TÄTIGKEITSBERICHT DATENSCHUTZ 2021

Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Hamburg

30. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

2021

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

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

Auflage: 750 Exemplare
Foto Titelseite: Martin Schemm, bearbeitet von Thomas Krenz
Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH
Druck: oeding print GmbH

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

---

vorgelegt im April 2022
Thomas Fuchs
(Redaktionsschluss: 31. Dezember 2021)

INHALTSVERZEICHNIS

1. Vorwort

Der vorliegende 30. Tätigkeitsbericht Datenschutz 2021 ist ein besonderer Jahresbericht. Er dokumentiert ein Jahr des Abschieds, des Übergangs und des Neuanfangs: Die zweite und letzte Amtszeit des langjährigen Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Prof. Dr. Johannes Caspar ist im Frühjahr zu Ende gegangen, Ulrich Kühn hat knapp sechs Monate den Übergang gestaltet, und am 1. November habe ich nach meiner Wahl durch die Hamburgische Bürgerschaft das Amt angetreten.

Diese Konstellation erfordert zunächst eine Danksagung: An Johannes Caspar für 12 Jahre, in denen er das Amt geprägt und zu einer internationalen Marke gemacht hat. In denen er das öffentliche Bewusstsein für den Datenschutz, seine freiheitssichernde Funktion, seine Bedeutung für Menschenwürde und Persönlichkeitsschutz durch Gespür für Themen und mediale Präsenz, durch hohe fachliche Expertise und verfahrensbezogene Durchsetzung auf ein neues Niveau gehoben hat.

An Ulrich Kühn, seinen langjährigen Stellvertreter, für die umsichtige Steuerung des Interregnums, die in keiner Weise eine Zeit des Stillstands bedeutete, sondern mit der ersten förmlichen Mahnung gegen eine staatliche Stelle wegen des geplanten Einsatzes von Zoom einen eigenen Akzent setzte.

Und nicht zuletzt an die Mitarbeiter:innen des HmbBfDI, die, wie dieser Bericht eindrucksvoll zeigt, in einer Zeit, die weiter durch die tatsächlichen und datenschutzrechtlichen Herausforderungen der Pandemie geprägt war, sich konsequent für die Interessen und Rechte der Bürger:innen im Bereich des Datenschutzes eingesetzt haben.

Und das bei weiter ansteigenden Eingaben-Zahlen: Erstmals haben uns über 4.000 schriftliche Eingänge erreicht, knapp 3.000 davon förmliche datenschutzrechtliche Beschwerden. Das dokumentiert, wie sehr das Bewusstsein für die eigenen Rechte auf Privatheit und digitale Selbstbestimmung bei den Bürger:innen angekommen ist.

Und wie sehr der HmbBfDI als Anlaufstelle für die Durchsetzung dieser Rechte wahrgenommen wird. Deswegen bleibt es ein wichtiges Anliegen, die personellen und technischen Ressourcen diesen Anforderungen anzupassen. Die in der Hamburgischen Verfassung verankerte Unabhängigkeit des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit kann nicht zum Tragen kommen, wenn eine aufgabenadäquate Ausstattung der Behörde nicht gewährleistet ist.

Dies zumal in Zeiten, in denen die digitale Transformation sich weiter beschleunigt, in einigen Bereichen insbesondere des öffentlichen Sektors eigentlich gerade erst beginnt. Und damit die Aufgaben der Datenschutzbehörden sich verändern und weiten, die gestaltende Rolle zur beaufsichtigenden hinzukommt. Aber dazu später mehr.

Der HmbBfDI hat sich für die Zukunft viel vorgenommen. Und ich hoffe sehr, dass uns unsere Vorhaben gelingen werden und diese bei den Bürger:innen – im doppelten Wortsinn – auch ankommen. An dieser Stelle wünsche ich Ihnen eine gewinnbringende Lektüre dieses Jahresberichts und freue mich auf Ihre Anregungen und Reaktionen.

Thomas Fuchs

EINLEITUNG 1.

1. Einleitung

1.1 Europa – Der Datenschutz wächst zusammen

Datenschutz ist europäisch und international, das war schon immer so. Nichts ist so grenzüberschreitend wie der Datenverkehr. Seit 2018 gibt es mit der Datenschutzgrundverordnung (DSGVO) hierfür einen einheitlichen Rechtsrahmen in der EU. Und dieser entwickelt sich gerade weiter: Mit dem Digital Services Act (DSA), dem Digital Market Act (DMA) und dem Data Governance Act (DGA) der Europäischen Kommission kommt die Regulierung des digitalen Sektors in Europa auf eine neue Stufe. Das übergeordnete Ziel all dieser Vorhaben ist klar: Es soll ein sicherer digitaler Raum geschaffen werden, in dem auch zukünftig die Grundrechte der Nutzer:innen geschützt werden.

Der grenzüberschreitende Blick wird durch die Urteile des Europäischen Gerichtshofs (EuGH) noch verstärkt, die den Datentransfer in die USA unter besondere Beobachtung stellen. Durch den Befund, dass die Daten europäischer Bürger:innen in den Vereinigten Staaten nicht denselben Schutz wie in der EU genießen, da sich grundsätzlich jedes amerikanische Technologie-Unternehmen den Zugriff der amerikanischen Geheimdienste auf ihre Daten gefallen lassen muss, ist der datenschutzkonforme Einsatz amerikanischer Systeme und Softwareprodukte problematisch.

Auch wenn datenschutzrechtliche Themen häufig zunächst – und für viele damit vermutlich sehr abstrakt – auf europäischer Ebene diskutiert werden, betreffen sie uns hier in Hamburg jeden Tag. Aus diesem Grund bilden in diesem Jahr die europäischen und internationalen Themen erstmals ein eigenes Kapitel im Tätigkeitsbericht. Auch wenn der HmbBfDI nicht mehr im Europäischen Datenschutzausschuss (EDSA) sitzt, ist er z.B. als Ländervertretung in der Social Media Expert Subgroup des EDSA intensiv eingebunden und vor allem als in Deutschland für Facebook und Google zuständige Behörde in besonderer Verantwortung.

