zu gewährleisten und müssen bei der Löschung geeignete Lösch- bzw. Vernichtungsmethoden zum Einsatz kommen.

Zur Unterstützung der Verantwortlichen bei der Auswahl und Bewertung technischer und organisatorischer Maßnahmen kann unter anderem das vom Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) bereitgestellte Standard-Datenschutzmodell (SDM) dienen, das mit dem Baustein 11 „Aufbewahrung“ und dem Baustein 60 „Löschen und Vernichten“ bereits einschlägige Maßnahmenkataloge umfasst.

7. Analyse von Handelsregister- und anderen Pflichtveröffentlichungen durch Unternehmen

Die Verarbeitung von personenbezogenen Daten aus öffentlich zugänglichen Quellen ist an Art. 6 Abs. 1 lit. f DSGVO zu messen. Regelmäßig liegen die Informationen zu den betroffenen Personen bereits durch die Registerveröffentlichungen vor, so dass eine Abwägung in der Regel zu Lasten der Betroffenen ausgeht.

Der HmbBfDI hat in diesem Jahr eine Vielzahl von Beschwerden zu einem in Hamburg ansässigen Unternehmen erhalten, das eine eigene Suchmaschine vorhält, in der nach Wirtschaftsdaten gesucht werden kann. Deren Ergebnisse sind auch über eine Google-Suche auffindbar. Grundlage der Datenverarbeitung sind dabei Handelsregisterbekanntmachungen und andere Pflichtveröffentlichungen. Eine zusätzliche Funktion des angebotenen Dienstes besteht darin, dass die Wirtschaftsdaten bildlich aufbereitet und dargestellt werden. Der Betrachter erhält einen umfassenden Überblick über die Vernetzung von Unternehmen und deren Vertreter, indem er ein Netzwerk mit den aktuellen Verbindungen zu anderen Unternehmen und Beteiligungen angezeigt bekommt.

Die eingereichten Beschwerden bezogen sich vorrangig darauf, dass Informations- und Auskunftspflichten nicht eingehalten und begehrte Löschungen personenbezogener Daten von dem verantwortlichen Unternehmen nicht vorgenommen worden seien. Vor diesem Hintergrund hat sich der HmbBfDI mit dem verantwortlichen Unternehmen zusammengesetzt und verschiedene Anpassungen an deren Prozesse gefordert. Die Rechtsgrundlage für die Datenverarbeitung wird nunmehr explizit genannt und das berechtigte Interesse noch deutlicher herausgestellt. Darüber hinaus war für den Betrachter eines von dem Verantwortlichen aufbereiteten Firmennetzwerkes nicht sofort erkennbar, welche Verbindungen innerhalb des dargestellten Netzwerks aktuell oder durch Geschäfts-

führerwechsel veraltet sind. Nunmehr enthält die Netzwerkdarstellung eine Legende, die dies klar verdeutlicht. Schließlich findet das Alter der Informationen eine bessere Berücksichtigung. Bei den Darstellungen, in denen Personen vorkommen, gewichtet das verantwortliche Unternehmen nunmehr, wie lange bspw. Geschäftsführer bereits aus dem Unternehmen ausgeschieden sind. Insbesondere werden künftig Personen komplett automatisch von der Darstellung ausgeschlossen, wenn ihre Verbindungen bzw. Rollen in der Darstellung länger als fünf Jahre zurückliegen bei Geschäftsführern und vergleichbaren Positionen sowie ein Jahr bei Kaufleuten und Vereinen.

Den Großteil der Beschwerden musste der HmbBfDI jedoch zurückwiesen, da die Datenverarbeitung rechtmäßig erfolgte. Die Verarbeitung von personenbezogenen Daten aus allgemein zugänglichen Quellen ist in der DSGVO nicht ausdrücklich geregelt. Es gelten daher die allgemeinen Regelungen. Für die Datenverarbeitung durch das verantwortliche Unternehmen ist vorliegend Art. 6 Abs. 1 lit. f DSGVO heranzuziehen. Im Rahmen der vorgenommenen Abwägungsentscheidungen fiel die Interessenabwägung regelmäßig zu Gunsten des verantwortlichen Unternehmens aus. Auch die bildliche Darstellung von Firmennetzwerken führt im Ergebnis nicht zu einem überwiegenden Interesse auf Seiten der Betroffenen. Die Informationen über ehemalige Beteiligungen an anderen Gesellschaften oder aktuell an parallelen Gesellschaften liegen bereits mit den Pflichtveröffentlichungen durch die öffentlichen Register vor. Das verantwortliche Unternehmen stellt diese Informationen lediglich zusätzlich bildlich dar. Diese Aufbereitung führt nur zu einer schnelleren und besseren Wahrnehmbarkeit bei den interessierten Nutzern, jedoch erfolgt dadurch kein tieferer Eingriff in die Persönlichkeitsrechte der Betroffenen, als dieser durch die Veröffentlichung der Daten durch die öffentlichen Register bereits ohnehin vorliegt.

8. Werbefinanzierte Angebote im Online-Zeitungsbereich / Treffen mit dem Bundesverband Deutscher Zeitungsverleger und deren Mitgliedern

Ein Umdenken in der Verlagsbranche hinsichtlich des Webtrackings bei Online-Medien scheint allmählich einzusetzen. Erste Verlage reagieren allerdings nur sehr langsam auf Beanstandungen durch die Aufsichtsbehörden zum Einsatz von massivem Webtracking auf ihren Webseiten.

Im März 2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder die Orientierungshilfe für Anbieter von Telemedien (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf) als Konkretisierung der Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 beschlossen und veröffentlicht. Wesentlicher Gegenstand der Orientierungshilfe ist die Verarbeitung personenbezogener Daten beim sog. Webtracking, wobei es sich nach dem Verständnis der Aufsichtsbehörden hierbei um eine Datenverarbeitung handelt, bei der in der Regel eine webseitenübergreifende Nachverfolgung des individuellen Verhaltens von Nutzern vorgenommen wird. Diese Art der Nachverfolgung wird hauptsächlich im Bereich des Werbe-Trackings eingesetzt, um so möglichst zielgenau die Vorlieben der jeweiligen Webseiten-Nutzer identifizieren zu können und den Werbeplatz auf der Webseite des Verantwortlichen höchstbietend zu verkaufen.

Die Vergabe der Werbeflächen auf der Webseite der Verantwortlichen erfolgt mittlerweile fast ausschließlich durch einen automatisierten Prozess, der Werbeplätze in Echtzeit verkauft und ausliefert. Dies ist unter dem Begriff Real-Time-Bidding oder Real-Time-Advertising bekannt und wird regelmäßig durch den HmbBfDI als nicht datenschutzkonform bewertet. Insbesondere die zahlreichen für den Nutzer und größtenteils auch für die Verantwortlichen selbst

nicht nachvollziehbaren Verkettungen von Daten durch eingesetzte Drittdienstleister, die an dem Prozess der Ausspielung zielgenauer Werbung beteiligt sind, der regelmäßig große Umfang der Datenverarbeitung sowie die fehlende Erwartbarkeit der betroffenen Nutzer, dass bspw. Informationen über sie darüber weitergegeben werden, welche Webseiten von ihnen besucht wurden, führen dazu, dass der Einsatz derartiger Trackingmethoden nur auf eine informierte Einwilligung durch den Nutzer gestützt werden kann. Solche Einwilligungen sind überwiegend nicht anzutreffen. Einfache Cookie-Banner erfüllen die Anforderungen nicht.

Besonderheit der Verlagsbranche ist es, dass diese sich zu großen Teilen durch Werbung und im Speziellen durch personalisierte Werbung finanziert. Die Befürchtung der Branche besteht offenbar darin, dass im Rahmen von implementierten Einwilligungslösungen ein Großteil der Nutzer eine Einwilligung in die Datenverarbeitung nicht erteilen und die Webseite verlassen werden bzw. die Verlage die für sie einträglichen Werbeformen nicht mehr nutzen können. Dadurch ginge den Verlagen ein Großteil der Einnahmen, die über Werbung generiert werden, verloren. Dies habe nach Ansicht der Verleger bedeutende Auswirkungen auf den Journalismus und wie Redaktionen künftig in Deutschland arbeiten werden. Durch das Ausbleiben eines großen Teils der Werbeeinnahmen werden Redaktionen nach Ansicht der Verlagsbranche in Zukunft deutlich verkleinert und lokale Redaktionen sogar ganz aufgelöst werden müssen. Außerdem bestehe die Gefahr, dass qualitativ guter Journalismus nicht mehr in dem Umfang gewährleistet werden könne. Vor diesem Hintergrund hat der HmbBfDI einen Austausch zwischen Aufsichtsbehörden und dem Bundesverband Deutscher Zeitungsverleger sowie deren Mitgliedern organisiert. Aus Sicht des HmbBfDI war es wichtig zu klären, wie der professionelle Journalismus mit seiner Finanzierungsnotwendigkeit die gesetzlichen Voraussetzungen erfüllen kann, die sich bis zu einer bislang nicht absehbaren Geltungserlangung einer möglichen künftigen ePrivacy-Verordnung ausschließlich nach den Vorschriften der DSGVO richten.

Die Bilanz des HmbBfDI nach zwei Treffen mit dem Bundesverband Deutscher Zeitungsverleger und deren Mitgliedern ist bisher eher ernüchternd. Weder konnte ein konkretes Einwilligungsmodell oder die Implementierung datenschutzfreundlicher Einstellungen realisiert werden, obgleich diese Zielsetzung von Seiten der Aufsichtsbehörden mehrfach deutlich gefordert wurde. Dabei existieren bereits branchenspezifische Lösungen in europäischen Nachbarländern, die die Anforderungen des HmbBfDI erfüllen würden.

Kurz vor Redaktionsschluss erreichte den HmbBfDI schließlich die Mitteilung des Bundesverbandes Deutscher Zeitungsverleger, dass sich die Branche nunmehr intensiv mit dem Thema der Einwilligung und zwar sowohl mit der rechtlichen Konformität als auch mit der technischen Umsetzung beschäftigt und der Bundesverband Deutscher Zeitungsverleger selbst zu dieser Thematik Informationsveranstaltungen für seine Mitglieder anbietet. Der HmbBfDI wird die weiteren Entwicklungen in seinem Zuständigkeitsbereich verfolgen, nicht zuletzt aufgrund vorliegender Beschwerden. Die Zeit, die erforderlichen Anpassungen vorzunehmen, wurde durch die Aufsichtsbehörden in ausreichendem Maße gewürdigt. Ein koordiniertes Vorgehen durch die Aufsichtsbehörden des Bundes und der Länder wird nunmehr gegenwärtig vorbereitet.

9. DOXXING BEI TWITTER

Auf Twitter wurden zum Jahreswechsel 2018/2019 umfangreiche Daten von Personen aus dem politischen und künstlerischen Bereich Deutschlands rechtswidrig veröffentlicht. Der HmbBfDI reagierte noch am Tag des Bekanntwerdens in den Medien und forderte Twitter zur Löschung der Links auf. Die Löschung ist noch am selben Tag erfolgt.

Am 04.01.2019 wurde dem HmbBfDI aus den Medienberichten bekannt, dass unbekannte Täter eine immense Anzahl von personenbezogenen Daten prominenter Persönlichkeiten auf Twitter veröffent-

licht haben. Im Fachjargon wird diese Art von Datenleck als Doxxing bezeichnet. Damit ist ein Phänomen gemeint, bei dem personenbezogenen Daten internetbasiert zusammengetragen und veröffentlicht werden – meist zu bösartigen Zwecken. Die Betroffenen sollen vorgeführt und ihre Daten zum möglichen Missbrauch freigegeben werden.

Wie sich herausstellte, wurden personenbezogene Daten Betroffener bereits im Dezember 2018 auf Twitter hochgeladen. Der Vorfall wurde aber erst nach den Feiertagen von Medien aufgegriffen und der breiten Öffentlichkeit bekannt. Nach Medienberichten sind Bundesbehörden bereits einen Tag vor Bekanntwerden in den Medien über die Vorfälle informiert worden. Dem HmbBfDI lagen bis dahin keine Beschwerden oder Meldungen vor.

Aufgrund der Dringlichkeit der Angelegenheit und des drohenden Schadens für die Rechte und Freiheiten der Betroffenen war ein schnelles Handeln geboten. Twitter hat seine deutsche Niederlassung in Hamburg, seine europäische Hauptniederlassung allerdings in Irland, so dass auch die irischen Kollegen über den Vorfall informiert wurden. Gleichzeitig hat der HmbBfDI der Twitter International Company eine entsprechende Liste mit Shortlinks zugesandt, die gelöscht werden sollen, erhielt allerdings keine umgehende Reaktion auf die Löschungsanordnung, womöglich aufgrund der Unklarheit bezüglich der Zuständigkeit.

Der HmbBfDI erhielt zwar verzögert, jedoch noch am selben Tag eine Reaktion von Twitter, was er zum Anlass nahm, mit der Verantwortlichen und mit anderen Aufsichtsbehörden einen schnelleren Kommunikationsfluss für solche dringenden Fälle zu vereinbaren.

RECHTSVERBINDLICHE ANORDNUNGEN UND BUSSGELDER IV.

1. HVV-Data Breach: Bußgeld wegen verspäteter Meldung und Benachrichtigung betroffener Personen

Die Pflicht zur Meldung eines Data Breaches bei der zuständigen Aufsichtsbehörde soll diese in die Lage versetzen, auf eine angemessene Reaktion hinsichtlich der aufgetretenen Sicherheitslücke hinzuwirken, um die Rechte und Freiheiten betroffener Personen zu schützen. Der HmbBfDI hat gegen die Hamburger Verkehrsverbund GmbH (HVV GmbH) daher ein rechtskräftiges Bußgeld in Höhe von 20.000 € wegen verspäteter Meldung eines Data Breaches sowie verspäteter Benachrichtigung der betroffenen Personen erlassen.

Am 6.7.2018 erhielt die HVV GmbH durch Hinweis eines Kunden Kenntnis von einer Sicherheitslücke auf der Website www.hvv.de, die durch das Einspielen eines Updates am 5.2.2018 entstanden war und den sog. Customer E-Service (CES) betraf. Die Sicherheitslücke bestand darin, dass sich im CES eingeloggte Kunden, die über eine HVV-Card verfügten und ihr CES-Kundenkonto mit mindestens einer aktiven Vertragsbeziehung in Hintergrundsystemen verknüpft hatten, durch Änderung der URL Daten anderer Kunden anzeigen lassen konnten, die eine HVV Card besitzen, über eine allgemeine Fahrtberechtigung verfügen und generierte Rechnungen hatten. Hatte sich also jemand als Kunde eingeloggt, erschien in der Adresszeile des Browsers eine URL, welche die eigene Kundenkontonummer enthielt. Wurde diese durch eine andere existierende Kundenkontonummer ersetzt, erhielt der Kunde Zugriff auf das andere Kundenkonto. Konkret gelang es dem Kunden durch Änderung der Kundenvertragsnummer innerhalb der URL Daten über Bestellhistorie, aktuelle Rechnungen und Bankdaten anderer Kunden einzusehen.

Zwar hatte die HVV GmbH unmittelbar auf das Bekanntwerden der Sicherheitslücke reagiert und die entsprechende Seite in den Wartungsmodus versetzt. Allerdings vergaß die HVV GmbH, der zwi-

schenzeitlich durch Geltung der DSGVO etablierten Meldepflicht innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde Rechnung zu tragen. So erhielt der HmbBfDI von diesem Vorfall erst am 11.7.2018 durch einen Anruf der Hochbahn AG Kenntnis, die um Mitteilung bat, ob es sich hierbei um einen nach Art. 33 Abs. 1 DSGVO meldepflichtigen Vorgang handelte. Mit E-Mail vom 12.7.2018 erhielt der HmbBfDI weitere Informationen zu dem aufgetretenen Sicherheitsbruch. Dieser E-Mail ließ sich entnehmen, dass auch eine Benachrichtigung der betroffenen Personen nicht erfolgt war, da davon ausgegangen wurde, dass das Risiko, dass die betroffene Sicherheitslücke tatsächlich ausgenutzt werde und es zu einem Missbrauch personenbezogener Daten kommen könne, gering sei.

Diese Auffassung konnte der HmbBfDI nicht teilen. So sind im „Mein HVV"-Account unter anderem Name, Adresse, Geburtsdatum und Mobilfunknummer hinterlegt. Zu den Daten, zu denen man sich über das CES Zugriff verschaffen kann, zählen darüber hinaus auch die Bestellhistorie, Rechnungen und Bankdaten, soweit sie in den Rechnungen der Kunden enthalten sind. Der unbefugte Zugriff auf derartige Daten ist geeignet, einer betroffenen Person erheblichen wirtschaftlichen Schaden zuzufügen. Denn solche Informationen können für Identitätsdiebstähle oder -betrüge, unbefugte SEPA-Lastschriften und die Übernahme anderer Internetaccounts genutzt werden.

Wir baten die HVV GmbH daher um Stellungnahme. Diese führte einige Punkte an, die die verspätete Meldung der Sicherheitslücke und zunächst unterbliebene Benachrichtigung begründen sollten. Zwar habe die HVV GmbH von der aufgetretenen Sicherheitslücke am 6.7.2018 Kenntnis erlangt. Zu diesem Zeitpunkt sei jedoch kein Zugriff auf das für eine Einschätzung der Sicherheitslage nötige Personal möglich gewesen. Es habe noch keine gesicherte Informationsgrundlage bestanden, um das Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen bewerten zu können. Auch habe man am 9.7.2018 und am 10.7.2018 durch den Datenschutzbeauftragten der Hamburger Hochbahn AG erfolglos versucht, die Sicherheitslücke beim HmbBfDI telefonisch zu melden. Zudem gehe man

von einem Entfallen der Benachrichtigungspflicht nach Art. 34 Abs. 3 DSGVO aus.

Die angeführten Gründe konnten nicht überzeugen. So war der HmbBfDI in den Tagen nach Auftreten der Sicherheitslücke durchgehend per E-Mail oder Fax erreichbar. Data-Breaches sind der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden zu melden, wenn sie zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. Dabei geht die Konzeption des Art. 33 Abs. 1 DSGVO davon aus, dass die Meldepflicht bei der zuständigen Aufsicht den Regelfall, die Möglichkeit, eine solche Meldung zu unterlassen dagegen die Ausnahme darstellt.

Der HmbBfDI hatte im Ergebnis auch keine Zweifel, dass die HVV GmbH neben der Aufsichtsbehörde auch die betroffenen Personen von der aufgetretenen Sicherheitslücke hätte benachrichtigen müssen. Dies ist nach Art. 34 Abs. 1 DSGVO stets und unverzüglich erforderlich, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen droht. Der HmbBfDI konnte auch nicht erkennen, dass eine solche Benachrichtigung nach Art. 34 Abs. 3 DSGVO entbehrlich gewesen wäre. So konnte sich die HVV GmbH etwa nicht mit Erfolg darauf berufen, geeignete technisch-organisatorische Sicherheitsvorkehrungen im Sinne von Art. 34 Abs. 3 lit. a DSGVO getroffen und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt zu haben. Hierzu war insbesondere das Versetzen der Internetseite in einen Wartungsmodus nicht geeignet. Nach Sinn und Zweck können von dieser Ausnahme nämlich nur solche Sicherheitsvorkehrungen erfasst sein, die vor Auftreten der Sicherheitslücke getroffen wurden.

Von der Benachrichtigung konnte auch nicht deshalb abgesehen werden, weil die HVV GmbH durch nachfolgende Maßnahmen sichergestellt hätte, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht, vgl. Art. 34 Abs. 3 lit. b DSGVO. Auch hierzu war das Versetzen der Internetseite in den Wartungsmodus nicht geeignet. Denn

um dessen Voraussetzungen zu erfüllen, wäre es erforderlich gewesen, Maßnahmen zu treffen, die einen Missbrauch bereits erbeuteter Daten verhindern, wie zum Beispiel eine Änderung von Passwörtern. Hierzu war die HVV GmbH gar nicht in der Lage, da sie zum Beispiel keine Kontrolle über die Bankdaten der Kunden und deren Nutzung hat.

Der HmbBfDI konnte im Ergebnis erreichen, dass die betroffenen Personen von dem aufgetretenen Sicherheitsbruch benachrichtigt wurden. Zur Pflichtenmahnung hielt er die zusätzliche Sanktionierung mit einem Bußgeld für erforderlich: Bei der Benachrichtigung betroffener Personen über aufgetretene Sicherheitslücken handelt es sich um eine essentielle Vorgabe der Datenschutzgrundverordnung. Denn regelmäßig sind nur die betroffenen Personen in der Lage, sich vor möglichen Schäden durch den Missbrauch ihrer Daten zu schützen. Die Pflicht zur Meldung aufgetretener Sicherheitslücken bei der zuständigen Aufsichtsbehörde soll die Aufsichtsbehörde in die Lage versetzen, auf einen angemessenen Umgang mit Sicherheitsbrüchen hinzuwirken und betroffene Personen vor potentiellen Schäden bewahren.

2. BUSSGELD FÜR DIE DURCHFÜHRUNG EINER WERBEMAßNAHME TROTZ WERBEWIDERSPRUCH

Der Versand eines Newsletters trotz erklärtem Widerspruch gegen Direktwerbung verstößt gegen die Rechte des Betroffenen und kann von der Datenschutzaufsichtsbehörde mit einem Bußgeld geahndet werden.

Im Berichtszeitraum hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) ein Bußgeldverfahren gegen die Hamburger Volksbank eG durchgeführt. Das Unternehmen hatte einem Kunden per E-Mail einen Newsletter mit werblichen

Inhalt geschickt, obwohl dieser Kunde zuvor der Zusendung weiterer Werbeanschreiben ausdrücklich widersprochen hatte.