Johannes Caspar hat an dieser Stelle in den letzten Jahren zu Recht darauf hingewiesen, dass die irische Datenschutzbehörde nicht mit denselben Maßstäben und Entschiedenheit, wie wir es von anderen europäischen Datenschutzaufsichtsbehörden gewohnt sind, das Datenschutzrecht durchsetzt. Das gelte insbesondere für amerikanische Unternehmen, die ihren Europasitz in Irland haben. Dies schwäche den europäischen Datenschutz allgemein und er drohe daran sogar zu scheitern, so Caspar weiter. Dieser Befund ist leider weiterhin aktuell.

Dem steht aber positiv die wachsende Zahl von bedeutenden Entscheidungen europäischer Aufsichtsbehörden, die die Anwendung der DSGVO in Europa stärken, gegenüber. Nur beispielhaft seien die Entscheidungen von Österreich und Frankreich zum Statistikprogramm „Google Analytics" des amerikanischen Unternehmens Google LLC oder Belgiens Entscheidung zu TCF 2.0 genannt. TCF 2.0 ist eine technische Standard-Infrastruktur des Wirtschaftsverbands der Onlinewerbebranche (IAB), die eine Grundlage für die Nachverfolgung des Surfverhaltens im Netz und damit für die personalisierte Werbung darstellt. Diese Entscheidung wird weitreichende Folgen für die digitale Werbewirtschaft haben, und sich vielleicht auch positiv auf den Schutz unserer Daten bei der Nutzung des Internets auswirken. So füllen zahlreiche Entscheidungen der Behörden, aber auch der mitgliedstaatlichen Gerichte, die DSGVO nun anhand konkreter Fälle mit Leben und schaffen so eine zusätzliche Rechtssicherheit.

An solche Entscheidungen knüpft der HmbBfDI in seinem Handeln an. Deswegen ist der Blick nach ganz Europa, und nicht nur nach Brüssel, von zunehmender Relevanz.

1.2 Deutschland – Beginn einer nationalen Datenpolitik

Die Digitalisierung kommt in eine neue Phase. In Deutschland haben nicht nur die letzten Jahre deutlich gemacht, wie sehr das Land beim Thema Digitalisierung Nachholbedarf hat, insbesondere mit Blick auf den öffentlichen Sektor. Und richtigerweise weitet sich der Blick von den infrastrukturellen Voraussetzungen auf das gesamte Feld

von Digitalisierung, Datennutzung, Datenzugang, Datensicherheit und Datenschutz.

Der Koalitionsvertrag der Ampelregierung zeigt den Handlungsbedarf auf, und dieser ist nicht zuletzt ein regulatorischer. Ein Datengesetz, ein Datenzugangsgesetz, ein Forschungsdatennutzungsgesetz, ein Medizindatengesetz oder ein Beschäftigtendatenschutzgesetz. Das sind nur fünf Beispiele von insgesamt 15 Gesetzesvorhaben, die in dem Koalitionsvertrag genannt werden. Dazu finden sich dort Pläne für ein Dateninstitut, Datenräume, Datentreuhänder, Datenspenden...

Diese Vorhaben vereint die Idee, den fortschreitenden Prozess der Digitalisierung demokratisch zu gestalten. So soll vermieden werden, dass nur wenige große Unternehmen die Macht über die Daten haben und wir die von ihnen gesetzten Standards nur hinterjagend eingrenzen können, wenn überhaupt. So kommt zum Beispiel der gemeinnützigen Nutzung von Daten eine besondere Bedeutung zu, auch als Chance für Wissenschaft und Forschung und für den wirtschaftlichen Fortschritt.

Dies verändert die Rolle des Datenschutzes. Das Recht auf Privatheit und informationelle Integrität der Bürger:innen ist in diesen Ansätzen zumindest theoretisch impliziert. Datenschutz muss daher von Beginn an mitgedacht werden, und so Teil einer neuen digitalen Architektur unserer Gesellschaft werden.

Das bedeutet, dass bei allen Projekten und Gesetzesvorhaben auch die Expertise der Datenschutzbehörden von Anfang an einbezogen werden sollte, eigentlich einbezogen werden muss. Und es bedeutet auch, dass wir als Aufsichtsbehörden Antworten geben sollten, wie legitime Ziele datenschutzkonform erreicht werden können.

Dafür ist ein gewisses Umdenken hin zu einem gestaltenden, konstruktiven Datenschutz notwendig. Das wird die Aufsichtsbehörden fordern, aber es wird sich lohnen.

1.3 Hamburg – Datenschutz als Bürger:innenrecht

4.000! Diese Marke wurde 2021 erstmals überschritten. So viele Hamburger:innen richteten sich mit einem Anliegen, überwiegend mit einer Beschwerde, an den HmbBfDI.

Die Breite der Themen ist groß: Die Außenkamera des Nachbarn, unaufgeforderte personalisierte Werbung, Verwendung von persönlichen Daten bei Versicherungen oder Energieunternehmen, Datenschutz beim Arbeitgeber, Auskunftspflichten beim Makler und vieles mehr.

Die Beschwerde und das Auskunftsrecht sind Bürger:innenrechte. Sie schaffen die Möglichkeit, sich gegen die unberechtigte, nicht legitimierte Verwendung von persönlichen Daten zu wehren. Es ist gut, dass die Hamburger:innen dieses Recht zahlreich nutzen. Und deshalb ist es wichtig, dass der HmbBfDI den Hamburger:innen auch in angemessener Zeit und hoher Qualität antworten kann. Dies ist leider nach wie vor nicht der Fall. Die technische und personelle Ausstattung der Behörde ist für diese Zahl der Verfahren nicht geschaffen. Und bei allem Einsatz ist die Zahl der „Altfälle", die nicht zeitnah behandelt werden können, leider zu hoch. Hier ist unverändert Verbesserungsbedarf gegeben, für den der HmbBfDI 2022 sehr konkrete Vorschläge machen wird.

Hinzu kommen die zunehmenden Beratungen der öffentlichen Stellen, die auch in diesem Bericht einen breiten Raum einnehmen. Diese Aufgabe nimmt der HmbBfDI gerne war und stellt erfreut fest, dass die Bedeutung dieser Aufgabe im Vorfeld von Projekteinführungen zunehmend wächst. Zumal der Senat mit seiner Digitalstrategie die zunehmende Digitalisierung städtischer Dienstleistungen in den nächsten Jahren richtigerweise weiter vorantreiben wird.

1.4 Datenschutz und Kommunikation

Datenschutz ist auf den ersten Blick ein technisch-juristisches Thema – überwölbt von einem komplexen europäischen Rechtsrahmen und IT-Prozessen, die die meisten Anwender:innen kaum nachvoll-

ziehen können. Die Datenschutz-Profis haben es sich dabei in einer Sphäre des Expert:innenwissens gemütlich gemacht.

In der politischen Diskussion dient Datenschutz oftmals als Ausrede, wenn etwas nicht gelingt, oder lieber nicht gemacht werden soll. Und oft lässt sich tatsächlich beobachten, dass Datenschutz auch sinnvolle Projekte oder Vorhaben verhindert. Nicht, weil sie rechtlich oder technisch nicht umsetzbar sind, sondern weil die Angst, etwas falsch zu machen, dazu führt, dass Projekte vorschnell aufgegeben werden oder die Hürden höher gesehen werden, als sie tatsächlich sind.

Das trägt zu einem Bild bei, das den Datenschutz als Innovationsbremse sieht. Dieses Bild ist falsch, aber gleichwohl kann man es nicht ignorieren. Auch falsche Bilder können sich verfestigen.

Aus diesem Grund ist eine alltagsnahe und verständliche Kommunikation von Datenschutzthemen in einer Sprache, die auch Menschen außerhalb der technisch-juristischen Sphäre verstehen, so wichtig. Dies gilt erst recht bei der Vermittlung von Datenschutzthemen gegenüber jungen Menschen und der Vermittlung von Daten- und Medienkompetenz an Schulen und anderen Bildungsstätten. Der HmbBfDI möchte so das Vertrauen in den Datenschutz stärken und die Hamburger:innen befähigen, ihr Grundrecht auf informationelle Selbstbestimmung aktiv wahrzunehmen.

PRÜFUNGEN 2.

2. Prüfungen

2.1 Überblick

Im Berichtszeitraum hat der HmbBfDI die Prüfung der CRIME-Datei Aurelia weitergeführt. Ähnlich tiefgreifende Mängel, wie sie bei einer Prüfung der CRIME-Datei „Gruppen- und Szenegewalt" im Berichtszeitraum 2016/2017 offenbar wurden, konnten nicht festgestellt werden.

Bereits im November 2020 hatte der HmbBfDI mit der Prüfung der beim Landeskriminalamt 71 (Staatsschutz) geführten Datei „Aurelia" begonnen (siehe TB Datenschutz 2020, I 2). Diese landeseigene CRIME-Datei („Criminal Research and Investigation Management Software") dient der Gefahrenabwehr einschließlich der vorbeugenden Bekämpfung von Straftaten, einschließlich extremistischer und terroristischer Straftaten aus den Bereichen Ideologien und nicht zuordenbarer politisch motivierter Kriminalität. Der HmbBfDI musste im Rahmen der Prüfung der CRIME-Datei „Gruppen und Szenegewalt" im Berichtszeitraum 2016/2017 erhebliche Defizite bei der Führung der Datei feststellen. Dies führte letztlich zu einem Erlass einer formellen Beanstandung gegen die Behörde für Inneres und Sport (BIS) (vgl. TB Datenschutz 2016/2017, II 1.2). Aus diesem Grund war nun zu prüfen, ob die CRIME-Datei Aurelia datenschutzkonform geführt wird. Der HmbBfDI hat bei einem Vor-Ort-Termin zur Erläuterung der Datei ihren Inhalt kursorisch gesichtet und sich in der Folge die Zugriffssicherung, die Einhaltung von Speicher- und Löschfristen und die Protokollierung erläutern lassen. Der HmbBfDI hat zudem stichprobenhaft bei einzelnen Personen die Voraussetzung für die Speicherung überprüft. Die Prüfung hat zu keiner Beanstandung geführt.

Die Verarbeitung von personenbezogenen Daten durch Sicherheitsbehörden ist für den Bürger nicht immer nachvollzieh- und erkennbar. Datenschutzrechtliche Prüfungen von Maßnahmen der Polizei oder der Nachrichtendienste sind somit ein wichtiger Teil der Arbeit

von Aufsichtsbehörden. Bereits im kommenden Berichtszeitraum steht erneut die turnusgemäß durchzuführende Pflichtprüfung der sog. Antiterror-Datei (ATD) und der Rechtsextremismus-Datei (RED) an (vgl. zur letzten Prüfung TB Datenschutz 2020, I 1). Zudem beginnt nach §§ 73, 78 Abs. 3 Gesetz über die Datenverarbeitung der Polizei (PolDVG) im Gefahrenabwehrrecht erstmals der gesetzlich angeordnete Turnus für die Kontrolle der Einhaltung der gesetzlichen Vorschriften bei polizeilichen Maßnahmen nach §§ 20 bis 31 und 50 PolDVG. Der HmbBfDI ist danach im Abstand von höchstens zwei Jahren gesetzlich verpflichtet, u.a. die Datenverarbeitung durch den verdeckten Einsatz technischer Mittel (§ 20 PolDVG) oder die elektronische Aufenthaltsüberwachung (§ 30 PolDVG) zu prüfen.