Gemäß Art. 21 Abs. 2 Datenschutz-Grundverordnung (DSGVO) haben Adressaten von Werbemaßnahmen das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke der Direktwerbung einzulegen. Die Ausübung des Widerspruchrechts ist an keine Bedingungen geknüpft. Der Widerspruch muss auch nicht in einer bestimmten Form ausgeübt werden. Er kann schriftlich, mündlich oder elektronisch eingelegt werden. Die Umsetzung des Widerspruchs muss unverzüglich erfolgen. Nur in Einzelfällen kann es für ein Unternehmen unzumutbar sein, einen eingegangen Werbewiderspruch unverzüglich umzusetzen. Dies kann etwa dann der Fall sein, wenn konkrete Werbeaktionen bereits angelaufen sind und die Kontaktdaten der betroffenen Person sich schon in der Verarbeitung befinden.

Das Unternehmen hat den Verstoß eingeräumt und vorgetragen, dass nach dem Eingang des Widerspruchs die Löschung der E-Mailadresse des Beschwerdeführers aus dem Newsletter-Verteiler aufgrund eines Bearbeitungsfehlers eines Beschäftigten versehentlich unterblieben sei.

Bei Verstößen gegen die Rechte der betroffenen Personen gemäß Art. 21 Abs. 2, 3 DSGVO werden nach Art. 83 Abs. 5 lit. b DSGVO im Einklang mit Art. 83 Abs. 2 DSGVO Geldbußen von bis zu 20.000.000 € oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher der Beträge höher ist. Bei der Festsetzung der Geldbuße haben die Aufsichtsbehörden gemäß Art. 83 Abs. 1 DSGVO sicherzustellen, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Der vom Verordnungsgeber vorgesehene hohe Bußgeldrahmen dient dem Ziel einer einheitlichen und konsequenten Durchsetzung der Vorschriften der DSGVO in der gesamten Europäischen Union (vgl. Erwägungsgründe 129 und 148 zur DSGVO)

und ist auch Ausdruck der enormen wirtschaftlichen Bedeutung der Verarbeitung personenbezogener Daten.

Der HmbBfDI hat wegen des Verstoßes ein Bußgeld im mittleren vierstelligen Bereich verhängt. Die im Verhältnis zur Bußgeldobergrenze vergleichsweise geringe Bußgeldhöhe ist mehreren Faktoren geschuldet, die in diesem Fall zu Gunsten des Unternehmens zu berücksichtigen waren. So hat der HmbBfDI insbesondere berücksichtigt, dass der Verstoß auf den Bearbeitungsfehler eines einzelnen Beschäftigten zurückzuführen ist und kein systematischer Mangel bei der Bearbeitung von Widersprüchen gegen Direktwerbung vorliegt. Ferner hat das Unternehmen die Umsetzung weiterer organisatorischer Maßnahmen zugesichert, um zukünftig auch Bearbeitungsfehler einzelner Beschäftigter verhindern zu können. Auch dies wurde mildernd berücksichtigt. Schließlich wurde zu Gunsten des Unternehmens gewertet, dass es bislang nicht wegen ähnlicher Verstöße in Erscheinung getreten ist und sich im weiteren Verlauf des Verfahrens kooperativ gezeigt hat.

Das Unternehmen hat die Geldbuße akzeptiert und keinen Einspruch eingelegt.

3. Videmo

Anlässlich der Ermittlungen zu den G20-Ausschreitungen wurde durch die Polizei eine automatisierte Gesichtserkennungssoftware eingesetzt, für deren Nutzung eine Datenbank mit einem wachsenden Umfang von anfänglich 17 Terabyte angelegt wurde. In diese Datenbank sind von Bürgerinnen und Bürgern bei der Polizei hochgeladene private Aufnahmen, polizeieigenes Videoüberwachungsmaterial sowie Material aus öffentlichen Verkehrsmitteln und aus den Medien – insgesamt ca. 32.000 Video- und Bilddateien (Stand August 2018) – eingeflossen.

Die in den Bild- und Videodateien enthaltenen Gesichtsmerkmale wurden per Gesichtserkennungssoftware eindeutigen Identifikatoren in Form individueller Gesichts-IDs zugeordnet und maschinenlesbar vorgehalten. Über diesen Datenbestand werden seither Gesichter einzelner Tatverdächtiger immer wieder automatisiert abgeglichen.

Durch dieses Verfahren wird erheblich in die Rechte und Freiheiten einer Vielzahl Betroffener eingegriffen. Die biometrische Erfassung erfolgt zunächst unterschieds- und anlasslos. Sie betrifft massenhaft Personen, die nicht tatverdächtig sind und dies zu keinem Zeitpunkt waren. Die Berechnung von mathematischen Gesichtsmodellen zu Strafverfolgungszwecken geschieht ohne Kenntnis der Betroffenen und ermöglicht der Polizei, Profile über Standort, Verhalten und soziale Kontakte von Personen über einen örtlich und zeitlich nicht näher festgelegten Zeitraum zu erstellen, zu verknüpfen und auszuwerten. Ins Blaue hinein vorgenommene Abgleiche mit Referenzdatenbeständen sind möglich. Unbekannte Personen, etwa auf Demonstrationen, werden durch Referenzdatenbestände, etwa auf sozialen Netzwerken, jederzeit identifizierbar.

Betroffene können sich nicht mit einem Rechtsbehelf wehren, da sie hiervon keine Kenntnis haben. Verwechslungen von Personen, sog. False Positives, sind möglich. Kontrollen durch unabhängige Stellen laufen ohne Melde- und Informationspflichten ins Leere, da für der-

artige Datenbanken keine besonderen gesetzlichen Vorgaben existieren. Ein Richtervorbehalt zur Anordnung und Begrenzung solcher Maßnahmen besteht nicht.

Der HmbBfDI hat die Polizei dazu angehört und danach das Vorgehen gegenüber dem Innensenator beanstandet. Als die Praxis daraufhin nicht geändert wurde, hat der HmbBfDI mit Bescheid vom 18.12.2018 die Löschung der Template-Datenbank angeordnet. Hiergegen hat die Innenbehörde am 14.1.2019 Klage erhoben.

Am 23.10.2019 fand vor dem Verwaltungsgericht Hamburg die mündliche Verhandlung statt. In dieser wurde zunächst das genaue Vorgehen von Polizei und Staatsanwaltschaft herausgearbeitet. Dabei zeigten sich erhebliche Defizite im Hinblick auf technische und organisatorische Maßnahmen, wie zum Beispiel unbegrenzte Speicherfristen und mangelhaften Verfahrensdokumentationen. Auch das Gericht schien erhebliche Zweifel an der Rechtmäßigkeit der Datenverarbeitung zu haben. Zur Überraschung aller Anwesenden wirkten sich diese Mängel im Ergebnis aber nicht aus. Das Gericht verkündete am gleichen Tag sein Urteil und gab der Klage der Innenbehörde darin statt. Da die schriftlichen Urteilsgründe zu Redaktionsschluss im Dezember 2019 noch nicht vorlagen, kann hier nur auf die mündliche Urteilsbegründung und die dazu ergangene Pressemitteilung des VG Hamburg Bezug genommen werden.

Das Gericht kam wohl zu der Erkenntnis, dass § 48 BDSG als hinreichende Rechtsgrundlage die Datenverarbeitung der Polizei rechtfertigt. Daran hatte und hat der HmbBfDI nicht zuletzt aufgrund der mangelnden Bestimmtheit der Norm für massenhafte Abgleiche von Gesichtern und nach Maßgabe des Verhältnismäßigkeitsprinzips vor dem Hintergrund der Schwere der Grundrechtseingriffe erhebliche Zweifel. Das Gericht war der Ansicht, der HmbBfDI sei gar nicht dazu befugt, zu überprüfen, ob im vorliegenden Fall eine Rechtsgrundlage für die Datenverarbeitung vorliege, da eine solche Kompetenz gesetzlich nicht geregelt sei. Dies sei vielmehr eine verfassungsrechtliche Frage, deren Klärung dem BVerfG vor-

behalten bleibe. Der HmbBfDI habe nur die Anwendbarkeit einfachen Rechts zu überprüfen.

Diese Argumentation begegnet grundsätzlichen rechtsdogmatischen Zweifeln. Im Bereich des Datenschutzrechts gilt der Grundsatz, dass Daten nicht verarbeitet werden dürfen, ohne dass die Voraussetzungen einer einschlägigen Rechtsgrundlage erfüllt sind. Danach ist eine Verarbeitung von Daten, die ohne Rechtsgrundlage erfolgt – zumal wenn dies durch öffentliche Stellen erfolgt – grundsätzlich unzulässig. Die Frage nach einer unzulässigen Verarbeitung von personenbezogenen Daten fällt in die Prüfungskompetenz der Aufsichtsbehörden. Das gilt auch und gerade für das Bestehen einer Rechtsgrundlage für einen Eingriff in die Grundrechte. Ausgangspunkt der Überprüfung der Datenverarbeitung der Polizei war nicht etwa die fehlende Verfassungsmäßigkeit von § 48 BDSG, wofür in der Tat das Bundesverfassungsgericht zuständig wäre. Vorliegend ging es hingegen um die Frage, ob die Verarbeitung der Daten, wie sie konkret durch die Polizei Hamburg erfolgt, von einer Rechtsnorm legitimiert wird und somit die einfachgesetzliche Anforderung des Datenschutzrechts erfüllt ist. In den Prozess der Normauslegung und -prüfung in Bezug auf einen bestimmten Sachverhalt fließen dabei naturgemäß verfassungsrechtliche Aspekte wie der Bestimmtheitsgrundsatz und der Grundsatz der Verhältnismäßigkeit ein. Hierzu hat der HmbBfDI in seiner Anordnung umfassende Ausführungen zu allen in Betracht kommenden Rechtsgrundlagen, insbesondere zu § 48 BDSG gemacht, ohne dass dies jedoch inhaltlich Gegenstand der mündlichen Verhandlung wurde.

Durchaus erstaunlich ist zudem die Erkenntnis des Gerichts, dass die Rechtsfragen derartig eindeutig seien, dass eine Berufung nicht zuzulassen sei. Hier wird verkannt, dass eine massenhafte Speicherung von Gesichtsprofilen, gerade auch unbeteiligter Bürgerinnen und Bürger zum Zweck der Strafverfolgung rechtlich kontroverse Fragen mit erheblicher Tragweite für die Rechte und Freiheiten von betroffenen Personen aufwirft. Zudem ist es die erste Entscheidung dieser Art zur Anwendbarkeit von § 48 BDSG in ganz Deutschland.

Nach Vorliegen der Urteilsgründe wird der HmbBfDI sehr zügig darüber befinden, die Zulassung zur Berufung zu beantragen.

Es ist positiv hervorzuheben, dass das Verwaltungsgericht, das betonte, nicht über die Rechtmäßigkeit der Verarbeitung der Gesichtsprofile in der Datenbank durch die Polizei zu entscheiden, in der mündlichen Verhandlung dennoch auf den tatsächlichen Einsatz der Software zu sprechen kam. Insoweit hat es auf Versäumnisse verwiesen, die sich nicht auf die fehlende Rechtsgrundlage, also das „Ob", sondern auf das „Wie" der Durchführung bezogen. Obwohl diese Aspekte eigentlich nicht zum Streitgegenstand gehören, wurden die aufgeworfenen Bedenken des Gerichts vom HmbBfDI aufgenommen. Das betrifft zum einen die fehlende sog. Errichtungsanordnung nach § 490 StPO genauso wie zum anderen eine fehlende Verschriftlichung der Absprachen zwischen Polizei und Staatsanwaltschaft bezüglich des Einsatzes der Software. Die Polizei hatte in der mündlichen Verhandlung auf Nachfrage des Gerichts mitgeteilt, dass bei einem Zugriff auf Videmo zum Zwecke des Abgleichs von Gesichtern keine automatische Protokollierung erfolgt, sondern vielmehr die Nutzung der Software händisch vermerkt werde. Letztlich wird somit keine revisionssichere Dokumentation erzeugt, eine effektive datenschutzrechtliche Kontrolle der Zugriffe auf die gespeicherten Daten ist damit nicht möglich.

Bis zum Redaktionsschluss wurden die Mängel nicht von der Polizei behoben. Insbesondere hinsichtlich der von dem Gericht kritisierten fehlenden technischen Protokollierung beim Einsatz der Software hat der HmbBfDI die Polizei aufgefordert, eine technische Lösung zu entwickeln bzw. das technisch Mögliche in dieser Sache zumindest aufzuzeigen. Dies ist trotz mehrmaliger Nachfrage bislang nicht erfolgt. Auch aus diesem Grund bleibt die Zulässigkeit jedenfalls des Einsatzes der konkreten Software bis auf Weiteres zweifelhaft. Der HmbBfDI wird in diesen Fragen auf Klärung bestehen.

4 Anweisung zur Beschränkung der Videoüberwachung in einer Shisha-Bar

Gastronomen, die in ihren Räumlichkeiten Beschäftigte und Gäste in einer rechtswidrigen Weise videoüberwachen, müssen mit einer Beschränkungsanordnung und der Festsetzung eines Zwangsgelds rechnen.

Durch eine Beschwerde wurde der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) auf die Videoüberwachung einer Shisha-Bar aufmerksam. In den Räumen und im Außenbereich der Bar waren 17 Kameras installiert. Dies führte zu einer nahezu lückenlosen Videoüberwachung des gesamten Betriebs. Auch die Sitzbereiche für Gäste wurden umfassend überwacht.

Eine Videoüberwachung ist nach höchstrichterlicher Rechtsprechung nur dann erforderlich, wenn in Bezug auf die beobachteten Räume eine erheblich über das allgemeine Lebensrisiko hinausgehende Gefährdungslage besteht. Eine solche Gefährdungslage konnte der Geschäftsführer nicht belegen, er hatte dies auch gar nicht behauptet. Aus den zur Verfügung gestellten Informationen ergaben sich keine hinreichenden Gründe, die einen Betrieb der Videoüberwachungsanlage während der Geschäftszeiten rechtfertigen konnten. Bei allen vorgebrachten Argumenten für die Durchführung der Videoüberwachung handelte es sich um typische Gefahren beim Betrieb einer Bar. Genügte dies für die vorgefundene, umfassende Videoüberwachung, so gäbe es in der ganzen Europäischen Union kaum noch unüberwachte gastronomische Betriebe. Das Verhältnis muss nach dem gesamten Konzept des europäischen Datenschutzrechts aber gerade umgekehrt sein: Die Videoüberwachung ist der zu rechtfertigende Ausnahmefall. Für das Eintreten dieses Ausnahmefalls bedarf es entweder eines abstrakt besonders gefährdeten Betriebs (zum Beispiel Juwelier oder Tankstelle) oder eines konkret durch Straftaten besonders betroffenen Betriebs. Beides war vorliegend nicht gegeben. Es handelte sich mit Blick auf die geschilderten

Vorfälle und Probleme mit den Beschäftigten und Gästen um eine ganz gewöhnliche Bar.

Der HmbBfDI teilte dem Geschäftsführer daher mit, dass die Videoüberwachung der Shisha-Bar während der Geschäftszeiten unzulässig sei und bat um Mitteilung, ob die Videoüberwachung datenschutzkonform auf die Zeit beschränkt werde, zu der die Bar geschlossen sei oder weiterhin ein durchgehender Betrieb beabsichtigt sei. Eine Rückmeldung des Geschäftsführers zu dieser Frage blieb aus. Er äußerte sich auch nicht zu der Anhörung des HmbBfDI, die nach § 28 Verwaltungsverfahrensgesetz vor dem Erlass eines Verwaltungsakts, der in die Rechte eines Beteiligten eingreift, durchzuführen ist. Aufgrund dieses unkooperativen Verhaltens hat der HmbBfDI von seiner Abhilfebefugnis gemäß Art. 58 Abs. 2 lit. f Datenschutzgrundverordnung (DSGVO) Gebrauch gemacht und das Unternehmen angewiesen, während der Geschäftszeiten der Bar keine personenbezogenen Daten der Gäste und Beschäftigten durch Videoüberwachung der Räume der Bar und dem dazugehörenden Außenbereich zu verarbeiten. Das Unternehmen wurde ferner aufgefordert, die Maßnahme innerhalb von zwei Wochen nach Bestandskraft des Bescheids umzusetzen und die Umsetzung gegenüber dem HmbBfDI nachzuweisen.

Das Unternehmen hat die Anweisung des HmbBfDI ignoriert und den Nachweis nicht erbracht. Es hat auch keine Klage gegen die Anweisung vor dem Verwaltungsgericht erhoben oder auf andere Weise versucht, Kontakt mit dem HmbBfDI aufzunehmen. Zur Durchsetzung der Anweisung hat der HmbBfDI schließlich ein Zwangsgeld im mittleren vierstelligen Bereich festgesetzt.

5. Google Suchmaschine – Neue Rechtsprechung von EuGH, BVerfG und OVG Hamburg

Fälle rund um das Auslisten von Suchergebnissen aus Suchmaschinen betreffen einen sehr persönlichen Bereich des Datenschutzrechts. Die Sachverhalte sind häufig emotional aufgeladen, so dass die gerichtliche Auseinandersetzung gesucht wird.

Mit der Datenschutzgrundverordnung (DSGVO) wurde festgelegt, dass Personen einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde haben. Die Praxis zeigt, dass bei Entscheidungen, die die namensbezogene Auffindbarkeit von Google-Suchergebnissen betreffen, von diesem Instrument in Form von Klagen vor dem Verwaltungsgericht wiederholt Gebrauch gemacht wird. Der HmbBfDI war zuletzt an zwei Verfahren vor dem Hamburgischen Oberverwaltungsgericht (OVG) beteiligt (5 Bf 279/17 und 5 Bf 291/17). Zwar fanden diese Verfahren ihren Ursprung vor Inkrafttreten der DSGVO, doch zogen sich die Berufungsverfahren so lange hin, dass zwischenzeitlich das Recht sich stark verändert hatte. In der Konsequenz hat das OVG zwei Entscheidungen zum Recht auf Vergessenwerden gefällt, welches in Art. 17 DSGVO umgesetzt wurde. Diese zeigen, dass das Recht auf Vergessenwerden in Bezug auf die Auslistung von Google-Suchergebnissen auch im fünften Jahr nach dessen Erschaffung durch den Europäischen Gerichtshof (EuGH) noch immer grundlegende Fragen aufwirft.

Schwierigkeiten bereitet bereits die Frage, ob der HmbBfDI als zuständige Aufsichtsbehörde tätig werden kann. Während innerhalb Deutschlands diese Zuständigkeit aufgrund des hamburgischen Firmensitzes der Google Germany GmbH besteht, stellt sich im europäischen Kontext die Frage, ob nicht die Google Ireland Limited als Hauptniederlassung i.S.v. Art. 4 Nr. 16 DSGVO agiert, so dass alle Auslistungsfälle eigentlich in den Zuständigkeitsbereich der irischen Aufsichtsbehörde fielen. Das OVG tendierte in diese Richtung,

musste jedoch keine abschließende Entscheidung treffen. Denn aufgrund der Regelung aus Art. 56 Abs. 2 DSGVO kann der HmbBfDI über „lokale Fälle“ in eigener Zuständigkeit entscheiden. Es besteht eine Vereinbarung mit der irischen Aufsichtsbehörde, dass Fälle, bei denen es sich um deutschsprachige Suchergebnisse handelt, die Vorgänge aus Deutschland beschreiben, jedenfalls keiner Unterrichtung nach Irland bedürfen. Dies ist in hohem Maße sachgerecht, da eine materielle und rechtliche Würdigung dieser Fälle nur bei Kenntnis der spezifischen inländischen Umstände gelingen kann.

Im Kontext der jetzigen Rechtsprechung ist der HmbBfDI jedoch angehalten, Fälle, in denen es bspw. um fremdsprachige Suchergebnisse geht, immer der irischen Behörde zur Entscheidung vorzulegen. Hier steht eine europäische Abstimmung bevor, da die Frage von Googles Hauptniederlassung für Auslistungsfälle europaweit nicht einheitlich gesehen wird. Insbesondere hält sich die irische Aufsichtsbehörde mittlerweile für nicht mehr zuständig.

Das OVG hat zudem weitreichend die zivilrechtliche Rechtsprechung des Bundesgerichtshofs und diverser Oberlandesgerichte übernommen, die in diesen Fällen zur Reichweite der Abwehransprüche aus Persönlichkeitsrechten im Konflikt zur Meinungs- und Informationsfreiheit erarbeitet wurde. Der Hintergrund ist, dass bei einer verwaltungsgerichtlichen Klage gegen den HmbBfDI kein weitreichenderer Anspruch bestehen soll, als wenn gegen den verantwortlichen Suchmaschinenbetreiber im Zivilrechtswege vorgegangen würde. So führt dies zu einer Vereinheitlichung der Rechtsprechung. Beide Berufungen der Beschwerdeführer wurden zurückgewiesen. In einem Fall ist eine Nichtzulassungsbeschwerde beim Bundesverwaltungsgericht anhängig.

Grundlegende Fragen klärten 2019 auch der Europäische Gerichtshof (EuGH) und das Bundesverfassungsgericht (BVerfG). Der EuGH entschied am 24. September 2019, dass die Google LLC bei Auslistungsersuchen von EU-Bürgern Links aus der Ergebnisliste grundsätzlich nicht weltweit, sondern nur in allen EU-Versionen

der Suchmaschine blockieren muss (C-507/17). Zusätzlich muss der Suchmaschinenbetreiber mittels Geoblockings Internetnutzer aus EU-Staaten davon abhalten, auf die entsprechenden Links in Nicht-EU-Versionen der Suchmaschine zuzugreifen. Links zu Informationen mit sensiblen personenbezogenen Daten dürfen, so der EuGH in einer weiteren Entscheidung, nur dann nach einem Auslistungsantrag in den Suchergebnissen bleiben, wenn sie für die Informationsfreiheit der Internetnutzer unbedingt erforderlich sind (C-136/17). Bei Berichten über Straftaten gab der EuGH dem Suchmaschinenbetreiber dabei Kriterien für eine umfangreiche Abwägung vor. Muss keine Auslistung erfolgen, so muss Google zumindest die Ergebnisliste so ausgestalten, dass an erster Stelle der aktuelle Stand des Gerichtsverfahrens wiedergegeben wird.

In den beiden vom BVerfG am 06. November 2019 entschiedenen Fällen wurden die vom BVerfG angeforderten Stellungnahmen des HmbBfDI bestätigt. Das BVerfG erwog in seiner Entscheidung „Recht auf Vergessen I“ (1 BvR 16/13) ein solches Recht nicht nur gegenüber dem Betreiber der Suchmaschine, sondern auch gegenüber dem Inhalteanbieter. Nach dem BVerfG ist auch bei ursprünglich rechtmäßiger Berichterstattung eines Nachrichtenmagazins zu Mordfällen aus 1981 zu prüfen, welche zumutbaren technischen Möglichkeiten seinem Online-Archiv zustehen, die Auffindbarkeit der Beiträge über die Namenssuche des Straftäters in der Google Suchmaschine zu verhindern. Keine Verletzung von Grundrechten sah das BVerfG dagegen durch die Ablehnung der Auslistung eines Links zum 2010 veröffentlichten Pressebeitrag „Die fiesen Tricks der Arbeitgeber“ aus den Google-Suchergebnissen zum Namen einer Geschäftsführerin („Recht auf Vergessen II“ - 1 BvR 276/17).

Die in den Entscheidungen aufgestellten Grundsätze, mit denen die Gerichte das Recht auf Vergessenwerden konkretisieren, dienen dem HmbBfDI als Leitlinien bei der Prüfung von Beschwerden gegen die Ablehnung von Auslistungsersuchen durch Suchmaschinenbetreiber wie Google. Der HmbBfDI ist zudem regelmäßig in Kontakt mit anderen europäischen Datenschutzbehörden und den gemein-

samen europäischen Datenschutzgremien. Der Europäische Datenschutzausschuss EDSA hat am 02. Dezember 2019 einen ersten Teil von Leitlinien zu den Kriterien für das Recht auf Vergessenwerden in Suchmaschinen verabschiedet, die eine Auslegung von Art. 17 DSGVO bieten (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf). Weitere Leitlinien sollen zum Umgang mit Beschwerden gegen abgelehnte Auslistungsersuchen erarbeitet werden.

Vor dem Verwaltungsgericht Hamburg sind derzeit vier Klagen anhängig, in denen die Kläger begehren, den HmbBfDI zu verpflichten, gegenüber der datenschutzrechtlich verantwortlichen Google LLC die Entfernung von Suchergebnissen anzuordnen. Über die Klagen wird voraussichtlich 2020 entschieden.

6. BUSSGELD GEGEN FACEBOOK WEGEN UNTERLASSENER MITTEILUNG ÜBER DEN DATENSCHUTZBEAUFTRAGTEN IN DEUTSCHLAND

Werden wirksam bestellte Datenschutzbeauftragte nicht bei der zuständigen Aufsichtsbehörde gemeldet, drohen Bußgelder.

Durch eine Beschwerde wurde der HmbBfDI im März 2019 darauf aufmerksam, dass die Facebook Germany GmbH keinen Datenschutzbeauftragten gemeldet hatte. 2017 war der Aufsichtsbehörde mitgeteilt worden, dass die damalige Datenschutzbeauftragte das Amt nicht weiter ausführte. Die Mitteilung über einen neuen Datenschutzbeauftragten war jedoch nicht erfolgt. Dies ist nach Art. 37 Abs. 7 DSGVO jedoch verpflichtend vorgesehen. Verstöße gegen diese Vorgabe sind nach Art. 83 Abs. 4 lit a) DSGVO bußgeldbewehrt.

Auf Nachfrage bestätigte die Facebook Germany GmbH, dass keine Mitteilung bei der für dieses Unternehmen zuständigen hamburgischen Aufsichtsbehörde erfolgt war. Mit Wirksamwerden der DSGVO sei das in Irland ansässige Datenschutzteam der Hauptniederlassung für alle europäischen Töchterunternehmen als Datenschutzbeauftragter benannt worden. Man habe dies aber nicht in Hamburg gemeldet. Im Rahmen eines vom HmbBfDI eingeleiteten Bußgeldverfahrens meldete Facebook in verschiedener Hinsicht rechtliche Zweifel daran an, dass es sich dabei um einen bußgeldbewehrten Verstoß gehandelt habe. Die rechtlichen Argumente Facebooks betrafen zum Beispiel die Frage, ob die rein deutsche Pflicht zur Benennung ab 10 bzw. 20 Beschäftigten überhaupt wirksam war sowie die teilweise unzureichende Umsetzung der europäischen Vorgaben durch das nationale Verfahrensrecht. So ist in der rechtswissenschaftlichen Literatur umstritten, ob nach deutschem Recht fahrlässige Verstöße, ohne dass eine fahrlässige Begehung im Tatbestand ausdrücklich vorgesehen ist, überhaupt bußgeldbewehrt sind, auch wenn das europäische Recht dies zweifellos fordert. Ferner versteht sich das europäische Recht als reines Unternehmenssanktionsrecht. Verstöße von Beschäftigten sind stets dem Unternehmen zuzurechnen, sofern nicht ein echter Exzess vorliegt und der Beschäftigte ausschließlich im Eigeninteresse handelt. Nach dem deutschen Recht können Verstöße aber nur unter bestimmten Voraussetzungen dem Unternehmen zugerechnet werden. Das Auseinanderklaffen von deutschem und europäischem Recht wird von niemandem ernstlich bestritten. Es ist aber noch nicht abschließend gerichtlich geklärt, welches Recht gelten soll.

Dem HmbBfDI sind diese Argumente bekannt, dies kann aber nicht zu einer Passivität aufgrund von Rechtsunsicherheit führen, wenn der HmbBfDI einen Verstoß festgestellt hat. Die offenen Rechtsfragen werden nur gerichtlich geklärt werden können. Es wurde daher ein Bußgeld in Höhe von 51.000 € gegen die Facebook Germany GmbH erlassen. Das Bußgeld mag auf den ersten Blick niedrig klingen. Es ergeht aber nicht gegen den milliardenschweren Mutterkonzern, sondern gegen die deutsche Tochter wegen eines ausschließlich in

Deutschland begangenen und geregelten Verstoßes gegen die Mitteilungspflicht. Die Facebook Germany GmbH ist ein Unternehmen mit einem Jahresumsatz von rund 35 Millionen, dessen Schwerpunkt – im Gegensatz zum Mutterkonzern – nicht in der Verarbeitung personenbezogener Daten liegt und das nach außen kaum auftritt. Das Bußgeld dürfte angesichts der Fahrlässigkeit des Verstoßes und der Tatsache, dass Facebook den Verstoß sofort abgestellt hat und durchgehend ein Datenschutzbeauftragter bestellt war, der lediglich nicht mitgeteilt wurde, als empfindlich anzusehen sein.

Dieser Fall sollte allen anderen Unternehmen eine deutliche Warnung sein: Die Benennung des Datenschutzbeauftragten und die Mitteilung an die Aufsichtsbehörde sind Pflichten, die die DSGVO ernst nimmt. Schon kleinere Verstöße gegen derartige Pflichten können zu nicht unerheblichen Geldbußen führen. Es ist dem umsichtigen und professionellen Umgang Facebooks mit dem Verstoß geschuldet, dass die Geldbuße nicht noch deutlich höher ausfiel.

7. ÜBERSICHT GERICHTSVERFAHREN

Seit Wirksamwerden der DSGVO ist der HmbBfDI an über 20 Gerichtsverfahren aktiv beteiligt, ausschließlich als Beklagter. In einigen Fällen wurden Klagen gegen seine Bescheide eingereicht, in vielen anderen Fällen wurde er verklagt, weil Beschwerdeführer mit seinen Entscheidungen nicht einverstanden waren.

Vor Inkrafttreten der DSGVO waren Beschwerden bei der Behörde als „Eingaben“ anzusehen und nach dem Petitionsrecht zu behandeln. Hiergegen gibt es eindeutig keinerlei Rechtsbehelf bei einer Ablehnung. Ob sich diese Rechtsauffassung nach dem Wirksamwerden der DSGVO so fortsetzen lässt, konnte mit gutem Grund bezweifelt

werden. Der HmbBfDI hat deshalb seine ablehnenden Entscheidungen stets mit einer Rechtsbehelfsbelehrung versehen, auch wenn eine § 37 Abs. 6 VwVfG entsprechende Pflicht im HmbVwVfG nicht existiert. Diese Rechtsbehelfsbelehrung haben viele Adressaten anscheinend als Aufforderung verstanden. In zahlreichen Fällen wurden Klagen gegen seine Bescheide erhoben. Mehrere Klagen waren von vornherein vollkommen aussichtslos, wie auch jeder Nicht-Jurist hätte erkennen können. Es ist selbstverständlich das gute Recht, eines jeden Betroffenen, einen zulässigen Rechtsbehelf zu ergreifen. In diesen Fällen wäre es jedoch nur zusätzliche Arbeit für den HmbBfDI und vermeidbare Kosten für die Klägerinnen und Kläger.

Bei zahlreichen anderen Fällen handelt es sich um Verfahren zum Google-Delisting, in denen der HmbBfDI keinen Anspruch gegen Google erkennen konnte und der Ansicht war, dass Google die Anträge zu Recht abgelehnt hatte. Was die Betroffenen dazu bewogen hat, Klagen gegen den HmbBfDI einzulegen, anstatt direkt gegen Google vorzugehen, ist unbekannt. Es lässt sich dazu nur sagen, dass dies ein umständlicherer Weg ist, der deutlich weniger Erfolg verspricht. Während es erfolgreiche Urteile von Zivilgerichten gegen Google gibt, hat der HmbBfDI bislang jeden Fall gewonnen, in dem er zu der Ansicht gelangte, dass die Anträge auf Delisting von Google zu Recht abgelehnt wurden (vgl. Kap. IV.6).

Insgesamt herrscht deutschlandweit noch erhebliche Rechtsunsicherheit im Hinblick auf die Frage, ob und wenn ja, in welchem Umfang, überhaupt Ansprüche gegen Datenschutzbehörden auf ein Einschreiten bestehen. Die DSGVO hat sich hier – wie an vielen anderen Stellen – ins Vage zurückgezogen. Es ergehen deswegen unterschiedlichste Urteile mit unterschiedlichsten Begründungen. Während in Berlin weiterhin von einem Petitionsrecht ausgegangen wird, geht ein bayerisches Gericht von einer Ermessensentscheidung aus. Das entspricht zwar der bekannten deutschen Dogmatik, dürfte aber einer europaweiten Vereinheitlichung im Weg stehen. Das OVG Hamburg hat sich mit der Frage zwar intensiv auseinandergesetzt, aber ausdrücklich erklärt, sich (noch) nicht eindeutig festlegen zu

wollen. Hier wird noch abzuwarten sein, wie sich das OVG Hamburg endgültig positioniert oder bis das Bundesverwaltungsgericht entscheidet.

Der HmbBfDI ist auch in zwei Fällen verklagt worden, weil er ein bestimmtes Vorgehen verboten hat. Über die für der Polizei eingesetzte Software zur Gesichtsanalyse wird an anderer Stelle berichtet (Kap. IV.4). Ein anderes Verfahren begleitet die Behörde seit Jahren. Der HmbBfDI hatte einem Betrieb für Autowaschdienstleistungen die seiner Auffassung nach extensive Videoüberwachung der eigenen Beschäftigten untersagt. Der Fall geht auf eine Beschwerde aus dem Jahr 2013 zurück. Obwohl das Gericht bereits im Juni 2017 eine mündliche Verhandlung durchführte, gibt es bislang keine Entscheidung. Der HmbBfDI hat bereits im vorletzten Tätigkeitsbericht von dem Fall berichtet (TB 2016/2017, Kap. IV.1), die Parteien warten aber immer noch auf eine Entscheidung. Inzwischen hat sich das anwendbare Recht (eventuell) geändert und das Unternehmen ist verkauft worden. Das für November 2017 in Aussicht gestellte Urteil ist hingegen leider immer noch nicht ergangen.

V. BERATUNGEN UND DATENSCHUTZ-KOMMUNIKATION

1. Novellierung des PolDVG und des HmbVerfSchG

Die Behörde für Inneres und Sport (BIS) hat im Berichtszeitraum sowohl ihre Entwürfe zur Novellierung des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) als auch zum Hamburgischen Verfassungsschutzgesetz (HmbVerfSchG) vorgelegt. Beide Regelungswerke beinhalten erhebliche Änderungen im Bereich des Datenschutzes. Der HmbBfDI hat die Entwürfe trotz sehr kurzer Beteiligungsfristen einer kritischen datenschutzrechtlichen Prüfung unterzogen.

Im Sommer 2019 erreichten den HmbBfDI im Rahmen zweier Drucksachenabstimmungen sowohl Entwürfe der BIS für ein grundlegend überarbeitetes PolDVG, sowie ein HmbVerfSchG. Die BIS hatte sich insbesondere mit der Überarbeitung des PolDVG Zeit gelassen: So war die europäische Richtlinie, deren Umsetzung die Überarbeitung dienen sollte, bereits seit drei Jahren erlassen worden und die Umsetzungsfrist bereits seit einem Jahr abgelaufen. Nicht zuletzt auch deshalb war der HmbBfDI überrascht, dass ihm im Zuge der Drucksachenabstimmung äußerst kurze Fristen von sieben (PolDVG) bzw. zehn (HmbVerfSchG) Werktagen zur Stellungnahme eingeräumt wurden, obwohl derartige Beteiligungsfristen grundsätzlich angemessen auszugestalten sind. Hiervon konnte angesichts des Umfangs und der Komplexität der geregelten Materie nicht ausgegangen werden. Der HmbBfDI hat daher die Gelegenheit genutzt, sich sowohl im Rahmen der im Innenausschuss der Bürgerschaft durchgeführten Expertenanhörungen, als auch im Rahmen der Senatsanhörungen in den Gesetzgebungsprozess miteinzubringen.

Beide Stellungnahmen des HmbBfDI sind auf der Website unter https://datenschutz-hamburg.de/assets/pdf/Stellungnahme_HmbBfDI_polizeirechtliche_Vorschriften_2019-06-24.pdf, https://datenschutz-hamburg.de/assets/pdf/Stellungnahme_HmbBfDI_HmbVerfSchG-Novellierung_2019-07-22.pdf.

1.1 PolDVG-Novelle

Grund für die im Juni 2019 in die behördliche Drucksachenabstimmung eingebrachte und am 4. Dezember 2019 von der Bürgerschaft angenommene Novellierung des PolDVG war ganz überwiegend die Umsetzung der Europäischen Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (sog. JI-Richtlinie), die grundsätzlich bis zum 6. Mai 2018 hätte erfolgen müssen. Erst im Juni 2019 legte die BIS jedoch mit dem Entwurf zum PolDVG ein Regelungswerk aus dem Bereich des Gefahrenabwehrrechts vor, das neben diesen dringend vorzunehmenden Umsetzungen auch den nicht weniger dringenden Anpassungen an die Vorgaben des Bundesverfassungsgerichts aus dem sog. BKAG-Urteil (Urteil v. 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) diente. Das höchste deutsche Gericht hatte in seiner Entscheidung bezüglich der besonders eingriffsintensiven verdeckten Überwachungsmaßnahmen durch die Polizei datenschutzrechtlich bedeutsame Vorgaben im Hinblick auf Verfahrensausgestaltung, Eingriffsschwellen sowie Bestimmtheit von Normen getroffen. Es galt daher für den HmbBfDI zu prüfen, ob das umfassend novellierte Gesetz sowohl den europarechtlichen Anforderungen, als auch den nationalen verfassungsrechtlichen Vorgaben gerecht geworden ist.

Obwohl der Entwurf im Hinblick auf die Umsetzung der JI-Richtlinie und der Judikatur des Bundesverfassungsgerichts in vielen Aspekten als gelungen und moderat bezeichnet werden kann, mussten vom HmbBfDI einige datenschutzrechtliche Defizite aufgezeigt werden:

- Der HmbBfDI hatte zunächst kritisiert, dass der Entwurf an unterschiedlichen Stellen die Möglichkeit eröffnet, die Verarbeitung von personenbezogenen Daten durch die Polizei auf eine Einwilligung des Betroffenen zu stützen. Bereits aus unionsrechtlichen Gründen ließ sich daran zweifeln, ob die JI-Richt-

linie überhaupt Raum für eine Einwilligung überließ. Zweifel bestanden aufgrund des zwischen den Akteuren bestehenden Ungleichgewichts (Staat – Bürger) und damit an der Freiwilligkeit einer solchen Einwilligung. Es konnte erreicht werden, dass zumindest im Bereich der Verarbeitung von besonderen Kategorien personenbezogener Daten (vgl. § 4 PolDVG) die Einwilligung als Grundlage der Verarbeitung wieder aus dem Entwurf entfernt wurde.

- Datenschutzrechtliche Bedenken, denen nicht abgeholfen wurde, hat der HmbBfDI auch hinsichtlich der Ausgestaltung der neu eingeführten elektronischen Aufenthaltsüberwachung in § 30 PolDVG (sog. elektronische Fußfessel) angebracht. Denn hier handelt es sich um eine Maßnahme, die eine besonders intensive Auswirkung auf die Grundrechtsausübung des Betroffenen hat. Daher war es nicht verwunderlich, dass auch im Rahmen der Expertenanhörung durch die Bürgerschaft der überwiegende Teil der Experten auf dem Gebiet des Polizeirechts, wie der HmbBfDI, die niedrige Eingriffsschwelle der Norm kritisiert haben. Entgegen des Anratens des HmbBfDI, wonach der Einsatz der Fußfessel entweder auf die Gefahr von terroristischen Straftaten oder zumindest einer qualifizierten Gefahrensituation begrenzt werden sollte (vgl. § 56 BKAG), ist die Maßnahme nun theoretisch auch bei jeder Form der Körperverletzung möglich.

- Zweifel bestanden auch bezüglich der Ausgestaltung der in § 35 Abs. 3 S. 2 ff. PolDVG zu findenden sog. Mitziehregel bei der Datenspeicherung in automatisierten Dateisystemen. Diese Regelung verlängert im Falle einer neuen polizeilichen Speicherung die Speicherdauer aller bereits vorhandenen Speicherungen, da sich die (gesamte) Speicherdauer für alle im Übrigen bestehenden Speicherungen nach der längsten richtet. Soweit hierdurch für zeitlich frühere Speicherungen die genannte Höchstprüffrist von 10 Jahren zweimal erreicht wird, ist eine weitere Speicherung dieser personenbezogenen Daten darüber hinaus zulässig, wenn dies wegen besonderer Gründe im Ein-

zelfall erforderlich ist. Man mag hier ein legitimes Bedürfnis der Polizei an einem langfristigen Überblick über die kriminellen Aktivitäten eines Betroffenen anerkennen. Ein pauschales Hinausschieben der Löschung auch bei Delikten im Bagatellbereich oder gänzlich fehlendem Sachzusammenhang/Schweregrad ist aber nicht geboten.

- Durchsetzen konnten sich dagegen zumindest teilweise datenschutzrechtliche Bedenken des HmbBfDI und mehrerer Experten des Polizeirechts an der Ausgestaltung des Entwurfs des § 49 PolDVG. Nach dieser Vorschrift soll der Polizei eine „automatisierte Anwendung zur Auswertung vorhandener Daten" erlaubt sein. Dem ursprünglichen Entwurf dieser Vorschrift fehlte eine Definition der davon erfassten technischen Verfahren, eine Begrenzung im Hinblick auf den zeitlichen Umfang der Maßnahme aber auch prozedurale Absicherungen. Letztlich war nicht ersichtlich, inwieweit hier Technologien aus dem sog. Big-Data-Bereich gerechtfertigt werden sollten. Eine Überarbeitung der Norm als Ergebnis der Beratungen im Innenausschuss, führte zur Aufnahme des Grundsatzes der Erforderlichkeit, sowie einer Beschränkung „auf den Einzelfall". Zudem hat eine Mitteilungspflicht an die Bürgerschaft Eingang in das Gesetz gefunden. Die Vorschrift wird nunmehr rechtstaatlichen Anforderung besser gerecht.

- Für europarechtswidrig und rechtspolitisch verfehlt erachtet der HmbBfDI die nicht vollständige Umsetzung des Art. 47 der JI-Richtlinie in § 72 PolDVG. Aus § 72 PolDVG folgt, dass der HmbBfDI im Bereich des Gefahrenabwehrrechts – anders als im Bereich seiner Aufsicht über die Anwendung der DSGVO – nicht die Möglichkeit haben soll, Anordnungen zur Abhilfe von Verstößen gegenüber der Polizei zu treffen. Er soll lediglich die Datenverarbeitung beanstanden und dann seine eigene Beanstandung gerichtlich feststellen lassen können. Die BIS war bereits innerhalb der Behördenabstimmung darauf hingewiesen worden, dass fraglich ist, ob für derartige Feststellungsklagen

überhaupt eine Klagebefugnis und/oder ein Feststellungsinteresse besteht. Jedenfalls aber handelt es sich um eine unzureichende Umsetzung der JI-Richtlinie. Art. 47 der Richtlinie verlangt vom Gesetzgeber jedes Mitgliedstaates, dass jede Aufsichtsbehörde über wirksame Abhilfebefugnisse verfügt. Ganz überwiegend wird daher vertreten, dass es sich bei dem in Art. 47 JI-Richtlinie genannten Regelbeispiel der Anordnungsbefugnis um eine Mindestvoraussetzung für wirksame Abhilfemaßnahmen handelt und insofern auch kein Umsetzungsspielraum für den nationalen Gesetzgeber besteht. Die wohl hinter der getroffenen Regelung stehende Befürchtung, dass entsprechende Anordnungen die Aufgabenwahrnehmung der Polizei konterkarieren könnten, ist nicht nachvollziehbar, weil dem HmbBfDI die Anordnung einer sofortigen Vollziehung gegenüber der Polizei ohnehin nicht möglich ist. Das bedeutet, dass selbst bei Vorliegen einer Anordnung, die Polizei bis zur endgültigen gerichtlichen Klärung die gegenständliche datenschutzrechtliche Verarbeitung fortführen könnte.