2. 2 Verschlüsselte E-Mail-Kommunikation für Jugendämter

Nach einem langen Vorbereitungsprozess soll die verschlüsselte E-Mail-Kommunikation zwischen Jugendämtern und externen Stellen in 2022 flächendeckend nutzbar werden.

Was bisher geschah:
Im Oktober 2017 hat der HmbBfDI die E-Mail-Kommunikation mit externen Stellen durch den Allgemeinen Sozialen Dienst (ASD) des Fachamtes Jugend- und Familienhilfe im Bezirksamt Wandsbek geprüft. Hierbei wurde festgestellt, dass in ausnahmslos allen kontrollierten Fällen nicht hinreichend verschlüsselte E-Mails auch und gerade mit sensiblen personenbezogenen Sozialdaten von Kindern und Jugendlichen versendet wurden (vgl. 26. TB, II 5).

Nach § 78a SGB X ist jede datenverarbeitende Sozialleistungsstelle verpflichtet, diejenigen technischen Maßnahmen zu treffen, die erforderlich sind, um den Datenschutz sicherzustellen. Zum Schutz der sensiblen Informationen, die in den E-Mais enthalten waren, ist

die Verwendung einer sogenannten Ende-zu-Ende-Verschlüsselung erforderlich. Entgegen den gesetzlichen Anforderungen an eine datenschutzkonforme elektronische Übertragung von Sozialdaten waren die überprüften E-Mails nicht hinreichend verschlüsselt; eine Ende-zu-Ende-Verschlüsslung wurde nicht vorgenommen. Während der Prüfung wurde darüber hinaus vom Jugendamt bestätigt, dass derartige Inhalte vermutlich in nahezu allen Akten gefunden werden können. Der HmbBfDI hat im Zuge der Prüfung bereits 2017 die Sozialbehörde gebeten, die erforderlichen Maßnahmen zu ergreifen.

Im Tätigkeitsbericht des Jahres 2018 wurde berichtet, dass in Absprache zwischen Sozialbehörde, Senatskanzlei und dem HmbBfDI für die Verschlüsselung der Mails des ASD an externe Kommunikationspartner zukünftig der „Governikus MultiMessenger (GMM)" genutzt werden soll, der u.a. S/MIME oder GPG-verschlüsselte Mails senden und empfangen kann (vgl. 27. TB, III 3). Diese IT-Infrastrukturkomponente wurde im Auftrag des IT-Planungsrats entwickelt. Sie wird in Hamburg von der Senatskanzlei allen Behörden und Ämtern zur Verfügung gestellt.

Nachdem das Jahr 2019 ohne nennenswerten Fortschritt zur Behebung des Mangels vergangen war, wurde die E-Mail-Verschlüsselung unter Nutzung des GMM in einem Jugendamt Mitte 2020 erfolgreich pilotiert. Alle Beteiligten der Pilotierung waren sich einig, dass nunmehr diese pilotierte Lösung in allen Jugendämtern der Bezirke genutzt werden sollte. Trotz wiederholter Nachfragen des HmbBfDI in der Sozialbehörde verstrich nach der Pilotierung ein weiteres Jahr, bis die Sozialbehörde dieses Thema Mitte 2021 wieder aufgenommen hat.

Der aktuelle Stand:
In der Auftaktsitzung Ende Oktober 2021 herrschte unter den an der weiteren Planung Beteiligten Konsens, dass die Federführung für den Rollout-Prozess unter Leitung des neu bestellten Chief Digital Officer (CDO) der Bezirksämter erfolgen soll. Der CDO ist dem

Staatsrat für die Bezirksverwaltung der Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke (BWFGB) unmittelbar unterstellt. Durch ein Teilprojekt, das die Sozialbehörde leiten wird, soll die Einbindung der Jugendhilfe-Träger erfolgen. Eine erste Abschätzung des weiteren Projektverlaufs wurde dem HmbBfDI im November 2021 mitgeteilt. Danach sollen die noch zu erledigenden Vorbereitungsaufgaben für den Rollout-Prozess bis Ende März 2022 abgeschlossen werden. Der Rollout-Prozess soll bis Ende Oktober 2022 beendet sein. Ab diesem Zeitpunkt können dann alle Jugendämter der Bezirke mit den Jugendhilfeträgern verschlüsselt kommunizieren. Auch wenn dann 5 Jahre seit der durchgeführten Prüfung verstrichen sein werden, ist der HmbBfDI verhalten optimistisch, dass mit diesem Schritt der Einstieg in eine stärkere Nutzung der verschlüsselten Kommunikation mit Externen erfolgen wird. Es wäre für die Hamburgische Verwaltung ein sehr großer Entwicklungsschritt hin zu einer datenschutzgerechten elektronischen Kommunikation.

3.3 AutoAkte

Der Einsatz künstlicher Intelligenz in der Verwaltung bietet die Chance hoher Effizienzsteigerungen. Bei der Gestaltung ist einem möglichen Verlust der eigenen Datensouveränität vorzubeugen.

Mit dem Projekt AutoAkte entwickelt die Senatskanzlei mithilfe künstlicher Intelligenz eine technische Hilfestellung für die elektronische Aktenführung. In derzeit fünf Testbehörden werden die in das Aktenverwaltungs- und Archivsystem ELDORADO eingespeisten Dokumente automatisch analysiert und zum Training eines KI-Systems verwendet. Die Ausweitung auf die meisten weiteren Behörden ist geplant. Anhand von Texterkennung und der Häufung bestimmter Begriffe wird ein KI-Modell entwickelt. Auf dessen Basis kann die Software ermitteln, welche Inhalte in welcher Akte zu finden sind. Wird daraufhin ein neues Dokument angelegt, schlägt die Software Akten vor, in denen es aufgrund der verwendeten Begriffe wahrscheinlich ist, dass sie ähnliche Themen betreffen. Die Entscheidung, in welche Akte das so analysierte Dokument verortet wird, trifft das Verwaltungspersonal. Die AutoAkte-Software ist für diese Entschei-

dung ein unterstützendes Hilfsmittel zur Effizienzsteigerung. Einzelne Akten können aufgrund ihres sensiblen Inhalts von der Analyse ausgenommen werden, indem das Aktenzeichen in dem System als Ausnahme markiert wird.