- Schließlich wurden dem HmbBfDI mit § 73 PolDVG weitere gesetzliche Prüfpflichten übertragen, derer er im Abstand von höchstens zwei Jahren nachzukommen hat. Der Sinn derartiger Prüfpflichten steht außer Frage. Der HmbBfDI musste insofern jedoch darauf verweisen, dass die bereits bestehende Aufgabenlast des HmbBfDI mit den vorhandenen personellen Ressourcen kaum bewältigt werden kann.

1.2 HmbVerfSchG-Novelle

Das Recht der Nachrichtendienste ist eine Frage der nationalen Sicherheit und war damit nicht Gegenstand des unter (1.1.) genannten europäischen Datenschutzpakets (vgl. Art. 4 Abs. 2 S. 3 EU-Vertrag). Somit galt es hier nicht, Anforderungen einer europäischen Richtlinie umzusetzen. Mit dem im Juli 2019 im Rahmen der Drucksachenabstimmung vorgelegten Gesetzesentwurf beabsichtigt die BIS aber insbesondere die Anpassung des HmbVerfSchG an die Vorgaben

höchstrichterlicher Rechtsprechung, sowie die Harmonisierung mit anderen Bundes- und Ländergesetzen. Im Fokus stand das bereits erwähnte BKAG-Urteil des Bundesverfassungsgerichts vom 20. April 2016. Obwohl sich das Urteil unmittelbar auf polizeiliche Maßnahmen bezieht, hatte die BIS insofern erkannt, dass es darüber hinaus auch allgemeine Vorgaben für den Bereich der heimlichen Überwachungsmaßnahmen enthält, die zumindest teilweise auch Auswirkungen auf das Recht der Nachrichtendienste haben.

Hier hatte die BIS bereits einigen Bedenken des HmbBfDI im Zuge der Behördenabstimmung Rechnung getragen. Dazu gehörte beispielsweise die Empfehlung, die Besonderheiten der elektronischen Aktenführung durch angemessene Sicherungsmechanismen zu berücksichtigen. Hier hatten sich dem HmbBfDI insofern Bedenken gestellt, als die elektronische Aktenführung gegenüber der herkömmlichen Papierakte ganz neue Nutzungsmöglichkeiten eröffnet, damit für das informationelle Selbstbestimmungsrecht der Betroffenen aber auch höhere Gefahren begründet. Der Entwurf enthält nunmehr sowohl eine Eingrenzung der Abgleichmöglichkeiten als auch die Verpflichtung bei jeder Abfrage zum Zweck der Datenschutzkontrolle eine Protokollierung der Abfrage vorzunehmen und orientiert sich damit an den Regelungen des Bundesverfassungsschutzgesetzes.

Zudem konnte erreicht werden, dass der grundrechtlich geschützte Anspruch auf datenschutzrechtliche Auskunft nicht – wie ursprünglich vorgesehen – davon abhängig gemacht wird, dass der Betroffene einen konkreten Sachverhalt und ein besonderes Interesse darlegt. Eine Notwendigkeit für derartige Beschränkungen des Auskunftsrechts ohne Ermessen war nicht ersichtlich.

Dass die BIS vom ursprünglich gewählten Weg einer Streichung der Beanstandungskompetenz des HmbBfDI Abstand genommen hat, ist eigentlich selbstverständlich. Das vollständige Absehen von Abhilfekompetenzen hätte eine zweifelhafte Privilegierung des Landesamts für Verfassungsschutz gegenüber der Polizei oder anderen öffentlichen Stellen dargestellt, die verfassungsrechtlich nicht geboten ist

und hinter das bislang geltende Recht zurückgefallen wäre. Vielmehr hat das Bundesverfassungsgericht wiederholt die herausgehobene Bedeutung der unabhängigen aufsichtsrechtlichen Kontrolle für den schwach ausgestalteten Individualschutz betont, der heimlichen Überwachungsmaßnahmen immanent ist. Zu bedauern ist dagegen, dass dem HmbBfDI keine Anordnungskompetenz für diesen Bereich übertragen wurde. Der HmbBfDI hatte bereits in der Behördenabstimmung darauf hingewiesen, dass eine solche Befugnis auch gerade deshalb wünschenswert gewesen wäre, weil sie sich letztlich auch positiv auf die Legitimation des Landesamts für Verfassungsschutz ausgewirkt hätte. So handelt es sich hier um einen Bereich, in dem Betroffene nur selten klagen. Eine Anordnungsbefugnis hätte hier die Möglichkeit eröffnet, Maßnahmen des Verfassungsschutzes einer gerichtlichen Klärung zuzuführen.

Der Kritik des HmbBfDI, dass der Entwurf von einer grundsätzlichen nachträglichen Mitteilungspflicht über Maßnahmen zugunsten des Betroffenen absieht, wurde nicht abgeholfen. Heimliche Überwachungsmaßnahmen stellen nach der eingangs erwähnten Rechtsprechung des Bundesverfassungsgerichts in aller Regel einen erheblichen Eingriff in die Grundrechte der Betroffenen dar. Insofern wäre es konsequent gewesen, die Rechtsprechung des Bundesverfassungsgerichts im Hinblick auf die grundrechtssichernde Wirkung von Verfahren hinsichtlich polizeilicher Befugnisse auch auf den Bereich des Verfassungsschutzes zu übertragen. Danach gehört zu den Anforderungen an eine verhältnismäßige Ausgestaltung von heimlich durchgeführten Überwachungsmaßnahmen auch die gesetzliche Anordnung von Benachrichtigungen der Betroffenen. Geheimhaltungsinteressen können im Einzelfall gegen eine solche Benachrichtigung stehen, ein grundsätzlicher Verzicht dürfte aber nicht geboten sein.

Bedenken hat der HmbBfDI außerdem bezüglich der umfänglichen Herabsetzung des Schutzes von Minderjährigen vorgetragen. Der Entwurf sieht in § 10 Abs. 1 vor, dass unter bestimmten Voraussetzungen auch personenbezogene Daten von Minderjährigen in Akten und amtseigenen Dateien gespeichert werden können, wenn diese

das zwölfte Lebensjahr vollendet haben (bisher: des vierzehnten Lebensjahres). Damit geht die hamburgische Regelung noch über das hinaus, was auf Bundesebene möglich ist. Ob hier eine weitere Absenkung des Alters gegenüber der im Bundesrecht bestehenden Regelung sinnvoll ist, erscheint fraglich, weil ein Austausch dieser Daten mit dem Bundesamt und anderen Landesämtern wegen der dort bestehenden höheren Altersgrenzen nicht möglich sein wird. Im Zentrum der Kritik stand dabei auch die Tatsache, dass mit der Verarbeitung von Daten von Kindern ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung gestattet wird. Dieser folgt nicht zuletzt daraus, dass „Jugendsünden" nicht auf Dauer vorgehalten werden und Entwicklungen nicht behindern dürfen, da sie eine stigmatisierende Wirkung für den Jugendlichen entfalten können. Es gelten daher erhöhte Anforderungen an die Bestimmtheit derartiger Normen. Diesem Grundsatz wird der Entwurf nicht immer gerecht. Nicht bestritten werden soll, dass die ebenfalls in § 10 Abs. 1 eingefügte Ermächtigung zur Übermittlung von personenbezogenen Daten Minderjähriger jeden Alters an andere öffentliche Stellen im Zusammenhang mit dem Kindeswohl seine Berechtigung hat. Die Notwendigkeit, dass das Landesamt bei Verwahrlosung, Gewalt oder Radikalisierung in der Lage sein muss, zuständige öffentliche Stellen zu informieren, liegt auf der Hand. Die Norm ist aber in ihrer jetzigen Ausgestaltung zu weit gefasst. Während das Gesetz eine Offenlegung aus (theoretisch allen) Gründen des Kindeswohls zulässt, sollte eine Begrenzung auf die Gefährdung des Kindeswohls vorgenommen werden.

Kritisch ist hervorzuheben, dass der Gesetzesentwurf jedoch in wesentlichen Bereichen Neuland betritt und die Befugnisse des Landesamts gerade bei der Erhebung und Weitergabe von Daten wesentlich erweitert. Dies betrifft vor allem die Übermittlung personenbezogener Daten durch das Landesamt für Verfassungsschutz an externe Stellen, bei der das Landesamt für Verfassungsschutz teilweise sein eigentliches Aufgabenprofil verlässt. So werden bei der Übermittlung personenbezogener Daten an private Stellen zum Schutz schutzbedürftiger Personen wie Minderjähriger rein präventive Zielrichtungen

verfolgt, die für die von der Übermittlung betroffenen Personen aufgrund der Sensibilität der Informationen erhebliche stigmatisierende Wirkung entfalten können. Aber auch hinsichtlich der Übermittlung personenbezogener Daten an öffentliche Stellen bietet der Entwurf weitreichende Verarbeitungsbefugnisse für das Landesamt für Verfassungsschutz. So ermöglicht der Entwurf eine Offenlegung insbesondere für Zwecke der öffentlichen Sicherheit oder für sonstige Aufgaben, die in ihrer Intensität der Gefährdung den genannten Aufgaben entsprechen. Hierdurch wird praktisch ein gänzlich neues Verständnis des Verfassungsschutzes begründet, der durch gezieltes Streuen von Informationen auftritt, zu einer Durchlaufstelle von Daten zu werden droht und damit auch in Konflikt mit dem grundsätzlich geltenden Trennungsgebot gerät. Der HmbBfDI hat Kritik an dem von Hamburg beschrittenen Weg zu einer Erweiterung der Kompetenzen der Verfassungsschutzbehörde in schriftlicher und in mündlicher Form vor dem Innenausschuss der Bürgerschaft vorgebracht.

Das Gesetz soll Mitte Januar 2020 in die Bürgerschaft zur Abstimmung gehen. Änderungsanträge von mehreren Fraktionen sind angekündigt. Es ist zu hoffen, dass der Kritik des HmbBfDI am Ende Rechnung getragen wird.

2. STRATEGIE INTELLIGENTE TRANSPORTSYSTEME

Der HmbBfDI hat auch in diesem Berichtszeitraum seine Mitarbeit in den Strategie-Gremien der Stadt fortgesetzt und einzelne Projekte bei der Umsetzung der ITS-Strategie beraten.

Mit der ITS-Strategie hat sich die Stadt die Digitalisierung und Vernetzung einzelner Transportsysteme auf die Fahnen geschrieben, um so insbesondere zu mehr Verkehrssicherheit, Verlässlichkeit, Effizienz und Umweltschutz beizutragen (Senatsdrucksachen 2015/0014 und 2016/00784). Dem Datenschutz hierbei ange-

messen Rechnung zu tragen, ist eine anspruchsvolle Aufgabe. Der HmbBfDI hat die einzelnen Akteure daher bereits in den vergangenen Jahren beraten (vgl. 26. TB, VI 2.1; 27. TB V.2.). Auch innerhalb dieses Berichtszeitraums hat er die laufenden Projekte auf ihrem Weg zu einer datenschutzkonformen Umsetzung begleitet und durch vertiefende Gespräche und die Teilnahme an Gremien die Projektverantwortlichen hinsichtlich der Belange des Datenschutzes sensibilisiert.

2.1. TESTSTRECKE AUTOMATISIERTES UND VERNETZTES FAHREN

Bei der Teststrecke automatisiertes und vernetztes Fahren handelt es sich um eine neun Kilometer lange nutzeroffene Strecke im öffentlichen Verkehrsraum, auf der in den kommenden Jahren die einzelnen Stufen automatisierten Fahrens erprobt werden sollen. Hierfür will der Landesbetrieb Straßen, Brücken und Gewässer (LSBG) diese Strecke nach und nach mit der erforderlichen Infrastruktur ausrüsten.

Bereits im vergangenen Berichtszeitraum hatte der HmbBfDI den LSBG hierzu beraten (27. TB V.2.2.1.). Der LSBG hatte im November 2018 angezeigt, dass im Rahmen einer ersten Stufe der geplanten Teststrecke die dort installierten Ampeln mit sog. Roadsite Units ausgestattet werden sollten. Diese können die einzelnen Ampelphasen unidirektional per W-LAN an empfangsbereite Fahrzeuge aussenden. Gegen eine solche Infrastructure2Vehicle-Kommunikation bestanden aus Sicht des HmbBfDI keine datenschutzrechtlichen Bedenken, da es hierbei zu keiner Verarbeitung personenbezogener Daten kommen konnte.

Hieran hatte sich im Prinzip auch in diesem Berichtszeitraum nichts geändert. Allerdings hatte die Stadt nunmehr mit Volkswagen einen neuen Projektpartner für die Nutzung der Teststrecke gewonnen. Den HmbBfDI erreichten in diesem Zusammenhang daher einige Anfragen. Denn abhängig von der im jeweiligen Fahrzeug eingesetzten Technik können beim automatisierten Fahren personenbezogene Daten verarbeitet werden. Dies gilt vor allem für eine Großstadt

wie Hamburg, da derartige Fahrzeuge regelmäßig über zahlreiche Kameras und Sensoren zur Umfelderfassung verfügen. Die Anfragen musste der HmbBfDI jedoch an die Kolleginnen und Kollegen in Niedersachsen verweisen, die für die Datenverarbeitungen durch Volkswagen zuständig sind. Denn die Stadt hatte keinerlei Zugriff auf die im Zuge der Erprobung des autonomen Fahrens durch Volkswagen erhobenen Daten. Sie stellte lediglich die Teststrecke zur Verfügung, durch die nach wie vor keine personenbezogene Daten verarbeitet wurden. Auf dieser Grundlage konnte kaum von einer gemeinsamen Verantwortung der Stadt und Volkswagen ausgegangen werden.

Es zeigte sich jedoch erneut, wie wichtig ein kontinuierlicher Austausch über Veränderungen bei der Realisierung solcher Langzeitprojekte ist. Aufgrund der nutzeroffenen Ausgestaltung der von der Stadt installierten Teststrecke war für den unbefangenen Betrachter nicht ohne weiteres klar, wer hier eigentlich der tragende Akteur bei der Datenverarbeitung ist. Hier stoßen allerdings auch datenschutzrechtliche Informationspflichten an ihre Grenzen: Denn diese knüpfen an eine Verantwortlichkeit im datenschutzrechtlichen Sinne an. Hinsichtlich des autonomen Fahrens war diesen Pflichten also nur durch Volkswagen nachzukommen. Da die Stadt keinerlei personenbezogene Daten verarbeitete, war sie hier nicht in der Pflicht. Der HmbBfDI hat sich hinsichtlich des Geschehens auf der Teststrecke sehr kurzfristig nach Ankündigung der Fahrten mit den Kollegen aus Niedersachsen ausgetauscht. Gerne hätten wir allerdings die Möglichkeit gehabt, diesen Austausch früher zu suchen.

2.2. Automatisierte Verkehrserhebungen durch Wärmebildkameras

Verkehrszählungen geben Aufschluss über die Auslastung der Straßen und bieten hierdurch eine wertvolle Grundlage dafür, Verkehrsplanung wirtschaftlich und effektiv auszugestalten. Manuelle Erfassungen des Verkehrs sind eine datensparsame Alternative, jedoch mit hohem Personaleinsatz verbunden und selten geeignet, den Verkehrsfluss des gesamten Tages hinreichend wiederzugeben. Es ist

daher nachvollziehbar, dass man im Bereich der Städteplanung ein hohes Interesse daran hat, derartige Aufgaben zu automatisieren.

So sahen das auch die Projektbeteiligten der Behörde für Wirtschaft, Verkehr und Innovation (BWVI), des Landesbetriebs für Geoinformation und Vermessung (LGV) und der Hamburger Verkehrsanlagen (HHVA), die den Trend aus anderen Großstädten zur automatisierten Erfassung aufgriffen und dem HmbBfDI anzeigten, an 420 Kreuzungen den motorisierten Verkehr (ITS-Projekt „Automatisierte Verkehrsmengenerfassung“) und an 40 weiteren Orten den Radverkehr (ITS-Projekt „Hamburger Radverkehrszählnetz) automatisiert erfassen zu wollen. Hierzu sollte die Stadt mit 2000 Wärmebildkameras an Ampel- und Laternenmasten ausgestattet werden, die Verkehrsteilnehmerinnen und Verkehrsteilnehmer klassifiziert als Pkw, Lkw oder Radfahrer erfassen können. Gleichzeitig sollten die so erhobenen Daten auf der OpenData-Plattform (Urban Platform) des LGV bereitgestellt werden und damit auch von privaten Akteuren genutzt werden können.

Das Echo in der Presse war groß. Den HmbBfDI erreichten irritierte Nachfragen, was vermutlich der hohen Zahl der zu installierenden Kameras geschuldet war. Datenschutzrechtliche Bedenken stellten sich jedoch in diesem Zusammenhang nicht. Vielmehr hatten die Projektbeteiligten den Aspekt des Datenschutzes von Beginn an konsequent in ihre Planungen mit einbezogen. Aufgrund der eingesetzten niedrig auflösenden Wärmebildkameras konnte man bereits an der Personenbeziehbarkeit der Aufnahmen zweifeln, da auf den Bildern im Wesentlichen nur die Zahl der Verkehrsteilnehmer und ihre Kategorie erkannt werden konnten. Bereiche wie Hauseingänge sollten von den Kameras etwa durch entsprechende Ausrichtung oder den Einsatz von Filtern nicht erfasst werden. Die Projektbeteiligten hatten bei der Entwicklung des Datenschutzkonzepts jedoch noch einen anderen wesentlichen Aspekt berücksichtigt, der im Ergebnis jegliche Bedenken ausräumte: So wurden die Bilder der Kameras nach Auszählung der Verkehrsteilnehmerinnen und Verkehrsteilnehmer gelöscht. Damit ließ sich auch nachträglich, etwa durch entsprechendes Zusatzwissen, kein Personenbezug herstellen.

3. eTicketing: Übergabe des Smartphones zu Prüfzwecken

Zur Kontrolle von Fahrscheinen, die in der HVV-App erworben wurden, dürfen Kontrolleurinnen und Kontrolleure sich das Telefon des Fahrgasts aushändigen lassen – das Datenschutzrecht steht nicht entgegen.

Wer sein Bus- oder Bahnticket in der dafür vorgesehenen App des HVV kauft, kann dies bei einer Fahrkartenkontrolle belegen, indem er sein Handy vorzeigt. Was aber, wenn die Kontrolleurinnen und Kontrolleure die Echtheit des Tickets genauer prüfen wollen? Die HVV-Tarifbestimmungen sehen vor, dass sie das Smartphones des Fahrgasts hierfür auch selbst in die Hand nehmen dürfen. Gleich mehrere Petentinnen und Petenten zweifelten an der Rechtmäßigkeit dieses Vorgehens und baten den HmbBfDI um seine Einschätzung. Immerhin sind auf einem Smartphone zahlreiche personenbezogene Daten über den Besitzer und andere Personen gespeichert, von Kontakten und Kommunikationsinhalten über Fotos bis hin zu Daten aus Fitnesstrackern oder Banking-Apps.

Der HmbBfDI konnte grundsätzlich nachvollziehen, dass die Übergabe des Smartphones an einen Fremden Bedenken auslöst. Ein aufsichtsbehördliches Einschreiten war allerdings aus seiner Sicht nicht veranlasst, schon weil die Sichtkontrolle des Handy-Tickets durch Kontrolleurinnen und Kontrolleuren der HVV-Mitgliedsunternehmen nicht der DSGVO unterfällt.

Diese regelt nämlich nur die (ganz oder teilweise) automatisierte Datenverarbeitung (Art. 2 Abs. 1 Var. 1 und 3 DSGVO). Die nichtautomatisierte Verarbeitung ist nur umfasst, wenn personenbezogene Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Var. 3). Keiner dieser Fälle liegt bei der Kontrolle von Handy-Tickets vor. Bereits aus den Tarifbestimmungen des HVV für Fahrkarten zum Selbstausdrucken und Fahrkarten per Smartphone, Abschnitt 3, Unterabschnitt b ergibt sich, dass der Fahrgast selbst

sein Telefon bedienen und das Ticket in der App öffnen soll. Das Kontrollpersonal liest lediglich den Bildschirminhalt; das eTicket wird nicht zusätzlich durch ein Gerät gescannt. Auch eine spätere systematische Speicherung erfolgt nicht. Werden Fahrgäste bei der Kontrolle mit einem ungültigen Ticket erwischt und mit einem erhöhten Beförderungsentgelt belegt, dürfte dies eine eigenständige Verarbeitung darstellen.

Selbst wenn man in der Sichtkontrolle eines Smartphones eine Verarbeitung personenbezogener Daten im Sinne der DSGVO erkennen würde, dürfte diese von der Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. f DSGVO gedeckt sein. Es ist davon auszugehen, dass sie zur Wahrung berechtigter Interessen der Verkehrsunternehmen erforderlich ist und Interessen oder Grundrechte und Grundfreiheiten der betroffenen Fahrgäste nicht überwiegen. Regelmäßig hat nämlich der HVV keine Möglichkeit, anders als durch eine gründliche Kontrolle festzustellen, dass Fahrgäste den vereinbarten Fahrpreis nicht gezahlt haben. Ein Handy-Ticket ist durch Möglichkeiten der Bildbearbeitung anfälliger für Manipulationen als ein Ticket aus dem Automaten.

Das Risiko, dass Kontrolleurinnen und Kontrolleure sich unbefugt Zugriff verschaffen auf personenbezogene Daten des Fahrgasts oder das Gerät anderweitig manipulieren, ist dabei überschaubar. Das Personal der Verkehrsunternehmen ist – entsprechend den Tarifbestimmungen – ausdrücklich angewiesen, die Smartphones der Fahrgäste nicht zu bedienen. Zudem halten sie sich während der Kontrolle, die üblicherweise wenige Sekunden dauert, in unmittelbarer Nähe des Fahrgastes auf, der ihren Umgang mit dem Gerät beobachten und einschreiten kann, wenn der Kontrolleur oder die Kontrolleurin eigenmächtig die App verlässt. Dagegen, dass während der Kontrolle Anrufe eingehen oder Push-Mitteilungen erscheinen, können sich die Fahrgäste leicht selbst schützen: indem sie den Flugmodus aktivieren.

4. Google Analytics und ähnliche Dienste nur mit Einwilligung nutzbar

Website-Betreibende in Hamburg sollten ihre Websites umgehend auf Dritt-Inhalte und Tracking-Mechanismen überprüfen. Wer Dienste nutzt, die eine Einwilligung erfordern, muss die Einwilligung dafür einholen oder diese Dienste entfernen.

Ein Großteil der Aufsichtsbehörden – darunter auch der HmbBfDI – haben sich im Rahmen einer Pressemitteilung vom 14. November 2019 zum Umgang mit Diensten geäußert, die ein Nutzertracking zum Gegenstand haben. Vor dem Hintergrund des neuen Rechtsrahmens, der mit Geltungserlangung der Datenschutzgrundverordnung eingetreten ist, wurde der Einsatz von Webanalyse-Diensten wie bspw. Google Analytics neu bewertet sowie ausdrücklich abermals darauf hingewiesen, dass Veröffentlichungen aus der Zeit vor Geltung der DSGVO, wie die „Hinweise des HmbBfDI zum Einsatz von Google Analytics“ keine Gültigkeit mehr beanspruchen können.

Tracking-Tools erheben z.B. durch das Setzen von Cookies Daten über die individuelle Nutzung von Internetdiensten und Apps. Die Unterscheidung der Nutzer erfolgt durch Cookie-, Geräte- oder Werbe-IDs und kommt daher häufig ohne weitere Personendaten aus. Daher ist in der Regel eine direkte Identifizierung im Sinne einer konkreten Namenszuordnung zwar nicht möglich. Allerding kann eine Identität durch die Auswertung der Nutzungsdaten – insbesondere in Kombination mit anderen Mechanismen, siehe ErwG 30 DSGVO – in dem Sinne zugeordnet werden, dass es sich um dieselbe Person handelt. Die Person ist also konkret adressierbar. Zu den anderen Mechanismen im Sinne des ErwG 30 DSGVO zählen u.a. das Vergeben von Cookie-IDs, Werbe-IDs, Unique-User-IDs oder andere Identifikatoren, die einen personalisierten Rückgriff auf eine einzelne Person auch ohne Kenntnis des konkreten Klarnamens zulassen. Daher handelt es sich bei solchen Nutzungsdaten gemäß Art. 4 Nr. 1 DSGVO um personenbezogene Daten. Eine Anonymisierung der Daten und damit Ausschluss des Anwendungsbereichs der

DSGVO allein durch die Kürzung der IP-Adresse ist schon vor dem Hintergrund, dass diese nur ein Nutzungsdatum unter vielen ist, nicht möglich.

Google Analytics ist kein Tool, das allein zur Reichweitenmessung dient, sondern ein umfassendes Tracking-Instrument, das in den letzten Jahren stark fortentwickelt wurde. Außer dem Nutzen für den Webseitenbetreiber in Form von Nutzungsstatistiken zielt es auf die Informationsgewinnung durch Google. In der vom HmbBfDI beanstandeten und von Google den Webseitenbetreibern empfohlenen Standardeinstellung soll zunächst zwischen der Google LLC und dem Webseitenbetreiber ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO abgeschlossen werden. Darüber hinaus wird dem Webseitenbetreiber, soweit die Standard-Einstellung ausgewählt wird, zusätzlich der Abschluss eines „Controller-Controller-Agreement" zur zwingenden Bedingung gemacht, aus dem sich ergibt, dass sowohl Google als auch der Webseitenbetreiber in eigener Verantwortlichkeit handeln und die Möglichkeit einer eigenen anderweitigen Verarbeitung der Daten vorbehalten bleibt. Eine derartige Aufspaltung von Verarbeitungsvorgängen ist allerdings lebensfremd, da es sich bei dem durch Google Analytics im Rahmen des Seitenbesuchs durch den Nutzer ausgelösten technischen Vorgang, der gleichzeitig Daten sowohl für den Webseiten-Betreiber selbst erhebt als auch an Google überträgt, um einen einzigen Lebenssachverhalt handelt. Ein „Aufschwingen" vom Auftragsverarbeiter zum eigenverantwortlichen Datenverarbeiter innerhalb einer Verarbeitungstätigkeit bzw. ein dauerhafter Wechsel als Auftragsverarbeiter und / oder Verantwortlicher ist dem gesetzlichen Rollenverständnis der DSGVO fremd. Unter Berücksichtigung der europäischen Rechtsprechung (EuGH, Urteil v. 29.07.2019, Az: C-40/17) ist daher in der von Google empfohlenen Standardeinstellung von einer gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO auszugehen.

Daher ist auch nach Auffassung des HmbBfDI für den Einsatz von Google Analytics oder ähnlicher Dienste eine Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO erforderlich. Das ergibt sich zum einen

aus der aktuellen europäischen Rechtsprechung (EuGH, Urteil v. 1.10.2019, Az: C-673/17 „Planet49"), nach der für das Setzen von für die Erbringung des Dienstes nicht notwendigen Cookies eine informierte Einwilligung einzuholen ist. Zum anderen verpflichtet Google den Webseitenbetreiber selbst dazu, wirtschaftlich zumutbare Schritte zu ergreifen, um sicherzustellen, dass ein Nutzer transparente, umfassende Informationen über das Speichern von und das Zugreifen auf Cookies oder andere Informationen auf dem Endgerät des Nutzers erhält und dass sich der Nutzer damit einverstanden erklärt. Wie eine derartige Einwilligung rechtssicher ausgestaltet sein muss, führt der EuGH in seiner Entscheidung zu „Planet49" umfassend aus. Eine Einwilligung ist danach nur dann wirksam, wenn die Website-Besuchenden der Datenverarbeitung eindeutig und informiert zustimmen und die einwilligungsbedürftige Datenverarbeitung erst dann begonnen wird, nachdem die Einwilligung erteilt wurde. Der HmbBfDI legt diese Maßstäbe bei seiner Aufsichtstätigkeit zu Grunde und überprüft fortlaufend unter welchen Einstellungsoptionen welche Datenverarbeitungen beim Einsatz von Google Analytics erfolgen.

5. HINWEISE ZU FUNKRAUCH-WARNMELDERN

Eine Mehrzahl Betroffener hat sich über den ungewollten Einbau von Funkrauchwarnmeldern beschwert. Sie äußerten die Ansicht, Einbau und Betrieb würden unzulässig in Ihre Datenschutzrechte eingreifen. Die Prüfung hat ergeben, dass Funkrauchwarnmelder datenschutzrechtlichen Regelungen unterliegen und der Betrieb auf eine Rechtsgrundlage gestützt werden kann. Eigentümer, Wohnungsverwalter oder Vermieter müssen Kontrollrechte gegen sich gelten lassen und Informationspflichten erfüllen.

Die Anwendbarkeit datenschutzrechtlicher Regelungen folgt aus der untrennbaren Verarbeitung nicht personenbezogener und per-

sonenbezogener Daten, wie etwa einer Demontageerkennung. Die Verarbeitungen können auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gestützt werden, wobei auch lit. b und c (iVm. § 45 Abs. 6 HBauO) mögliche Rechtsgrundlagen darstellen. Einwilligungen kommen bei wirtschaftlicher Betrachtung aufgrund jederzeitiger Widerrufbarkeit nicht in Betracht.

Funkrauchwarnmelder dienen berechtigten Interessen von Eigentümern, Vermietern oder Verwaltern. Diesen weist die Rechtsordnung die Pflicht zu geeignete Brandschutzmaßnahmen zu installieren. Daneben schützen Rauchwarnmelder die körperliche Unversehrtheit der Bewohner.

Demgegenüber erschien fraglich, ob die Verarbeitungen auch erforderlich waren. Betroffene haben vorgetragen, analoge Rauchwarnmelder stellten eine zumutbare Alternative dar. Solche Rauchwarnmelder werden im jährlichen Turnus vor Ort geprüft. Funkrauchwarnmelder können demgegenüber granularer überprüft werden. Es findet eine vollständige Ferninspektion statt, die unterjährig durchgeführt wird. Dies kann ein höheres Brandschutzniveau gewährleisten. Insbesondere, wenn Betroffene nicht selbst in der Lage sind Defekte zu beheben, wie etwa bei besonders schutzbedürftigen Personen. Dies bedeutet im Umkehrschluss nicht, dass Funkrauchwarnmelder notwendig sind, um den Anforderungen des § 45 Abs. 6 HBauO zu genügen. Auch analoge Rauchwarnmelder sind geeignet die Betriebssicherheit einer Wohnung zu gewährleisten.

Eine Abwägung der gegenläufigen Positionen hat letztlich kein Überwiegen der Grundrechte und Grundfreiheiten Betroffener ergeben. Demontageerkennung und Abstandsmessung lassen keinen tiefgehenden Rückschluss auf die private Lebensführung zu.

Betroffene haben die Befürchtung geäußert, Funkrauchwarnmelder seien in der Lage, Bewegungsprofile zu erstellen. Objektive Anhaltspunkte dafür waren indes nicht ersichtlich. Bewegungsprofile erfordern granulare Echtzeitmessungen. Aus einem geprüften Übermitt-

lungsprotokoll gehen solche granularen Werte nicht hervor. Vielmehr werden monatlich Statusmeldungen in verschlüsselter Form übermittelt. Die Geräte können auch nicht von außen konfiguriert werden, da die Datenübertragung unidirektional erfolgt.

Im Übrigen sind Betroffene nicht schutzlos. Sie können Auskunftsansprüche geltend machen und personenbezogene Daten auch als fotooptische Reproduktion herausverlangen und somit eigenständig Kontrollrechte ausüben. Soweit sich Verantwortliche dafür entscheiden mehr Daten zu verarbeiten, müssen sie auch Transparenz- und Kontrollrechte umfänglich gegen sich gelten lassen. Sofern konkrete Anhaltspunkte für eine Manipulation einzelner Funkrauchwarnmelder vorliegen, besteht die Möglichkeit einer Beschwerde bei der zuständigen Aufsichtsbehörde.

Betroffene haben auch die Befürchtung geäußert, Funkrauchwarnmelder könnten unbemerkt Gespräche aufzeichnen. Ultraschallsensoren verfügen über eine spezielle Art Mikrofon, um den reflektierten Schall zu detektieren. Sie senden hochfrequente Schallimpulse aus und vergleichen das resultierende Echo mit der Laufzeit der Schallwellen. Ziel ist die Detektion von Hindernissen. Die Mikrofone agieren jedoch in Frequenzbereichen außerhalb menschlicher Stimmen.

Dem Eingriff in die Privatsphäre steht mit dem verfolgten Zweck des Schutzes von Leib und Leben der Betroffenen ein überragendes Schutzgut gegenüber. Zwar kann bei einer Abwägung zwischen dem Recht auf Privatsphäre und dem Schutzgut von Leib und Leben nicht pauschal letzterem der Vorzug eingeräumt werden. In der vorliegenden Konstellation konnte aber im Hinblick auf die Eingriffstiefe kein Überwiegen des Rechts auf Privatsphäre festgestellt werden.

6. Datenschutzbewusstsein in Vereinen schärfen

Auch Vereine und Stiftungen verarbeiten teils sensible Daten ihrer Mitglieder und müssen daher für Datenschutzkompetenz sorgen; häufig muss der HmbBfDI erst einmal ein Bewusstsein dafür schaffen.

Auch im aktuellen Berichtszeitraum erreichten den HmbBfDI zahlreiche Beratungsanfragen von Vereinen und Vereinsmitgliedern sowie einige Beschwerden betroffener Personen. Dasselbe gilt für den Bereich der oftmals ehrenamtlich geführten Stiftungen. Begrenzte Kapazitäten ermöglichten leider nicht immer eine zeitnahe Betreuung in wünschenswertem Umfang.

Das Spektrum der Fragen war ebenso breit wie das der Vereine. Sehr viele Vereine sind auf die Mitwirkung ehrenamtlicher Mitglieder angewiesen, die keine ausgewiesenen Datenschutzexperten sind. Die finanziellen Mittel sind häufig begrenzt. Das führt auf Seiten der Verantwortlichen zu der Hoffnung, dass die Datenschutzgrundverordnung im Verein nur eingeschränkt umgesetzt werden muss und im Übrigen die Datenschutzregelungen für die Vereine vom HmbBfDI ausgestaltet werden.

Häufig wurde vorgebracht, die Benennung eines oder einer Datenschutzbeauftragten überfordere die kleinen Vereine, weil die Ehrenamtlichen nicht über entsprechende Fachkenntnisse und nicht über die Zeit und die Bereitschaft verfügen, die hohe Verantwortung zu übernehmen, die damit einhergeht.

Gegen gesetzgeberische Einschränkungen der Geltung der Datenschutzgrundverordnung für Vereine und kleine Unternehmen hatte sich die Datenschutzkonferenz (DSK) mit einer Entschließung gewandt. Denn auch beim Wegfall der Benennungspflicht von Datenschutzbeauftragten bleiben die Pflichten des Datenschutzrechts bestehen, während Datenschutzkompetenz bei den Vereinen ver-

loren ginge (siehe Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23.04.2019: „Keine Abschaffung der Datenschutzbeauftragten“, https://www.datenschutzkonferenz-online.de/media/en/20190423_keine_abschaffung_der_dsb.pdf). Aus Sicht der Verantwortlichen in der Vereinsführung mag der Wunsch nach weniger strikten Datenschutzvorschriften nachvollziehbar erscheinen. Betrachtet man diese Frage jedoch aus der Warte der betroffenen Personen, muss man zu dem Ergebnis kommen, dass ihre Daten genauso schutzbedürftig sind, wie gegenüber kommerziellen Verarbeitern, die das Recht auf informationelle Selbstbestimmung achten müssen. Jedoch hat der Gesetzgeber die Kritik aufgenommen, hat § 38 Bundesdatenschutzgesetz (BDSG) geändert und die Anzahl der Daten verarbeitenden Personen, die für die Benennung einer oder eines Datenschutzbeauftragten maßgeblich sind, von 10 auf 20 erhöht.

Führt man sich das Spektrum vor Augen, in dem Vereine sich betätigen, erscheint – trotz der nachvollziehbaren Argumente der Verantwortlichen – die Einhaltung des Datenschutzrechts besonders wichtig. In einem Tierschutz- oder Musikverein mag dies nicht auf den ersten Blick einleuchten, wohl aber beim Satzungszweck von Selbsthilfevereinen, deren Mitglieder gesundheitliche Einschränkungen haben, Kulturvereinen ethnischer Prägung, Vereinen, die sich um Haftentlassene kümmern oder Parteien oder Gewerkschaften, bei denen schon allein die Mitgliedschaft entsprechende Eigenschaften oder Anschauungen offenbart. Selbst in Sportvereinen gibt es regelmäßig Inklusionsgruppen, die mit staatlichen Zuschüssen gefördert werden und bei denen Gesundheits- und Sozialdaten verarbeitet werden. Auch einige Kindergärten werden von kleinen Vereinen betrieben; die Verarbeitung der Daten der Kinder erfordert noch einmal erhöhte Sensibilität.

Um diesem Missverständnis entgegenzuwirken und Orientierung zu bieten, hat der HmbBfDI unter anderem gemeinsam mit dem Hamburger Sportbund eine Informationsveranstaltung für Sportvereine ausgerichtet sowie den Hamburger Stiftungstag mit einem

Workshop begleitet. Ziel des HmbBfDI wird weiterhin bleiben, das Datenschutzbewusstsein in den Vereinen zu fördern, damit dort für ausreichende Datenschutzkompetenz gesorgt wird. Die Beratungskapazitäten hierfür sind zwar leider nur in geringem Maße vorhanden. Anders als gegenüber kommerziellen Anbietern, wo Anfragen auf Beratung grundsätzlich abgelehnt werden, ist der HmbBfDI bestrebt, alle Anfragen aus gemeinnützigen Einrichtungen und Vereinen möglichst zu beantworten.

7. Privates Fotografieren in Kitas und Schulen unter der DSGVO

Aus den datenschutzrechtlichen Vorschriften der DSGVO lässt sich kein grundsätzliches Fotoverbot an Schulen und Kitas herleiten. Fotoaufnahmen von Eltern bei Schulaufführungen oder Kita-Veranstaltungen sind zu rein persönlichen oder familiären Zwecken vielmehr auch ohne Einholung einer Einwilligungserklärung der Abgebildeten zulässig. Dem Teilen der Fotos in sozialen Medien sind dabei aber äußerst enge Grenzen gesetzt.

Die Zulässigkeit des Fotografierens in Kitas und Schulen war im vergangenen Jahr Gegenstand verschiedener Eingaben und Beratungsfragen beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Die Unsicherheit beim Umgang mit diesem Thema spiegelt sich auch in der Berichterstattung der Presse wider, in der über Fotoverbote an Schulen z.B. bei Einschulungen berichtet wurde. Die von einzelnen Schulen zu Beginn des Schuljahres 2019/2020 verhängten pauschalen Fotoverbote lassen sich dabei nicht durch die datenschutzrechtlichen Vorschriften der DSGVO begründen. Für die datenschutzrechtliche Bewertung ist vielmehr die Person des Verantwortlichen, der Zweck der Aufnahme bzw. die beabsichtigte Verarbeitung, insbesondere die Frage der Veröffentlichung der Fotos entscheidend. In der Praxis sind daher Fotoaufnah-

men der Eltern z.B. bei einer schulischen Feierlichkeit datenschutzrechtlich anders zu beurteilen, als Fotoaufnahmen der Schule z.B. für das Fertigen von Schülerausweisen oder Porträt- und Gruppenfotos durch einen Schulfotografen. Kita- oder Schulleitungen können allerdings unabhängig von datenschutzrechtlichen Vorschiften von dem durch sie auszuübenden Hausrecht Gebrauch machen und Eltern Fotoaufnahmen beispielsweise aus pädagogischen oder organisatorischen Gründen teilweise oder ganz untersagen.

Aufnahmen durch Eltern in der Kita oder Schule

Das Fotografieren eigener oder auch anderer Kinder und Personen bei einer Schul- oder Kita-Veranstaltung stellt zwar eine Verarbeitung personenbezogener Daten nach Art. 4 Nr. 1 und 2 DSGVO dar. Der bei digitaler Fotografie nach Art. 4 Nr. 1 und 2 DSGVO grundsätzlich eröffnete sachliche Anwendungsbereich der DSGVO ist aber durch die Regelung des Art. 2 Abs. 2 DSGVO begrenzt. Sofern Eltern z.B. bei einer Einschulungsfeier oder einem Kita-Sommerfest Fotos aufnehmen, kann der Anwendungsausschluss des Art. 2 Absatz 2 lit. c DSGVO zum Zuge kommen. Danach findet die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen, die zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird (sog. Haushaltsausnahme). Von dieser Ausnahme werden Fotos erfasst, die für die eigene Erinnerung aufgenommen und nicht über den Freundes- oder familiären Kreis hinaus veröffentlicht werden. Folglich ist das Foto, das im privaten Erinnerungsalbum zu Hause abgelegt wird, als Datenverarbeitung nicht durch die Vorschriften der DSGVO erfasst. Das gilt auch, wenn nicht nur das jeweils eigene Kind, sondern auch andere Personen auf dem Foto zu erkennen sind.

Veröffentlichung der Aufnahmen z. B. in einem sozialen Netzwerk

Problematisch ist jedoch die Aufnahme eines Fotos, das nicht nur im Erinnerungsalbum abgelegt, sondern z.B. über soziale Medien veröffentlicht und damit einem größeren Personenkreis zugänglich gemacht wird. Die Vorschrift des Art. 2 Absatz 2 lit. c DSGVO knüpft

an eine „persönliche oder familiäre Tätigkeit“ an, was nach allgemeiner Ansicht sehr eng zu verstehen ist. Soweit das Foto in einem sozialen Netzwerk nur innerhalb einer geschlossenen Gruppe, die auf einen fest definierten Kreis von Personen aus dem sozialen Umfeld des Fotografierenden begrenzt ist, und zum Zweck der rein privaten Freundschaftspflege veröffentlicht wird, ist noch von einer persönlichen oder familiären Tätigkeit in diesem Sinne auszugehen. Wird das Foto hingegen zum Zweck einer auch beruflichen Kontaktpflege mit einer geschlossenen Gruppe geteilt, ist die Anwendungsausnahme des Art. 2 Absatz 2 lit. c DSGVO demgegenüber nicht mehr eröffnet. Zudem sind beim Verbreiten von Fotos in einer geschlossenen privaten Facebookgruppe die Wertungen des Kunsturhebergesetzes (KUG) zu beachten. Das KUG fordert für das Verbreiten von Personenfotos aus Gründen des Persönlichkeitsrechtsschutzes ebenfalls eine – zumindest konkludent erteilte – Einwilligung des/der Abgebildeten. Eine Ausnahme gilt dann, wenn das Foto bei einer öffentlichen Veranstaltung aufgenommen wurde, an der der Abgebildete teilgenommen hat. Diese Ausnahme greift allerdings wiederum nicht, wenn es sich um eine geschlossene Veranstaltung wie beispielsweise eine klasseninterne Veranstaltung gehandelt hat. Generell sollten über soziale Netzwerke daher auch in geschlossenen Gruppen in erster Linie Fotos der eigenen Kinder geteilt werden. Zudem ist auf eine hinreichende Sicherung der Gruppe durch Nutzernamen und Passwort zu achten.