Das Training der KI findet in einer Microsoft Azure Cloud statt. Zu diesem Zweck werden Kopien der vollständigen Akteninhalte in die Cloud geladen und dort für einen Zeitraum von einigen Stunden bis zu einigen Tagen gespeichert und analysiert. Die Daten werden verschlüsselt gespeichert, jedoch zur konkreten Verarbeitung in der Cloud zeitweise entschlüsselt. Anschließend werden die Rohdaten in der Cloud gelöscht, während das trainierte KI-Modell dort verbleibt. Die Originale der elektronischen Akten verbleiben im ELDORADO-System, das bei Dataport gehostet wird. Die Speicherung in der Cloud findet auf Servern im Europäischen Wirtschaftsraum statt auf Basis eines Auftragsverarbeitungsvertrags mit Microsoft. Ein Zugriff durch die US-amerikanische Konzernmutter ist nicht vorgesehen, aber technisch und faktisch nicht ausgeschlossen.

Aus Sicht der Senatskanzlei besteht kein tatsächliches Risiko, dass US-Sicherheitsbehörden an Akteninhalte gelangen, weil die unverschlüsselte Speicherung voraussichtlich kürzer ist als die angenommene Verfahrensdauer einer Datenanforderung nach US-Cloud Act und FISA 702. Eine solche risikobasierte Betrachtung deckt sich jedoch nicht mit der rechtlichen Bewertung des Europäischen Datenschutzausschusses in seinen Empfehlungen 01/2020. Zudem sind es lediglich die Rohdaten der in die Cloud kopierten Akteninhalte, die kurzfristig gelöscht werden. Das trainierte KI-Modell, das dauerhaft in der Cloud verfügbar ist, enthält ein detailliertes Regelwerk darüber, welche Inhalte in welcher Akte zu finden sind. Die Frage, ob und welche personenbezogenen Erkenntnisse aus dem KI-Modell ohne die Rohdaten zurückgewonnen werden können, kann noch nicht abschließend beurteilt werden.

Die Prüfung des sehr komplexen Verarbeitungsverfahrens dauert an. Der dringenden Empfehlung des HmbBfDI, den Pilotbetrieb mit Echt-

daten zu pausieren, bis Klarheit über die Rechtslage besteht, ist die Senatskanzlei nicht gefolgt.

2.4 Spendenwerbung mit personalisierter Website

Die Verarbeitung des Vor- und Nachnamens zu Werbezwecken für eine personalisierte Website ist nichts, was Betroffene erwarten – insbesondere wenn sie in keiner Beziehung zum Verantwortlichen stehen und keine Informationen zu dieser Datenverarbeitung erhalten haben.

Ende des Jahres 2020 wurde der HmbBfDI durch eine Beschwerde darauf aufmerksam, dass eine Hilfsorganisation Briefwerbung hatte verschicken lassen, in der Links zu personalisierten Websites – unter Nennung eines Vor- und Nachnamens – enthalten waren. Wenn die Werbeadressaten die Seiten aufriefen, wurden sie namentlich auf ein bestehendes Problem angesprochen und es wurden ihnen Vorschläge zu einer möglichen Unterstützung sowohl der Organisation bei der Bekämpfung dieses Problems als auch einer konkreten Person unterbreitet („Ihr Patenkindvorschlag"). Über die persönlichen Websites war außerdem eine direkte Reaktion auf diese Vorschläge möglich („Werde mein Pate!").

Für die Einrichtung der personalisierten Landingpages der Werbeempfänger hatte die verantwortliche Stelle deren Namen verarbeitet, die sie nicht selbst bei den Betroffenen erhoben, sondern von dem Dienstleister erhalten hatte, von dem die Datensätze der Adressaten stammten. Dazu waren bei Erhebung der Daten keinerlei Hinweise erteilt worden; auch die Briefwerbung enthielt dazu keine Informationen. In dieser wurde allein auf den Adressdienstleister als Verantwortlichen für die Werbesendung und auf die Möglichkeit des Werbewiderspruchs diesem gegenüber hingewiesen.

Der HmbBfDI hat die gemeinnützige Organisation aufgefordert, zu dieser besonderen Werbeform und der damit einhergehenden Datenverarbeitung Stellung zu nehmen, insbesondere zu der Frage nach der Rechtsgrundlage für den Betrieb der personalisierten Websites.

Aus der schriftlichen Antwort und im Anschluss daran geführten Gesprächen ergab sich, dass es sich um eine erstmalig in dieser Form durchgeführte Werbeaktion handelte, die so ausgestaltet worden war, um die Rücklaufquote und damit im Ergebnis die Unterstützung für die von der Organisation geförderten Projekte zu erhöhen. Dabei wurden über die Namen der Werbeadressaten hinaus keine weiteren Informationen verarbeitet. Die Webeites waren nicht indexierbar und konnten nicht über Suchmaschinen gefunden werden, sondern allein über die konkreten – in den Schreiben angegebenen – Links und die richtige Schreibweise der Vor- und Nachnamen. Als Rechtsgrundlage für diese Datenverarbeitung berief die Organisation sich auf das berechtigte eigene sowie gemeinnützige Interesse, Art. 6 Abs. 1 lit. f) DSGVO. Die Hinweise des HmbBfDI darauf, dass Werbeadressaten, die in keinerlei Beziehung zur Hilfsorganisation stehen oder standen und keinerlei Informationen dazu erhalten haben, eine Verwendung ihrer Namen für personalisierte Websites nicht erwarten, führten zu einer Beendigung der Aktion und Löschung der personalisierten Websites.