Soweit eine Online-Veröffentlichung ohne Begrenzung auf einen bestimmten Personenkreis erfolgt, handelt es sich generell nicht mehr um eine persönliche oder familiäre Tätigkeit nach Art. 2 Abs. 2 lit. c DSGVO. Aufgrund des besonderen Datenschutzes von Kindern (vgl. Art. 6 Abs. 1 lit. f DSGVO) darf eine solche Veröffentlichung daher grundsätzlich nur mit Einwilligung der Sorgeberechtigten erfolgen. Ob neben oder anstelle der Einwilligung der Sorgeberechtigten eine Einwilligung der betroffenen Kinder bzw. Minderjährigen einzuholen ist, hängt von der Einwilligungsfähigkeit der betroffenen Kinder bzw. Minderjährigen ab. Art. 8 Abs. 1 DSGVO knüpft die Einwilligungsfähigkeit Minderjähriger in Bezug auf Dienste der Informationsge-

sellschaft an die Vollendung des sechzehnten Lebensjahres. Diese Altersgrenze kann analog herangezogen werden, wenn Fotos in Social Media-Accounts privater Dritter veröffentlicht werden sollen.

8. NEUE REGELUNGEN ZUR DATENVERARBEITUNG IN DER KREDITWIRTSCHAFT (PSD II)

Der Zahlungsverkehr hat in den letzten Jahren bedeutende technische Innovationen erfahren. Diese führten zu einem raschen Anstieg elektronischer und mobiler Zahlungen sowie der Entstehung neuer Zahlungsarten, die eine rechtliche Regulierung erforderlich gemacht haben und kritisch zu begleiten sind.

Den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) haben im Berichtszeitraum mehrere Anfragen zu den neuen Regelungen zur Datenverarbeitung in der Kreditwirtschaft erreicht. Vor dem Hintergrund, dass viele innovative Zahlungsmittel oder -dienste zunächst keiner bankrechtlichen Regulierung unterfielen, ist zu begrüßen, dass das neue Zahlungsdiensteaufsichtsgesetz (ZAG) Anfang diesen Jahres in Kraft getreten ist. Es setzt den aufsichtsrechtlichen Teil der Zweiten Zahlungsdiensterichtlinie, auch bekannt als PSD II (Payment Service Directive II), in deutsches Recht um. Die PSD II und das novellierte ZAG sollen dem Zweck dienen, die rasant fortschreitende Digitalisierung im Zahlungsverkehr rechtlich zu erfassen und durch eine stärkere Konturierung der Ausnahmetatbestände eine europaweit einheitliche Auslegung und Anwendung der Vorschriften zu fördern. Ziel sei es, den Wettbewerb zu stärken, die Sicherheit von Zahlungsdiensten zu erhöhen und den Schutz der Verbraucher zu verbessern.

Ein besonderes Augenmerk verdienen dabei die Regelungen zu Kontoinformations- und Zahlungsauslösediensten und der starken Kundenauthentifizierung.

8.1. Kontoinformations- und Zahlungsauslösedienste

Nicht-Banken können nunmehr als Informationsdienstleister auftreten, unterliegen aber nicht den bankrechtlichen Vorschriften, in denen auch datenschutzrechtliche Vorschriften enthalten sind. Zudem ist fraglich, ob die Informationsdienstleister an das Bankgeheimnis gebunden sind.

Ein Kernelement der neuen Regelungen ist die Aufnahme von Kontoinformations- und Zahlungsauslösediensten in den Katalog der Zahlungsdienste (vgl. § 1 Abs. 1 Nr. 1, 2 ZAG). Dabei handelt es sich um zwei unabhängig voneinander funktionierende Dienste, die sich dadurch auszeichnen, dass die Dienstleister nicht in den Besitz von Kundengeldern gelangen. Vielmehr sollen diese Dienstleister zukünftig im Zahlungsverkehr zwischen den Bankkunden und der kontoführenden Bank auftreten und bekommen damit einen Zugang zum Bankkonto.

Bei einem Zahlungsauslösungsdienst beauftragen die Betroffenen, Überweisungen in deren Namen von ihrem Konto auszuführen, welches bei einem anderen Zahlungsdienstleister, z.B. einer Bank oder Sparkasse, liegt. Der Zahlungsauslösedienstleister greift dabei auf Kontodaten der Betroffenen zu. Beispielsweise ermöglichen Zahlungsauslösedienste, Onlinekäufe umgehend zu bezahlen, indem die Zugangsdaten für das Onlinebanking und eine Transaktionsnummer (TAN) direkt an einen an den Onlineshop angebundenen Zahlungsdienstleister übermittelt werden.

Ein Kontoinformationsdienst hingegen ist ein Online-Dienst zur Mitteilung konsolidierter Informationen über ein Konto bei einem oder mehreren Zahlungsdienstleistern, die über Online-Schnittstellen des kontoführenden Zahlungsdienstleisters zugänglich sind. Durch den Kontoinformationsdienst sollen die Zahlungsdienstnutzer einen Gesamtüberblick über ihre finanzielle Situation zu einem bestimmten Zeitpunkt in Echtzeit erhalten. Hinter der Definition verbergen sich Dienste, die z.B. über eine App auf Konten zugreifen. In seinem Angebot muss der Kontoinformationsdienstleister sich jedoch nicht auf eine direkte Übernahme und Wiedergabe der Umsatzdaten der Online Banking-Konten beschränken; vielmehr kann es sich um die Darstellung bearbeiteter Umsatzdaten handeln. In der Definition des Kontoinformationsdienstes liegt auch sein kommerzielles Potenzial, denn Kontobuchungen können analysiert und für das Finanzmanagement genutzt werden. So kann etwa anhand der Ein- und Ausgaben das frei verfügbare Einkommen der Betroffenen berechnet und ein auf die Bedürfnisse der Betroffenen zugeschnittenes Produkt vorgeschlagen werden – beispielsweise mit Blick auf (Versicherungs-, Stromanbieter- oder Mobilfunk)Verträge oder die Bonität der Kunden.

Wer Zahlungsauslösedienste erbringen will, benötigt eine Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin (§ 10 ZAG). Sind ausschließlich Kontoinformationsdienste beabsichtigt, ist lediglich eine Registrierung notwendig (vgl. § 34 ZAG).

Sowohl Zahlungsauslöse- als auch Kontoinformationsdienstleister haben ihrem Antrag bzw. der Registrierung eine Beschreibung der Sicherheitsstrategie, einschließlich einer detaillierten Risikobewertung des erbrachten Kontoinformationsdienstes, und eine Beschreibung von Sicherheitskontroll- und Risikominderungsmaßnahmen zur Gewährleistung eines angemessenen Schutzes der Zahlungsdienstnutzer vor den festgestellten Risiken, einschließlich Betrug und illegaler Verwendung sensibler und personenbezogener Daten, beizufügen. Zudem haben sie eine Beschreibung der Prüfmodalitäten und der organisatorischen Vorkehrungen für das Ergreifen aller angemessenen Maß-

nahmen zum Schutz der Interessen seiner Nutzer und zur Gewährleistung der Kontinuität und Verlässlichkeit der von ihm erbrachten Zahlungsdienste vorzulegen. In der Beschreibung der Sicherheitsstrategie ist zudem anzugeben, auf welche Weise durch diese Maßnahmen ein hohes Maß an technischer Sicherheit und Datenschutz gewährleistet wird; das gilt auch für Software und IT-Systeme, die der Zahlungsauslöse- als auch Kontoinformationsdienstleister verwenden, an die der Zahlungsauslöse- als auch Kontoinformationsdienstleister alle oder einen Teil seiner Tätigkeiten auslagert.

Problematisch an der neuen Rechtslage ist, dass Nicht-Banken als Informationsdienstleister auftreten können, diese jedoch nicht den bankrechtlichen Vorschriften – in denen auch datenschutzrechtliche Vorschriften enthalten sind – unterliegen. Zudem ist fraglich, ob die Informationsdienstleister an das Bankgeheimnis gebunden sind. Das Bankgeheimnis gewährleistet, dass Kreditinstitute zur Verschwiegenheit gegenüber Dritten verpflichtet sind, wenn es um kundenbezogene Daten geht. Dieser Pflicht unterliegen Nicht-Banken jedoch nicht. Daran knüpft auch die Seriosität solcher Informationsdienstleister an. Vor dem Hintergrund, dass der Informationsdienstleister Zugriff auf das Bankkonto des Nutzers erhält, ohne dass er damit die Verfügungsgewalt über dessen Geld erhält, werden sich die Betroffenen stets die Frage stellen müssen, ob Sie dem Informationsdienstleister Ihre Daten anvertrauen können. Allein dieser Zugriff und die sensiblen Zahlungsdaten, die der Zahlungsdienstleister erhält, sind der Grund, dass diese Dienste registrierungspflichtig sind und von der Finanzaufsichtsbehörde beaufsichtigt werden.

Betroffene sollten daher stets prüfen, wem sie ihre Daten anvertrauen und weiterhin ihre Daten aus den Originalquellen im Blick behalten und nicht blind den Informationen, die vom Informationsdienstleister bereitgestellt werden, vertrauen. Ferner ist den Betroffenen zu raten, von ihren Betroffenenrechten gemäß DSGVO, insbesondere dem Auskunftsrecht, Gebrauch zu machen. Zum einen erhalten die Betroffenen so einen Überblick darüber, welche Daten zu ihrer Person gespeichert sind. Zudem können die Auskünfte es

erleichtern, gezielt weitere Rechte, wie auf Berichtigung, Löschung oder Einschränkung der Verarbeitung („Sperrung"), geltend zu machen.

Werden Betroffenen Datenschutzverstöße durch Informationsdienstleister bekannt, sind diese in jedem Fall der zuständigen Datenschutzaufsichtsbehörde zu melden. Die Datenschutzaufsichtsbehörde kann dann mit ihren Untersuchungs- und Abhilfemöglichkeiten auf die Einhaltung der DSGVO hinwirken.

Mit Blick auf die seit dem 25.05.2018 anzuwendende DSGVO hat das ZAG auch Auswirkungen auf das informationelle Selbstbestimmungsrecht der betroffenen Personen. Zwar sieht auch das ZAG Regelungen zum Umgang mit personenbezogenen Daten der Bankkunden vor, diese sind jedoch weniger restriktiv als die Vorgaben der DSGVO. Der Gesetzgeber scheint diese Problematik jedoch gesehen und bewusst im ZAG die Beachtung der datenschutzrechtlichen Vorschriften über die Verarbeitung personenbezogener Daten aufgenommen zu haben. Damit findet die DSGVO neben dem ZAG Anwendung! Dies wird an folgendem Beispiel deutlich:

Die PSD II bzw. das ZAG sieht vor, dass Zahlungsdienstleister die für das Erbringen ihrer Zahlungsdienste notwendigen personenbezogenen Daten nur mit der ausdrücklichen Einwilligung des Zahlungsdienstnutzers abrufen, verarbeiten und speichern dürfen. Hiernach wäre es zulässig, wenn die Bank dem Kontoinformationsdienstleister Zugriff auf alle Kontotransaktionen eines relevanten Zeitraumes geben würde. Problematisch ist hierbei, dass auch die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) hiervon betroffen sein kann. Bei Arztrechnungen wären es beispielsweise Gesundheitsdaten oder aber bei Beiträgen für politische Parteien, Gewerkschaften oder religiöse Einrichtungen würde die politische, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen und damit in die Verarbeitung einfließen und letztlich zu einer Profilbildung genutzt werden können. Dies ist nach der DSGVO grundsätzlich untersagt, es sei

denn die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere Zwecke ausdrücklich eingewilligt. In diesem Fall greift die DSGVO und die Betroffenen müssen eine doppelte Einwilligung erteilen. Ein Widerspruch liegt in diesem Fall nicht vor. Eine Übertragung aller Kontotransaktionen an den Kontoinformationsdienst widerspricht allerdings den Grundsätzen der DSGVO, wie der Zweckbindung, der Datensparsamkeit und der Datensouveränität (individuelle Kontrolle des Bankkunden über seine Daten).

8.2. Starke Kundenauthentifizierung im elektronischen Zahlungsverkehr

Starke Kundenauthentifizierung im elektronischen Zahlungsverkehr soll für mehr Sicherheit bei der Nutzung des Online-Bankings und beim Bezahlen im Internet führen, ist aber im Hinblick auf den Grundsatz der Datenminimierung und der Verwendung biometrischer Daten nicht unproblematisch.

Seit dem 14. September 2019 ist die starke Kundenauthentifizierung im elektronischen Zahlungsverkehr gemäß § 55 ZAG anzuwenden. Ihr Hauptziel ist mehr Sicherheit (insbesondere die Betrugsprävention) bei Nutzung des Online-Bankings und beim Bezahlen im Internet durch Einführung einer Zwei-Faktoren-Authentifizierung. Hierdurch soll sichergestellt werden, dass es sich bei dem Nutzer auch wirklich um den berechtigten Benutzer handelt, der seine Zustimmung für den Zugriff auf seine Kontoinformationen oder für die Übertragung von Geldbeträgen erteilt. Mit einigen wenigen Ausnahmen müssen daher alle Online-Transaktionen nunmehr anhand von mindestens zwei der nachfolgenden drei Merkmale authentifiziert werden:

- Wissen des Kunden: Abfragen, z.B. Passwort, Code, PIN
- Besitz des Kunden: Authentifizierung durch ein Gerät, z.B. Smartphone, Karte mit Nummer oder Wearable

- Sein des Kunden (auch Inhärenz genannt), wie z.B. Fingerabdruck, Irisscan, Stimm- oder Gesichtserkennung/Verwendung von biometrischen Merkmalen.

Im Hinblick auf den Grundsatz der Datenminimierung, wonach personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden müssen (Art. 5 Abs. 1 lit. a DSGVO), dürften bei der starken Kundenauthentifizierung mehr Daten verarbeitet werden als notwendig und erforderlich. So dürfte schon fraglich sein, ob bei der Nutzung des Online-Bankings und beim Bezahlen im Internet zur Erbringung der Leistung tatsächlich die Handynummer des Kunden erforderlich ist. Diese Frage stellt sich erst recht bei der Verwendung biometrischer Daten (Art. 4 Nr. 14, Art. 9 DSGVO), die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind und deshalb einen besonderen Schutz verdienen, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können.

Besonderes Augenmerk ist daher aus datenschutzrechtlicher Sicht auf das Merkmal „Inhärenz – Sein des Kunden" zu richten, denn die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die neben der passwortbasierten Authentifizierung bei Online-Diensten eine immer größere Rolle einnimmt. Hintergrund hierfür ist einerseits die Einzigartigkeit der genutzten Merkmale, andererseits aber auch die simple Anwendung, denn Kunden müssen sich keine komplizierten Passwörter mehr merken.

Das Grundprinzip der biometrischen Erkennung ist bei allen Systemen gleich. Alle biometrischen Systeme enthalten unabhängig von ihrem oft sehr individuellen technologischen Aufbau die Komponenten der Personalisierung oder Registrierung des Nutzers im System (Enrolment), die Erfassung der biometrisch relevanten Eigenschaften einer Person und die Erstellung von Datensätzen (Templates) sowie den Vergleich der aktuell präsentierten mit den zuvor abgespeicher-

ten Daten (Matching). Die Erfassung biometrischer Merkmale erfolgt sowohl bei der erstmaligen Erfassung zur Erstellung des sog. Referenzdatensatzes, als auch bei der späteren Erfassung zur Wiedererkennung durch Sensoren wie Kamera, Mikrofon, Tastatur, Druckpads, Geruchssensoren oder Fingerabdrucksensoren.

Erfassung, Auswertung und Vergleich biometrischer Merkmale ist naturgemäß mit Messfehlern behaftet, da sich die verwendeten Merkmale im Lauf der Zeit verändern. Dies kann auf natürlichen, etwa altersbedingten Änderungen beruhen, aber auch auf äußeren Einflüssen wie Verletzungen oder Krankheiten. Hinzu kommen äußerliche Veränderungen wie Änderung der Haartracht (Frisur, Bart), Tragen einer Brille, von Kontaktlinsen oder veränderte Kosmetik. Zudem wird das Merkmal dem System niemals in der gleichen Art und Weise vom Nutzer dargeboten. Die Position des Fingers z.B. auf einem Fingerabdrucksensor oder der Blickwinkel des Gesichts ändern sich bei jeder Nutzung geringfügig. Dies hat zur Folge, dass zwei digitale Abbilder eines biometrischen Merkmals niemals identisch sind.

Ein exakter Abgleich der Daten kann daher nicht erreicht werden. Die tatsächliche Entscheidung über Match oder Non-Match beruht vielmehr auf zuvor eingestellten Parametern, die einen Toleranzbereich bilden, in dem biometrische Daten vom System als “gleich” erkannt werden. Die biometrischen Merkmale werden nicht auf Gleichheit, sondern nur auf “hinreichende Ähnlichkeit” getestet. Dies hat zur Folge, dass biometrische Systeme nur mit systemtypischer Wahrscheinlichkeit bestimmen können, ob es sich um den wahren Berechtigten handelt.

Zudem ist das Missbrauchspotential bei biometrischen Merkmalen groß, denn nur mit einer kleinen Auswahl an Fotos von einer Person kann die gesamte Topologie eines Gesichts zuverlässig rekonstruiert werden. Und wenn die eigenen biometrischen Merkmale einmal in verwertbarer Form verloren sind, kann man sie nie wieder verwenden. Ein Passwort zur Authentifizierung hingegen kann jederzeit neu generiert werden.

9. Aktivitäten auf europäischer Ebene

9.1 Vertretung im EDSA

Die Tätigkeit des HmbBfDI im europäischen Datenschutzausschuss dauert an und ermöglicht es, auf die Arbeit dieses wichtigen Gremiums im Sinne der Bundesländer Einfluss zu nehmen.

Der Europäische Datenschutzausschuss (EDSA, https://edpb.europa.eu/edpb_de) ist das gemäß Artikel 68 ff DSGVO eingerichtete Organ der Europäischen Union, dessen wesentliche Aufgabe darin besteht, die einheitliche Anwendung der DSGVO sicherzustellen. In diesem Ausschuss sind die Aufsichtsbehörden aller Mitgliedstaaten des EWR (d.h. EU28 plus Island, Liechtenstein und Norwegen), der Europäische Datenschutzbeauftragte (EDPS) und die Europäische Kommission vertreten.

Deutschland ist dabei zum einen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) als gemeinsamem Vertreter gemäß § 17 Bundesdatenschutzgesetz (BDSG) vertreten. Die ebenfalls in § 17 BDSG vorgesehene Wahl eines Stellvertreters durch den Bundesrat ist auch mehr als anderthalb Jahre, nachdem der EDSA seine Arbeit aufgenommen hat, noch nicht erfolgt. Der HmbBfDI ist jedoch weiterhin (siehe 27. TB, V 6) von der Datenschutzkonferenz beauftragt, diese Rolle bis zu einer ordentlichen Wahl wahrzunehmen und so sicherzustellen, dass die Aufsichtsbehörden der Länder eine Stimme in dem europäischen Ausschuss haben.

Im Berichtszeitraum ist der EDSA zu elf Sitzungen in Brüssel zusammengekommen. In den Plenarsitzungen werden neben der Aussprache zu jeweils aktuellen Themen überwiegend Ergebnisse finalisiert und beschlossen, die auf Ebene der Fachgruppen (Expert Subgroups) erarbeitet wurden. In diesen Subgroups ist Deutschland durch eine Vielzahl von Mitarbeiterinnen und Mitarbeitern des Bundes- und verschiedener Landesdatenschutzbeauftragter vertreten

(siehe auch V 9.3), so dass sich, bedingt durch die föderale Struktur Deutschlands, regelmäßig ein hoher Koordinations- und Austauschbedarf für die EDSA-Sitzungen ergibt. Diesem wird man im direkten Kontakt mit den Länder- und Bundeskollegen, durch Telefonkonferenzen sowie – vor allem in Fällen der Festlegung auf einen verbindlichen gemeinsamen Standpunkt Deutschlands im EDSA – mit Unterstützung der beim BfDI eingerichteten Zentralen Anlaufstelle gerecht.

Im Berichtszeitraum konnte der HmbBfDI eine Reihe von Akzenten im EDSA setzen. Dies betrifft vor allem Fragen der europäischen Zusammenarbeit bei Fällen mit vielen Betroffenen in ganz Europa. Ausgehend von Beschwerden, die uns zu großen Verantwortlichen wie Facebook, Google und anderen erreicht haben, oder von Berichten in der Presse über Datenverarbeitungen solcher Unternehmen, die Anlass zu kritischen Nachfragen geben, sind mehr und mehr Probleme in Hinblick auf die einheitliche Anwendung der DSGVO in Europa zu erkennen. Wie sich zeigt, genügt es häufig nicht, solche Fälle an die jeweils zuständige federführende Aufsichtsbehörde (LSA) heranzutragen, wie dies in der DSGVO vorgesehen ist. Die Erwartung, dass regelmäßig innerhalb angemessener Zeiträume Entscheidungen durch die LSA vorgelegt werden, hat sich bislang nicht erfüllt. Der HmbBfDI hat dies wiederholt im EDSA kritisch angesprochen und verschiedene Hindernisse identifiziert. Dadurch konnte das Niveau der gegenseitigen Information der europäischen Aufsichtsbehörden untereinander verbessert und verschiedene grundsätzliche Fragen der Auslegung der Zusammenarbeit und Kohärenz vorangebracht werden (im Detail siehe V 9.2 und 9.4).

Auch auf der inhaltlichen Ebene sind Initiativen des HmbBfDI aufgegriffen worden. So wurde im Dezember 2019 die Technology Subgroup damit beauftragt, Leitlinien zu stimmbasierten Assistenten (siehe hierzu auch II 16) zu erarbeiten, in denen sowohl die rechtlichen wie auch die technischen Fragen solcher Systeme behandelt werden sollen. Der Anstoß für eine solche Befassung ging vom HmbBfDI aus. Wir werden uns daher – gemeinsam mit dem BfDI - an der inhaltlichen Arbeit hierzu beteiligen.

9.2 Enforcement ESG

Einheitliche Vollzugsstandards können nur erreicht werden, wenn Behördenhandeln in grenzüberschreitenden Fällen lückenlos überprüfbar ist.

Grenzüberschreitende Fälle werden im sogenannten One-Stop-Shop-Verfahren bearbeitet. Danach ist der Ansprechpartner für den Verantwortlichen ausschließlich die federführende Aufsichtsbehörde an seinem europäischen Hauptsitz. Beschwerdeführer können sich hingegen an ihre Heimatbehörde oder jede beliebige andere Datenschutzbehörde wenden, sodass mehrere Behörden betroffen sein können. Die federführende Behörde ermittelt den Fall aus und erlässt am Ende eine sogenannte Draft Decision – Beschlussentwurf, siehe Art. 60 Abs. 4 DSGVO. Über den Entwurf stellen alle betroffenen Behörden einen Konsens her, und die Beschwerdeführer werden schließlich von Ihrer Wunschbehörde über das gemeinsame Ergebnis informiert.

Diese kooperative Verfahrensweise war die Antwort des Unionsgesetzgebers auf die sehr uneinheitlichen Vollzugsstandards vor Geltungsbeginn der DSGVO. Der Gemeinschaft aller europäischen Aufsichtsbehörden sollte eine rechtliche Handhabe gegeben werden, um restriktivere Behörden zu einer Angleichung ihrer Vollzugspraxis zu bewegen. In der Praxis zeigen sich jedoch die Schwächen dieses Instruments. Nur die federführende Behörde ist zum Erlass des Beschlussentwurfs befugt und sie unterliegt dabei keinerlei rechtlichen Fristen. Legt sie keinen Beschlussentwurf vor, haben die übrigen Behörden keine rechtliche Möglichkeit, auf die Ermittlungen einzuwirken oder auch nur Informationen über den Verfahrensstand zu erhalten.

Insbesondere zu öffentlichkeitswirksamen Berichten über mögliche Datenschutzverletzungen einflussreicher IT-Unternehmen wird oftmals kein Beschlussentwurf erlassen mit der Begründung, es handele sich nicht um eine Beschwerde im engeren Sinne. Der HmbBfDI ist jedoch überzeugt, dass die Durchsetzung der DSGVO nur gelingen

kann, wenn federführende Aufsichtsbehörden entsprechenden Medienberichten nachgehen. Er ist der Überzeugung, dass federführende Behörden nach Art. 60 Abs. 2 Satz 3 DSGVO verpflichtet sind, einen Beschlussentwurf zu erlassen, wenn andere Behörden ihnen Hinweise auf mögliche Datenschutzverletzungen durch Verantwortliche ihn ihrem Zuständigkeitsbereich gegeben haben. Falls der Beschlussentwurf dann den begründeten Inhalt hat, dass kein Tätigwerden beabsichtigt ist, kann dies durch den EDSA überprüft werden.

Die Enforcement Expert Subgroup, ein Gremium des EDSA, erarbeitet derzeit ein Papier zum gemeinsamen Verständnis der Reichweite von Ermittlungen sowie zu Voraussetzungen und Inhalten von Beschlussentwürfen. Der HmbBfDI wirkt als Berichterstatter an der Erstellung des Papiers mit. Er setzt sich dafür ein, dass federführende Behörden in jedem Fall einen aussagekräftigen Beschlussentwurf anzufertigen haben, wenn Aufsichtsbehörden anderer Mitgliedstaaten ihnen Fälle möglicher Datenschutzverletzungen in ihrem Zuständigkeitsbereich melden.

9.3 Social Media ESG

Die Verarbeitung personenbezogener Daten im Rahmen sozialer Netzwerke werden auf europäischer Ebene intensiv diskutiert. Ein Schwerpunkt dabei ist die Reichweite und Bedeutung der gemeinsamen Verantwortlichkeit von Anbietern solcher Netzwerke und Dritten.

Der HmbBfDI vertritt die Aufsichtsbehörden der Länder in der Social Media Expert Subgroup des Europäischen Datenschutzausschusses (EDSA). Wie in der Geschäftsordnung der Datenschutzkonferenz (DSK) festgelegt, wird neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) jeweils ein Bundesland verantwortlich und ein weiteres stellvertretend in jede Expert Subgroup des EDSA entsandt. Für die Social Media ESG hat die DSK dem HmbBfDI diese verantwortliche Rolle zugewiesen.

Die Social Media Expert Subgroup wurde im Mai 2018 nahezu gleichzeitig mit dem Inkrafttreten der DSGVO gegründet, um Fragen der Funktion und der Aktivitäten sozialer Medien datenschutzrechtlich zu bewerten und entsprechend Leitlinien oder „Best Practice"-Empfehlungen zu entwerfen. Die Einrichtung dieser Expertengruppe war aufgrund der stetig wachsenden Bedeutung der sozialen Medien für die Gesellschaft, Wirtschaft und Politik notwendig geworden.

Auch in diesem Jahr lag der Fokus der Social Media Expert Subgroup auf der Rollen- und Pflichtenverteilung bei der Nutzung sozialer Medien durch Unternehmen und politische Parteien. Hintergrund sind zum einen erhebliche Missbrauchsfälle wie Cambridge Analytica und deren Auswirkungen auf die Meinungsbildung in demokratischen Systeme, zum anderen die Präzisierung der gemeinsamen Verantwortlichkeit durch die Rechtsprechung des Europäischen Gerichtshofs. Die Erklärung des EDSA zur Verwendung personenbezogener Daten im Zusammenhang mit politischen Kampagnen (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_de.pdf) wurde aufgrund der thematischen Nähe in der Social Media ESG abgestimmt.

Bereits im Juni 2018 gab der Europäische Gerichtshof mit seiner Entscheidung „Wirtschaftsakademie" (C-210/16) den ersten Impuls zu einer grundlegend neuen Bewertung der Rollenverteilung bei der Nutzung sozialer Netzwerke. Sein Urteil vom 29.07.2019 in Sachen Fashion ID (C-40/17) bestätigte, dass Betreiber von Websites, die Social Plugins einbinden (in jenem Fall den Facebook-Like-Button), gemeinsam mit dem Netzwerkbetreiber für die Erhebung und Weitergabe personenbezogener Daten, die beim Seitenaufruf an die Anbieter übermittelt werden, verantwortlich sind. Beide Urteile wurden in die Arbeit der Social Media Expert Subgroup einbezogen und sind insbesondere bei der Erstellung der Leitlinien zum Thema Targeting relevant. Der HmbBfDI hat hierbei die Rolle des sog. „Lead Rapporteur" inne, der die Gruppe der Berichterstatter koordiniert sowie das Ergebnis im EDSA vorstellen wird.

Die europäische Ausrichtung seiner Aktivitäten ist für den HmbBfDI ein wichtiges Instrument, um auf die Auslegung des rechtlichen Rahmens im europäischen Kontext, in der sich die ganz überwiegend grenzüberschreitend agierenden sozialen Medien bewegen, Einfluss nehmen zu können.

9.4 Cooperation ESG

Das Hauptziel der DSGVO, ein gleichmäßiges und hohes Datenschutzniveau europaweit herzustellen, kann nur durch den intensiven Austausch der Datenschutzbehörden untereinander erreicht werden.

In der Cooperation Expert Subgroup des Europäischen Datenschutzausschusses (EDSA) werden grundlegende Fragen der Zusammenarbeit zwischen den europäischen Aufsichtsbehörden diskutiert und versucht, sie einer Lösung zuzuführen. Dies erfolgt z.B. in Form von Leitlinien zur Auslegung der DSGVO oder in anderen Vereinbarungen über das gemeinsame Vorgehen.

Im Lauf der ersten Monate der Rechtsanwendung haben sich verschiedene Probleme bei der einheitlichen Anwendung der DSGVO in verschiedenen Mitgliedstaaten herausgestellt. Zu diesen gehören beispielsweise:

- Die Frage, in welchen Situationen der EDSA um eine Stellungnahme gemäß Artikel 64 DSGVO ersucht werden kann
- Der Spielraum für einvernehmliche Lösungen (sog. Amicable Solutions) im Falle von Beschwerden
- Der Umgang mit Beschwerden und anderen Fällen, die auf Vorgänge Bezug nehmen, die bereits vor Geltung der DSGVO begonnen haben
- Die Zuständigkeit bei einem Wechsel des Sitzlandes eines Verantwortlichen

Der HmbBfDI hat aus praktischer Betroffenheit solche Themen in die Subgroup eingebracht und ist an deren Ausarbeitung beteiligt. Dabei zeigt sich, dass viele der dabei angesprochenen Fragen von den verschiedenen europäischen Aufsichtsbehörden sehr unterschiedlich beantwortet werden und gemeinsame Ergebnisse daher nur mit entsprechendem Aufwand zu erreichen sind. Dieser Aufwand ist jedoch gerechtfertigt, da bei Verzicht auf solche Abstimmungen die Gefahr eines Auseinanderdriftens in der Vollzugspraxis und der Auslegung des gemeinsamen europäischen Rechts real ist. Bereits so zeigt sich, dass nationale Rechtsrahmen, an die sich die jeweiligen Aufsichtsbehörden zusätzlich und teilweise vorrangig gebunden sehen, die Situation meist nicht erleichtern. Solche Regelungen zu erkennen – auch soweit es ggf. das eigene Land betrifft – ist bereits ein wichtiges Ergebnis der gemeinsamen Beratungen.

9.5 Transparenz im EDSA

Der Europäische Datenschutzausschuss (EDSA) hat sich größtmöglicher Transparenz verpflichtet und möchte diesbezüglich mit gutem Beispiel vorangehen. Dementsprechend hat dieser das Rules of Procedure Drafting Team beauftragt, Fragen rund um den Zugang zu Dokumenten des EDSA zu klären und transparentere Abläufe zu schaffen. Der HmbBfDI beteiligt sich federführend als lead rapporteur an dieser Aufgabe.

Der Europäische Datenschutzausschuss hat sich dem Grundsatz der Transparenz verschrieben. Dazu heißt es in der Geschäftsordnung des ESDA: „Gemäß dem Grundsatz der Transparenz arbeitet der EDSA so offen wie möglich, um effizienter und rechenschaftspflichtiger gegenüber dem Einzelnen zu sein. Der EDSA erläutert seine Tätigkeit in einer klaren, für alle zugänglichen Sprache."
Entsprechend dieser eigenen Zielsetzung hat sich der EDSA in seiner Oktobersitzung mit Fragen rund um die Transparenz in eigenen Angelegenheiten befasst. Der HmbBfDI hat hierbei einige Punkte angesprochen, die im Sinne des Transparenzgedankens noch verbessert werden können. Insbesondere beim Zugang zu den Protokollen der

Sitzungen des EDSA hat der HmbBfDI auf Verbesserungspotential hingewiesen. Derzeit werden diese nicht vom EDSA veröffentlicht.

Dies hatte zur Folge, dass das Rules of Procedure Drafting Team, welches für die Geschäftsordnung des EDSA zuständig ist, mit der Aufgabe befasst wurde, die gesetzlichen Anforderungen an die Veröffentlichung der Protokolle zu prüfen und entsprechende Verfahren zu schaffen. Der HmbBfDI hat die Aufgabe übernommen, als lead rapporteur federführend dabei mitzuwirken. Ein erstes Treffen der Mitglieder des Rules of Procedure Drafting Team mit dem HmbBfDI findet am 6. Januar 2020 in Brüssel statt.

10. PRESSE- UND ÖFFENTLICHKEITS-ARBEIT

Auch 2019 war hinsichtlich der Anzahl der Presseanfragen beim HmbBfDI wie bereits im Vorjahr ein intensives Jahr. Insbesondere Themen wie Datenschutz bei Facebook, digitale Sprachassistenzsysteme oder auch das Urteil im VIDEMO-Verfahren haben für ein großes Anfrageaufkommen gesorgt.

Im Berichtsjahr 2019 hat sich die hohe Anzahl an Anfragen der Presse und der Medien zu unterschiedlichsten Datenschutzthemen gleichsam verstetigt. Neben einer ersten Bilanzierung nach dem ersten Jahr DSGVO spielten erneut datenschutzrelevante Vorfälle bei den großen US-amerikanischen Internetkonzernen eine Hauptrolle beim Medieninteresse. Neben dem Datenleck bei Twitter waren es vor allem gleich mehrere problematische Datenschutzaspekte bei Facebook sowie offene datenschutzrechtliche Fragen bezüglich Sprachassistenzsystemen. Wie schon in den Vorjahren sind zu diesen grenzüberschreitenden Themen erneut zahlreiche Anfragen ausländischer Medien beim HmbBfDI eingegangen.

Was die rein hamburgischen Themen mit Datenschutzbezug anbelangt, so gab es gehäufte Presseanfragen zum Urteil des Verwaltungsgerichts Hamburg bezüglich des Einsatzes von Gesichtserkennungssoftware im Zuge der G20-Ermittlungen (siehe IV 4). Des Weiteren sind hier zu nennen Anfragen zu den Novellierungen der Polizei- und Verfassungsschutzgesetze.

Darüber hinaus galt das Medieninteresse aber auch weiteren Bereichen des Datenschutzes. Hier ist insbesondere der Bereich Gesundheitsdaten zu nennen mit Presseanfragen zu Gesundheits-Apps oder dem Umgang mit Patientendaten. Des Weiteren spielten die Themen Videoüberwachung im öffentlichen Raum sowie Funkrauchwarnmelder eine größere Rolle. Zum ersten Jahrestag der DSGVO gab es zudem mehrere statistische Anfragen zur Zahl der Beschwerden, der Data Breaches und der Sanktionen.

Im Berichtszeitraum 2019 haben den HmbBfDI insgesamt 332 Presseanfragen erreicht, das sind ca. 10% weniger als im Vorjahr 2018 (368), als die Einführung der DSGVO und der Skandal um Cambridge Analytica überdurchschnittlich viele Anfragen auslösten. Im Durchschnitt wurden im Berichtsjahr 2019 rund 28 Anfragen pro Monat bearbeitet.

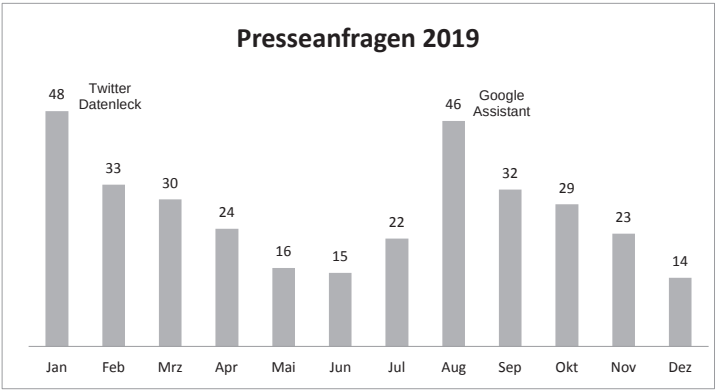


Abb. 1: Presseanfragen 2019 pro Monat mit Kennzeichnung „besonderer Ereignisse“

Wie Abb. 1 verdeutlicht, stechen die Monate Januar und August mit Anfragen-Peaks zum Twitter-Datenleck und zu Google Assistant deutlich hervor. Insgesamt lässt sich bezüglich der Presseanfragen zu den beiden Internet-Konzernen Facebook und Google sagen, dass die Anfragen hierzu ca. 26% der Gesamtzahl ausmachten. Damit ist das Interesse hieran im Vergleich zum Vorjahr gesunken (2018: 42% der Gesamtzahl). Von den beiden Konzernen liegt Facebook (15%) vor Google (11%).

Was die Herkunft der anfragenden Medien anbelangt, so bilden überregionale Medien wie schon im vorangegangenen Berichtszeitraum den Schwerpunkt. Anfragen ausländischer Medien sind im Jahr 2019 aufgrund diverser Themen rund um Facebook, Twitter und die Sprachassistenzsysteme angestiegen, wie die nachstehende Tabelle zeigt:

Presseanfragen…	2018	2019
regionaler Medien:	68	75
überregionaler Medien:	255	212
ausländischer Medien:	45	45
Gesamt:	368	332

Tabelle1: Presseanfragen beim HmbBfDI 2018 und 2019

Neben dem Tätigkeitsbericht zum Berichtsjahr 2019 gab es keine weiteren Veröffentlichungen im Printbereich. Das Internet-Angebot des HmbBfDI wird stets aktuell weiterentwickelt. Im Berichtszeitraum hat der HmbBfDI 18 Pressemitteilungen veröffentlicht.

Zudem haben der Hamburgische Datenschutzbeauftragte sowie einige Mitarbeiterinnen und Mitarbeiter der Behörde erneut Vorträge und Präsentationen zu Aspekten der DSGVO sowie verschiedenen Themen des Datenschutzes durchgeführt und sich an Gesprächsrunden oder Podiumsdiskussionen beteiligt.

Schließlich ist erwähnenswert, dass der HmbBfDI im Laufe des Jahres drei ausländische Delegationen in seinen Räumlichkeiten empfangen hat. Hierbei wurde die Arbeit der Aufsichtsbehörde vorgestellt und es wurden aktuelle Datenschutzthemen diskutiert. Die Delegationen, die sich aus Juristen bzw. aus Mitarbeitern von Datenschutzbehörden zusammensetzten, kamen aus Pakistan, der Türkei und Dänemark.

Als neues sehr wichtiges Instrument der Datenschutzkommunikation des HmbBfDI ist im Jahr 2019 noch die Datenschutz- und Medienkompetenzförderung insbesondere bei Kindern und Jugendlichen hinzugekommen (siehe hierzu ausführlich V 11).

11. DATENSCHUTZKOMPETENZ-FÖRDERUNG DURCH DEN HMBBFDI – „ICH HAB JA NIX ZU VERBERGEN!“

Mit dem Art. 57 Abs.1 lit. b Datenschutzgrundverordnung (DSGVO) wurde den Aufsichtsbehörden die Aufklärung der Öffentlichkeit über datenschutzrechtliche Themen - mit einem besonderen Augenmerk auf Kinder - als neue gesetzliche Aufgabe übertragen.

Bereits im Jahre 2010 wurden in Zusammenarbeit mit der Medienanstalt Hamburg Schleswig-Holstein, der Polizei Hamburg, dem NDR und der Schulbehörde das Projekt „Meine Daten kriegt ihr nicht“ erfolgreich realisiert. Aufgrund personeller Engpässe konnten jedoch die medienpädagogischen Bemühungen nicht mehr aktiv durch den HmbBfDI unterstützt werden. Die nun geschaffene Stelle der Referentin für Medienbildung und Schule soll diese Lücke schließen.

Medienpädagogisches Ziel des HmbBfDI ist es, alle Bevölkerungsgruppen umfänglich, zielgruppenorientiert und praxisnah zum Thema

Datenschutz aufzuklären. Dabei geht es vorrangig um die Sensibilisierung und Aufklärung zu einem datenschutzbewussten Umgang mit personenbezogenen Daten, aber auch um eine reflexive und kritische Betrachtung von gesellschaftlichen Transformationsprozessen im Zuge der rasant fortschreitenden Digitalisierung. Die Gefahr, dass Soziale Medien mit Hilfe von personenbezogenen Werbemaßnahmen aktiv in die politische und gesellschaftliche Meinungsbildung eingreifen, ist längst Realität geworden. Die Aufklärung und die Förderung von Medien- und Datenschutzkompetenz stellt daher eine der wichtigsten Aufgaben der künftigen Gesellschaft dar: Denn nur durch Aufklärung und gezielte Bildungsmaßnahmen kann eine aktive Teilhabe an der Gesellschaft und Demokratie gelingen. Die damit zusammenhängende Aufklärung bezüglich der rechtlichen Grundlagen des Datenschutzes, des Persönlichkeitsrechts sowie des Urheberrechts spielen insofern eine tragende Rolle in der Medienbildung des HmbBfDI.

Digitale Medien bilden einen wichtigen Teil in der heutigen Lebenswelt von Kindern und Jugendlichen. Wir erleben eine Digitalisierung unserer Gesellschaft, in der Soziale Medien, audiovisuelle on-demand Medien und das Internet im Allgemeinen immer mehr an gesellschaftlicher Relevanz gewinnen. Die Zahlen aus den neusten KIM und JIM Studien des Medienpädagogischen Forschungsverbunds Südwest überraschen daher wahrscheinlich nicht: 214 Minuten, das heißt 3 Stunden und 34 Minuten, betrug 2018 die durchschnittliche Mediennutzungsdauer von Jugendlichen pro Tag (Medienpädagogischer Forschungsverbund Südwest (mpfs) - JIM-Studie 2018, S. 31). Smartphones, kleine „Mini-Computer“, sind bei Jugendlichen omnipräsent. Mit ihnen kann man „kostenlos“ und unbegrenzt mit Freunden chatten, Soziale Netzwerke nach neuen Beiträgen durchsuchen, Internet-Videos auf einschlägigen Plattformen konsumieren und sich über das aktuelle Tagesgeschehen informieren. Das Smartphone bietet somit einen mobilen, barrierefreien Zugang zu Information und Kommunikation; nicht überraschend also, dass 97% der Jugendlichen heute ein Smartphone besitzen (Medienpädagogischer Forschungsverbund Südwest (mpfs) - JIM-Studie 2018, S. 8).