Der HmbBfDI hat in dieser Sache zu Beginn des Berichtsjahres 2021 eine Verwarnung i. S. d. Art. 58 Abs. 2 lit. b) DSGVO ausgesprochen. Diese hat Bestandskraft erlangt.

2.5 Prüfung der Videokonferenzsysteme beim IT-Dienstleister Dataport

Gemeinsam mit den Datenschutzaufsichtsbehörden aus Schleswig-Holstein, Sachsen-Anhalt und Bremen prüft der HmbBfDI seit Mitte 2021 mehrere Softwarelösungen für Videokonferenzen beim IT-Dienstleister Dataport.

Bereits im Frühjahr 2020 zeichnete sich ab, dass Videokonferenzdienste in der Pandemie ein essentieller Faktor für das Gelingen

dezentraler Arbeitsweisen in der Pandemie sein werden. Im letzten Tätigkeitsbericht lag daher ein besonderer Fokus auf den durch die Datenschutzaufsichtsbehörden des Bundes und der Länder aufgestellten Anforderungen zu Videokonferenzdiensten. Dabei wurden gerade deren Einsatzzwecke in sensiblen Bereichen betrachtet (vgl. 29. TB II 5 und II 10).

In 2021 hat sich der HmbBfDI insbesondere mit dem Einsatz solcher Dienste in der hamburgischen Verwaltung beschäftigt (vgl. Kapitel IV 6 zum Verfahren Zoom). Zusätzlich zu den aus datenschutztechnischer Sicht teilweise intransparenten kommerziellen Diensten setzte sich der HmbBfDI mit transparenteren und datenschutzfreundlicheren Alternativen auseinander. So nutzt der HmbBfDI beispielsweise seit diesem Jahr selbst zum Zwecke der Medienbildung eine Plattform, die auf dem quelloffenen Dienst BigBlueButton basiert (vgl. Kapitel VII 3). Einen Gegenentwurf zu marktmächtigen kommerziellen Anbietern, welcher hohe Transparenz sowie digitale Souveränität zum Ziel hat, stellt auch das vollständig quelloffene „Projekt Phoenix" von Dataport dar (Vgl. https://www.dataport.de/was-wir-bewegen/portfolio/dphoenixsuite/ und 29. TB IV 1). Die dPhoenixSuite enthält neben einem Audio- und Videokonferenzen-Modul u.a. Module für die Erstellung von Texten, Tabellen und Präsentationen und für die E-Mail-Kommunikation. Die Suite steht mittlerweile grundsätzlich allen Trägerländern zur Verfügung und wird von Dataport auch außerhalb der Kernträgerländer Bremen, Hamburg, Sachsen-Anhalt und Schleswig-Holstein für den öffentlichen Sektor vertrieben. Das Modul zur Videokommunikation basiert auf dem ebenfalls quelloffenen Jitsi Meet und wird durch zusätzliche Chat- und andere Mehrwertfunktionalitäten ergänzt. In Anbetracht dessen, dass bei Phoenix alle Verarbeitungsschritte durch Dataport als öffentlichem IT-Dienstleister kontrolliert werden, besteht grundsätzlich die Möglichkeit, das gesamte Verfahren intensiv prüfen und vor allem an eigene Bedarfe anpassen (lassen) zu können. Der HmbBfDI hat daher mit den anderen Datenschutzaufsichtsbehörden der Dataport-Trägerländer eine gemeinsame Prüfung angestoßen, um die Videokonferenzdienste Dataports genauer zu

untersuchen. Ziel ist es, eine einheitliche Beurteilung der geprüften Dienste durch die Aufsichtsbehörden vorzunehmen. Prüfgegenstand stellen dabei zwei Produkte im Kontext des Projekts Phoenix dar, die unter dem Produktnamen dOnlineZusammenarbeit 1.0 sowie 2.0 vertrieben werden, als auch eine „Bestandslösung" zur Realisierung von Videokonferenzen auf Basis von Cisco mit dem Produktnamen dVideokommunikation.

Die Prüfung wurde Mitte 2021 begonnen und ist bislang noch nicht abgeschlossen. Zum jetzigen Zeitpunkt kann jedoch bereits nach erster Analyse festgehalten werden, dass diverse Unterlagen von Dataport zur Verfügung gestellt werden konnten, die in Umfang und Aussagekraft denen anderer (kommerzieller) Anbieter deutlich überlegen sind. Die Prüfung wird im Laufe des Jahres 2022 abgeschlossen.

Ob und – falls ja – in welchem Umfang sich die Cisco-basierte Videokonferenzlösung von den Jitsi-basierten Diensten unterscheidet und welche Implikationen dies für die verantwortlichen Stellen haben wird, die diese Dienste jeweils für ihre individuellen Einsatzzwecke nutzen, wird spätestens im nächsten Tätigkeitsbericht dargestellt werden.

2.6 Koordinierte Prüfung von Medienunternehmen

Erste Ergebnisse der koordinierten Medienprüfung haben ergeben, dass die eingeholten Einwilligungen durch den Einsatz von Cookie-Bannern auf den jeweiligen Websites meist unwirksam sind und Nachbesserungen vorgenommen werden müssen.

Im Rahmen der koordinierten Prüfung (siehe 29. TB, III 4) verschickten neben dem HmbBfDI die beteiligten Behörden ab Mitte August 2020 einen gemeinsam erarbeiteten Fragebogen an ausgewählte

Medienunternehmen in ihrer jeweiligen Zuständigkeit. Auf den geprüften Medienwebsites konnte eine sehr hohe Anzahl von Cookies und von den Anbietern eingebundenen Drittdiensten festgestellt werden, die überwiegend dem Nutzertracking und der Werbefinanzierung dienen.

Über die implementierten Cookie-Banner fragen die jeweiligen Websites zwar in der Regel differenzierte Einwilligungen der Nutzerinnen und Nutzer für die Verwendung von Cookies und Drittdiensten ab. Mehrheitlich sind diese Einwilligungen allerdings nicht wirksam (https://datenschutz-hamburg.de/pressemitteilungen/2021/06/2021-06-30-medienwebsites). Vor allem die folgenden Mängel wurden festgestellt:

Bereits durch den ersten Aufruf der Website werden einwilligungsbedürftige Drittdienste und Cookies eingebunden, ohne dass die Nutzerinnen und Nutzer zuvor die Möglichkeit hatten, überhaupt eine Einwilligung zu erteilen. Weiterhin bestehen erhebliche Mängel hinsichtlich der transparenten Darstellung der Datenverarbeitungsprozesse. Es werden nur unzureichende oder sogar falsche Informationen über die Nachverfolgung des Nutzerverhaltens gegeben.

Darüber hinaus hat die koordinierte Prüfung ergeben, dass selbst wenn individuelle Nutzereinstellungen vorgenommen werden, weiterhin zahlreiche Cookies und Drittdienste aktiv in die Website eingebunden bleiben, die durch die individuellen Einstellungen der Nutzerinnen und Nutzer zuvor eigentlich abgelehnt wurden. In diesem Zusammenhang erfolgen im Rahmen der Einwilligungsdialoge auch Hinweise zu Datenverarbeitungen auf der Grundlage eines berechtigten Interesses (Art. 6 Abs. 1 lit. f) DSGVO), was ferner den falschen Eindruck erweckt, auch in derartige Verarbeitungsprozesse könne oder müsse eingewilligt werden.

Sämtliche Einwilligungsbanner räumen den Nutzerinnen und Nutzern zudem die Möglichkeit ein, unmittelbar auf der ersten Ebene die Zustimmung zum Einsatz aller Cookies und Drittdienstleister zu

erteilen, wohingegen eine genauso einfache Möglichkeit, das Nutzertracking in Gänze abzulehnen oder das Banner ohne Entscheidung schließen zu können, nicht besteht.

Die Datenschutzaufsichtsbehörden haben sich im Rahmen der Anpassung der „Orientierungshilfe für Telemedienanbieter:innen" zur Frage der Einfachheit einer Ablehnungsmöglichkeit nun deutlich positioniert (https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf, S. 17):

„Wenn Nutzende beim Aufruf eines Telemedienangebotes eine Einwilligungsabfrage nicht einfach ignorieren können, weil diese Inhalte des Angebots verdeckt, fehlt es somit regelmäßig an der Freiwilligkeit der Einwilligung, wenn die Erteilung der Ablehnung mit einem höheren Aufwand, z. B. an Klicks und Aufmerksamkeit, verbunden ist. Um sicherzustellen, dass sie eine wirksame Einwilligung nachweisen können, müssen Anbieter:innen von Telemedien daher dringend darauf achten, die zur Auswahl gestellten Optionen gleichwertig zu gestalten."

Schließlich lassen die Ausgestaltungen der jeweiligen Einwilligungsbanner zahlreiche Formen des sog. Nudging erkennen. Hierbei werden auf subtile Weise Nutzerinnen und Nutzer unbewusst zur Abgabe einer Einwilligung gedrängt, indem die Schaltfläche für die Zustimmung beispielsweise durch eine farbliche Hervorhebung deutlich auffälliger gestaltet ist als die Schaltfläche zum Ablehnen bzw. für die individuellen Einstellungen oder indem die Verweigerung der Einwilligung unnötig verkompliziert wird oder die Schaltfläche für Einstellungen/Optionen gar nicht als anklickbare Schaltfläche zu erkennen ist.

Mögliche aufsichtsrechtliche Maßnahmen gegen die vom HmbBfDI geprüften Medienunternehmen werden derzeit geprüft. Auch hierbei wird über die Zusammenarbeit der deutschen Aufsichtsbehörden, die an der koordinierten Prüfung teilnehmen, ein vergleichbares Vorgehen sichergestellt.

BERICHTE 3.

3. Berichte

3.1 Weiterleitung von Transparenzanfragen an das LKA

Für die Weiterleitungen oder Übermittlungen von personenbezogenen Daten zwischen zwei öffentlichen Stellen bedarf es, wie bei allen anderen Datenverarbeitungsvorgängen auch, einer Rechtsgrundlage. Personenbezogene Daten aus Transparenzgesetzanfragen von Bürgerinnen und Bürgern dürfen von der auskunftspflichtigen Stelle daher nicht ungeprüft und ohne Vorliegen der gesetzlichen Voraussetzungen an Sicherheitsbehörden weitergegeben werden. Geschieht dies dennoch, ist auch die Speicherung bei den Sicherheitsbehörden unzulässig.

Im Juli 2021 hat ein Antragsteller nach § 11 Hamburgisches Transparenzgesetz (HmbTG) das Bezirksamt Altona per E-Mail gebeten über Zeit und Ort aller im Bereich des Bezirksamtes zu diesem Zeitpunkt angemeldeten und genehmigten Infostände der Parteien „Alternative für Deutschland“ (AfD); „Nationaldemokratische Partei Deutschland“ (NPD) und Basisdemokratische Partei Deutschland (die Basis) in den Monaten August und September 2021 unter konkreter Nennung der jeweiligen Daten, Uhrzeiten und Adressen Auskunft zu erteilen. Das zuständige Fachamt des Bezirksamts hatte diese E-Mail (inkl. Name und Adresse des Antragstellers) an das LKA 71 (Staatsschutz) der Polizei Hamburg weitergeleitet mit der Bitte um Einschätzung, ob die Beantwortung der Anfrage zu einer erweiterten Gefährdungslage für die Infostände führen könnte.