In der medienpädagogischen Arbeit des HmbBfDI werden immer wieder Bedenken und Sorgen bezüglich des Datenschutzes in Schulen vorgetragen. Vor allem die „IT-Verantwortlichen" der Schulen, oftmals Lehrer und Lehrerinnen mit nur fundamentalen IT-Kenntnissen und wenig zeitlichen Ressourcen, fühlen sich alleine gelassen und unsicher. Häufig besteht die generelle Haltung: „Lieber nichts machen, als etwas falsch zu machen". So wird aus Datenschutz eine Innovationsbremse - ein Phänomen, das es zu verhindern gilt. Lehrer und Lehrerinnen aber auch Schulleiter und Schulleiterinnen brauchen eine Anlaufstelle, bei der sie sich (bestenfalls lokal) vollumfänglich beraten, informieren, weiterbilden und absichern können. Diese Anlaufstelle soll laut DSGVO der Datenschutzbeauftragte der Schulbehörde sein, der aber als Einzelperson aufgrund der Vielfältigkeit und Fülle an Anfragen der über 330 staatlichen Schulen (ohne Erwachsenenbildung) dem Anspruch wohl kaum gerecht werden kann.

Unabdingbar für den Bildungsprozess von Schülern und Schülerinnen sind neben der Vermittlung von traditionellem Wissen, auch verschiedene kognitive und lernmethodische Kompetenzen. Zu diesen Kompetenzen gehören personale, soziale, kommunikative und emotionale Kompetenzen (ausgeprägte Persönlichkeit, positives Selbstbild etc.), aber auch „Kompetenzen in der digitalen Welt" (Sekretariat der Kultusministerkonferenz - Bildung in der digitalen Welt, 2016), wie beispielswiese Informationskompetenz, Problemlösefähigkeit, Medienkompetenz, kritische Haltung, Reflexionsfähigkeit, Forschungsdrang, Neugier, Zeit- und Selbstmanagement. Der HmbBfDI begrüßt den kompetenzorientierten Lernansatz der Hamburger Rahmenlehrpläne, sieht hier aber noch Entwicklungspotential. Die bereits 2010 erkannten Defizite in der Datenschutzkompetenzvermittlung haben sich teilweise in Schulen verfestigt. In der täglichen Praxisarbeit des HmbBfDI wird vermehrt festgestellt, wie schwer es vielen Lehrern und Lehrerinnen fällt, diese Kompetenzen zu vermitteln. Oftmals wissen Lehrer und Lehrerinnen nur wenig über mögliche „Gefahren im Netz" und fühlen sich den Kindern und Jugendlichen im Umgang mit den digitalen Medien unterlegen und abgehängt. Es bedarf daher vermehrter Lehr- und Weiterbildungsange-

bote. Zudem muss sichergestellt werden, dass auch die Vermittlung von digitaler Kompetenz in die Lehrausbildung angehender Lehrer und Lehrerinnen und Pädagogen und Pädagoginnen integriert wird. Zusätzlich muss der Ausbau der digitalen (schulischen) Infrastruktur und die Ausstattung der Lehrer und Lehrerinnen mit digitalen Endgeräten weiter vorangetrieben werden.

Seit Mai dieses Jahres hat der HmbBfDI mit der Planung und Umsetzung eigener Datenschutz- und Medienkompetenzprojekte begonnen. Es wurden diverse Schulungen und Workshops für Schüler und Schülerinnen, Lehrer und Lehrerinnen und auch Mitarbeiter und Mitarbeiterinnen der freien Kinder- und Jugendarbeit durchgeführt. Ein erstes Workshop-Konzept wurde gemeinsam mit der Verwaltungsschule der Stadt Hamburg erarbeitet, das sich derzeit in der praktischen Erprobung befindet. Langfristiges Ziel ist es, Lehr- und Lernkonzepte als Handreichung und/oder Open Educational Resources (OER) u.a. über die Webseite des HmbBfDI zur Verfügung zu stellen.

Des Weiteren wurden vom HmbBfDI auch medienpädagogische Beratungen für Schulen angeboten. In diesen Terminen konnten bereits erste Hemmschwellen abgebaut und neue Ideen für die praktische Medienarbeit in Schulen entwickelt werden. Zudem arbeitet der HmbBfDI eng mit dem Landesinstitut für Lehrerfortbildung zusammen, sodass bereits neue Projekte angestoßen werden konnten und Workshops gemeinsam durchgeführt wurden.

Die Bürgerschaft hat in der Drucksache 21/15381 beschlossen, Initiativen der Medienkompetenzförderung in Hamburg zukünftig stärker unterstützen zu wollen. Hierfür soll unter anderem ein Monitoring System der Initiativen und Projekte im Bereich der Medienkompetenzförderung und Medienbildung aufgebaut werden. Außerdem gilt es zu prüfen, ob ein „Medienkompetenz Fond" analog zum Fond „Kultur und Schule" installiert werden kann. Der HmbBfDI partizipiert auf Einladung der Schulbehörde an den entsprechenden Planungstreffen und begrüßt dies außerordentlich. Um die Bevölkerung vermehrt über das Thema Datenschutz und Datensicherheit zu in-

formieren, werden außerdem öffentlichkeitswirksame Kampagnen zukünftig stärker in die strategische Ausrichtung der Aufsichtsbehörde mit aufgenommen. Hierzu gehört auch ein Internetauftritt zur Medienbildung auf der Webseite des HmbBfDI – dieser befindet sich bereits in der Konzeption und Gestaltung. Gemeinsam mit der Medienanstalt Hamburg Schleswig-Holstein, der Kriminalpolizei Hamburg, den Bücherhallen und dem „Blinde Kuh" e.V. wird es eine Vielzahl von Workshop-Angeboten am Safer Internet Day 2020 geben. Nähere Informationen hierzu werden rechtzeitig auf der Webseite des HmbBfDI zur Verfügung gestellt.

Weiterhin begrüßt der HmbBfDI die kooperierende, offene und vertrauensvolle Zusammenarbeit mit medienpädagogischen Organisationen und Institutionen, Hamburger Behörden und anderen Datenschutzaufsichtsbehörden in Deutschland.

INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT VI.

1. Zahlen und Fakten

Die statistische Aufbereitung der Aufgaben des HmbBfDI nimmt einen immer größeren Raum ein. Das liegt einmal daran, dass der doppische Produkthaushalt der Freien und Hansestadt Hamburg über Kennzahlen gesteuert wird und dass es gesetzliche Berichtspflichten aus der DSGVO und dem HmbDSG gibt. Außerdem wird die Behördenleitung regelmäßig über die aktuellen Zahlen informiert, damit sie ggf. lenkend eingreifen oder die Forderung nach Verstärkung gegenüber der Politik belegen kann. Es liegt insb. aber auch daran, dass seit Anwendung der DSGVO eine Umfragewelle über die Aufsichtsbehörden hereingebrochen ist, wie es sie in der Vergangenheit nicht gegeben hat. Regelmäßige Umfragen zur Anzahl der Beschwerden, der Meldungen von Datenschutzverletzungen, zu Sanktionen, zu Bußgeldern usw. kommen von europäischen Stellen, von nationalen Stellen und nicht zuletzt immer wieder von der Presse. Diese Umfragewellen führen dazu, dass die Mitarbeiterinnen und Mitarbeiter beim HmbBfDI einen immer größeren Teil ihrer Arbeitszeit für die Erfassung von statistischen Daten aufwenden müssen, die dann vom Zentralreferat des HmbBfDI zusammengetragen und aufgearbeitet werden. Es wird (leider) noch nicht statistisch erfasst, wie viele Umfragen es seit dem 24. Mai 2018 gegeben hat, aber es bleibt zu hoffen, dass sich die Lage in dieser Hinsicht irgendwann normalisieren wird.

Dabei fällt immer wieder auf, dass oft Äpfel mit Birnen verglichen werden. Nur selten werden bei den Umfragen genaue Definitionen mitgeliefert, so dass die Anfragen u.U. ganz unterschiedlich beantwortet werden. Die Behörde X kann beispielsweise eine ganz andere Vorstellung davon haben, was genau eine Beschwerde ist, als die Behörde Y. Um wenigstens einen Teil der statistischen Zahlen vergleichbar zu machen, hat die DSK in ihrer Sitzung am 08. November 2018 beschlossen, dass die unabhängigen Aufsichtsbehörden ihrer Berichtspflicht aus Art. 59 DSGVO ab dem Berichtsjahr 2019 nach einheitlichen Kriterien nachkommen. Die Teilnahme an dieser gemeinsamen Darstellung ist freiwillig, der HmbBfDI hat aber schon im letzten Tätigkeitsbericht darauf Bezug genommen und setzt diesen Beschluss der DSK ab dem aktuellen Tätigkeitsbericht vollumfänglich um.

Dabei ist zu beachten, dass sich die folgenden Zahlen nicht auf alle im Jahre 2019 beim HmbBfDI eingegangenen Vorgänge beziehen, sondern immer nur auf den Teil, der bereits statistisch ausgewertet ist. Ob ein schriftlicher Eingang beispielsweise eine Beschwerde oder eine Beratungsanfrage ist, kann erst nach einer vorläufigen Prüfung von der zuständigen Referentin oder dem zuständigen Referenten bestätigt werden. Zum Zeitpunkt der Drucklegung dieses Tätigkeitsberichts waren von den 3.641 beim HmbBfDI insgesamt eingegangenen Vorgängen des Jahres 2019 3.405 (93,5%) statistisch ausgewertet.

1.1 Beschwerden

Beschwerden im Sinne des o.g. Beschlusses der DSK sind schriftliche und verschriftete Eingänge, bei denen eine natürliche Person eine persönliche Betroffenheit darlegt und bei denen Art. 78 DSGVO („das Recht auf einen wirksamen Rechtsbehelf gegen eine Aufsichtsbehörde“) anwendbar ist.

Diese Kriterien wurden von 2.359 Eingängen des Jahres 2019 erfüllt, das sind rund 65% der statistisch ausgewerteten Eingänge. Obwohl die Zahl der gesamten Eingänge gegenüber dem Vorjahr annähernd gleich ist (3.641 zu 3.670), hat sich die Zahl der Beschwerden gegenüber dem Vorjahr (1.898, vgl. 27. TB, VI.1.1) signifikant erhöht.

1.2 Beratungen

Beratungen sind alle schriftlichen datenschutzrechtlichen Auskünfte gegenüber Verantwortlichen, betroffenen Personen und Regierungen (Behörden). Im Berichtszeitraum wurden vom HmbBfDI 582 solcher Beratungen durchgeführt. Dabei wurden 396-mal betroffene Personen, 168-mal verantwortliche Stellen und 18-mal Behörden beraten.

Neben den schriftlichen Beratungen wurden beim HmbBfDI für das Jahr 2019 noch 821 (betroffene Personen: 585; Verantwortliche: 180; Regierungen: 56) telefonische Beratungen registriert. D.h., ins-

gesamt wurden im Berichtszeitraum 1.403 datenschutzrechtliche Beratungen durchgeführt.

1.3 Meldungen von Datenschutzverletzungen

Eine Verletzung des Schutzes personenbezogener Daten, das „Datenleck", ist der Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden zu melden, wenn durch die Verletzung voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Im Berichtszeitraum wurden uns 611 solcher Verletzungen gemeldet, das sind fast dreimal so viele Meldungen wie im Vorjahr (210, 27. TB, VI.1.4). Die Gründe für solche „Datenlecks" sind vielfältig, allerdings dominiert mit 275 Meldungen der Versand von Postsendungen oder E-Mails an den falschen Adressaten.

1.4 Abhilfemaßnahmen

Mit dem Art. 58 Abs. 2 DSGVO wurden die Aufsichtsbehörden dazu befugt, verschiedene Maßnahmen zur Abhilfe von datenschutzrechtlichen Verstößen zu ergreifen. Der HmbBfDI hat im Berichtszeitraum davon wie folgt Gebrauch gemacht:

Maßnahme	Rechtsgrundlage	Anzahl 2019
Warnungen	Art 58 Abs. 2 lit. a	1
Verwarnungen	Art 58 Abs. 2 lit. b	14
Anweisungen und Anordnungen	Art 58 Abs. 2 lit. c – g und j	4
Geldbußen	Art 58 Abs. 2 lit. i	3[1)]
Widerruf von Zertifizierungen	Art 58 Abs. 2 lit. h	0

[1)] 4 weitere Ordnungswidrigkeitsverfahren sind eröffnet, es ist aber im Berichtszeitraum nicht mehr zur Verhängung des Bußgeldes gekommen.

1.5 Europäische Verfahren

Sachverhalte, bei denen davon ausgegangen werden kann, dass es auch Betroffene in anderen Ländern der Europäischen Union gibt, werden als Europäische Verfahren oder sog. grenzüberschreitende Fälle in das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission eingegeben. Zu dem Sachverhalt können sich anschließend Aufsichtsbehörden als betroffen melden und die Aufsichtsbehörde, die die Zuständigkeit für die Hauptniederlassung des Verantwortlichen hat, übernimmt die Federführung. Neben diesem Verfahren gibt es weitere europäische Zusammenarbeiten, z.B. die Amtshilfe oder gemeinsame Maßnahmen, die in Art. 60 ff. DSGVO geregelt sind. Die DSK hat festgelegt, dass über europäische Verfahren wie folgt berichtet wird:

Europäisches Verfahren	Anzahl 2019
Verfahren mit Betroffenheit	**19**
Verfahren mit Federführung	**6**
Weitere Verfahren gem. Kap VII DSGVO (Art. 60 ff)	Werden statistisch nicht erfasst.

Von den 6 Verfahren, in denen der HmbBfDI federführend war bzw. ist, wurden 3 im Berichtszeitraum beendet. Dabei legt die federführende Behörde zunächst den Entwurf eines Beschlusses (sog. „draft decisions“) vor, gegen den betroffene Behörden Einspruch einlegen können. Inhaltlich handelte es sich um eine Verwarnung eines Verantwortlichen, eine Einstellung eines Verfahrens wegen mangelnder Nachweisbarkeit eines Rechtsverstoßes sowie um eine Abgabe an die Staatsanwaltschaft zur weiteren strafrechtlichen Ermittlung.

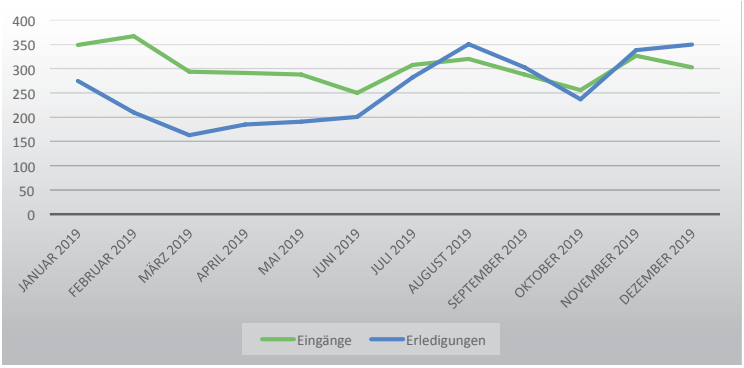
1.6 Förmliche Begleitung von Rechtsetzungsvorhaben

Nach dem genannten Beschluss der DSK werden hier pauschaliert die vom Parlament oder von der Regierung angeforderten und durchgeführten Beratungen als Gesamtzahl erfasst.

Nach der ‚Richtlinie zur Beteiligung der/des HmbBfDI' in der Fassung vom 24. Juli 2019 ist der HmbBfDI am Abstimmungsverfahren von Senatsdrucksachen zu beliefern, soweit Belange des Datenschutzes berührt werden. Im Jahre 2019 wurde der HmbBfDI an 81 Drucksachenabstimmungen beteiligt, von denen 41 Rechtsetzungsvorhaben zum Gegenstand hatten.

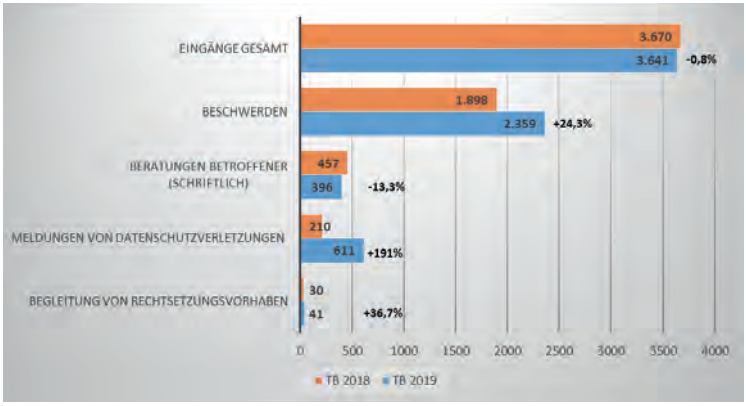
1.7 Entwicklung der Eingänge und Erledigungen

Ein wichtiger Indikator für die Arbeitsbelastung des HmbBfDI ist die Entwicklung der Eingänge, also aller schriftlich dokumentierten Beschwerden, Beratungen etc., im Vergleich zu den Erledigungen. Im folgenden Diagramm sind die monatlichen Eingänge und Erledigungen in 2019 abgebildet. Bei den Erledigungen sind auch die abschließenden Bearbeitungen von Vorgängen mit Eingangsdatum in 2017 und 2018 enthalten.



Im dritten Quartal wurden als Reaktion auf die große Lücke zwischen Eingängen und Erledigungen (befristete) personelle Verstärkungen realisiert. Dies führte zu einer deutlichen Entspannung der Situation. Dennoch hat sich allein in 2019 ein Rückstand von 555 Vorgängen aufsummiert. Rechnet man die noch offenen Eingänge aus 2017 und 2018 hinzu, ergibt sich aktuell ein Rückstand von insgesamt 1.200 Vorgängen.

1.8 Vergleich zum Tätigkeitsbericht 2018 im Überblick



2. Aufgabenverteilung (Stand: 1.1.2020)

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22 (7. OG), 20459 Hamburg
Tel.: 040/42854-4040
Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.datenschutz-hamburg.de

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

Beauftragter für den Haushalt, Verwaltungs- und Personalleiter
Arne Gerhards

Haushaltsplanung und -bewirtschaftung, Berichtswesen, Controlling
Robert Flechsig

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

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

Vorzimmer, Geschäftsstelle
Heidi Niemann

Registratur
Katharina Schmidt

Registratur, Auskünfte nach Art. 15 DSGVO
Ipek Sari

Datenschutzkompetenzförderung und Medienbildung, Öffentlichkeitsarbeit
Alina Feustel

Grundsatzfragen DSGVO, BDSG, HmbDSG und HmbTG, Vertretung des HmbBfDI in Gerichtsverfahren
Dr. Christoph Schnabel

Grundsatzfragen Sanktionen und Aktenführung, Einzelfallbearbeitung
Cornelia Goecke

Grundsatzfragen HmbVwVfG, VwGO, VwZG, Arbeits-, Dienst- und Disziplinarrecht
Richard Heyer

Grundsatzfragen Art. 58 DSGVO, Einzelfallbearbeitung
Steffen Sundermann

Informationsfreiheit und Akteneinsicht
Barbara Görnandt

Wirtschaftsverwaltung, Bezirks- und Parlamentsangelegenheiten, Parteien und Fraktionen, Wahlen und Volksabstimmungen, Umwelt, Kirchen
Eva-Verena Scheffler

Statistik, Meldewesen, Pass- und Ausweiswesen, Personenstands- und Archivwesen, öffentliches Bau- und Wohnwesen
Uta Kranold

Polizei, Staatsanwaltschaft, Gerichte, Strafvollzug, Verfassungsschutz, Feuerwehr, Notare, Ausländerwesen
Anna-Lena Greve

Gesundheits- und Sozialwesen, Forschung
Saskia Fritzsche

Öffentliches Verkehrswesen (insb. ÖPNV), eGovernment (Smart City), Ver- und Entsorgung, Informationsfreiheit
Swantje Wallbraun

Schulen und Hochschulen, Wohnungswirtschaft, Geodaten, Finanz- und Steuerwesen
Alexander Schiermann

Akkreditierung und Zertifizierung, Organisation der Vertretung der Länder im EDSA
Ulrich Kühn

Suchmaschinen (insb. Google, NorthData), Apps, Telekommunikation
Felix Wagner

Apps, Internet of Things, technisch-organisatorische Beratung und Prüfung, Akkreditierung und Zertifizierung
Herr Schneider

ePrivacy, Tracking, Cookies, Presse und Rundfunk, Akkreditierung und Zertifizierung
Katja Weber

Soziale Netzwerke (insb. Facebook, XING, Twitter), Akkreditierung und Zertifizierung
Frau Jacobson

Smart Devices (insb. Voice Assistants), Entwicklung von Prüftools
Roland Schilling

Suchmaschinen (insb. Google)
Dr. Jutta Hazay

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

Technische Grundsatzfragen bei Biometrie, Videoüberwachung, Konfiguration und Betrieb des Prüflabors, technisch-organisatorische Beratung und Prüfung
Eike Mücke

Technisch-organisatorische Beratung und Prüfung
Jutta Nadler

Technische Grundsatzfragen bei Netzwerken und mobilen Geräten, Konfiguration und Betrieb des Prüflabors, technisch-organisatorische Beratung und Prüfung
Robert Maka

Grundsatzfragen Wirtschaft, Internationaler Datenverkehr, Industrie und Handwerk, Landwirtschaft, Gewerkschaften
Dr. Jens Ambrock

Vereine, Sport, Steuerberater und Wirtschaftsprüfer, Stiftungen
Heike Wolters

Gewerbliche Dienstleistungen, Kreditwirtschaft, Rechtsanwälte, private Sicherheitsdienste und Detekteien
Oksan Karakus

Werbung- und Adresshandel, Logistik, Verkehr (ohne ÖPNV)
Sabine Siekmann

Beschäftigtendatenschutz, Markt- und Meinungsforschung
Arne Brest

Handel (stationär), Versicherungswirtschaft, Videoüberwachung (nicht-öffentlicher Stellen)
Bianka Albers-Rosemann

Auskunfteien, Versand- und Onlinehandel, Inkasso, Kultur, Bildung
Behrang Raji

Z