Der HmbBfDI vertritt die Auffassung, dass die (unaufgeforderte) Offenlegung der personenbezogenen Daten des Antragsstellers an das LKA nicht gerechtfertigt war: Die Verarbeitung von personenbezogenen Daten unterliegt dem Grundsatz der Zweckbindung (Art. 5 Abs. 1 Buchstabe b DSGVO). Danach ist eine Verarbeitung personenbezogener Daten zu anderen als den ursprünglichen Zwe-

cken nur unter bestimmten Voraussetzungen zulässig. Für öffentliche Stellen der Freien und Hansestadt Hamburg richtet sich die Zulässigkeit von zweckändernder Verarbeitung nach § 6 Hamburgisches Datenschutzgesetz (HmbDSG). Eine Übermittlung von personenbezogenen aus einem HmbTG-Verfahren an das LKA käme z.B. in Betracht, wenn die Übermittlung der Daten des Antragstellers zur Abwehr einer Gefahr für die öffentliche Sicherheit (§ 6 Abs. 2 Nr. 1 HmbDSG) oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich sind (§ 6 Abs. 2 Nr. 2 HmbDSG). Diese Voraussetzungen lagen hier jedoch nicht vor, weil sich aus der Anfrage keine tatsächlichen Anhaltspunkte oder Hinweise diesbezüglich ergaben. Eine Übermittlung der Daten war somit nicht gerechtfertigt.

Die Problematik ist beim HmbBfDI nicht neu: Anfragen zu Wahlständen rechtsradikaler Parteien wurden schon im TB Informationsfreiheit 2010/2011, Kap. 4.3 geschildert (damals allerdings ausschließlich aus informationsfreiheitsrechtlicher Sicht). Im TB Informationsfreiheit 2016/2017, Kap. 4.7, wurde das Problem erneut thematisiert. Damals wurde dem HmbBfDI mitgeteilt, dass die Angaben zum Teil standardisiert an Sicherheitsbehörden übermittelt werden, um diese über die Person des Antragsstellers in Kenntnis zu setzen. Der HmbBfDI hatte ein Ende dieser Praxis gefordert, was auch zugesagt wurde. Die nun gegenständliche Weiterleitung zielte augenscheinlich nicht drauf ab, das LKA auf den Antragsteller hinzuweisen, sondern erfolgte vielmehr mit dem Zweck, vom LKA eine Einschätzung der Gefährdungslage zu erhalten. Unabhängig von der Zielrichtung war die Weiterleitung der vollständigen Daten des Antragstellers nicht zulässig. Wir suchten das Gespräch mit dem Rechtsamt des Bezirksamts, das unsere Rechtsauffassung auf Grund der in den Vorjahren bereits erfolgten Klärung ohne Umschweife teilte. Es wurde zudem mitgeteilt, dass es sich bei der Weiterleitung der Transparenzanfrage des Antragsstellers inkl. der personenbezogenen Daten um ein einmaliges Versehen gehandelt habe. Die Daten des Anspruchstellers beim LKA wurden gelöscht. Eine erneute Sensibilisierung der Beschäftigten wurde zugesagt.

3.2 Kontaktnachverfolgung/Luca-App

Seit Anbeginn der Corona-Pandemie ist die Kontaktnachverfolgung ein entscheidendes Mittel zur Bewältigung der Krise gewesen. Nachdem sich bereits im Jahr 2020 gezeigt hat, dass offen ausgelegte Papierlisten dazu geführt haben, dass vielfach Personen falsche Kontaktdaten hinterlassen oder richtige von Dritten zweckwidrig genutzt wurden (Vgl. 29 TB, II 2), waren im Berichtszeitraum digitale Lösungen zur Kontaktnachverfolgung datenschutzrechtlich zu bewerten. Die Erfahrungen mit der analogen Kontaktnachverfolgung haben deutlich gezeigt, dass Datenschutz unverzichtbar ist, um das erforderliche Vertrauen in der Gesellschaft zu schaffen, womit die Wirksamkeit von Kontaktnachverfolgungsmaßnahmen überhaupt erst gewährleistet werden kann.

Dem HmbBfDI war und ist es wichtig, sich für eine datenschutzfreundliche Einhegung solcher digitaler Kontaktverfolgungssysteme einzusetzen. Daher beteiligte sich der HmbBfDI in einer von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) bestellten Taskforce. Unter der Leitung von Berlin und der Mitarbeit von Rheinland-Pfalz, Mecklenburg-Vorpommern, Baden-Württemberg und Hamburg erarbeiteten die Mitglieder dieser Taskforce eine von der DSK angenommene Stellungnahme („Kontaktnachverfolgung in Zeiten der Corona-Pandemie, Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden“, Stand: 26. März 2021) sowie eine Orientierungshilfe für Verantwortliche und Entwickler („Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurants- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19“, Stand: 29. April 2021).

In beiden Dokumenten hat die DSK besonders hervorgehoben, dass digitale Verfahren zur Verarbeitung von Kontakt- und Anwesenheitsdaten datenschutzkonform betrieben werden müssen. Nur dann können solche Lösungen die bessere Alternative zu Papierlisten sein.

Für den Einsatz in Hamburg wurde dem HmbBfDI mitgeteilt, dass der Senat sich entschlossen hatte, für eine digitale Kontaktnachverfolgung Lizenzen für die Luca-App zu erwerben, ein Dienst der Culture4life GmbH mit Sitz in Berlin. Die Hamburgischen Gesundheitsämter nutzten nach Lizenzierung die Applikation. Der HmbBfDI teilte der Kasse Hamburg u.a. auch unter Bezugnahme auf Medienberichten und Einschätzungen von unabhängigen Experten mit, dass datenschutzrechtliche Bedenken bezüglich des Einsatzes bestünden. Der Senat machte die Lizenzierung jedoch nicht von der Einschätzung des HmbBfDI abhängig und holte sich vorab keinen Rat ein.

In der Folgezeit erfolgten auf der Arbeitsebene konstruktive und kooperative Gespräche mit der Kasse Hamburg und der Sozialbehörde. Von Seiten der Stadt Hamburg bestand die Hoffnung, dass die Betreiber des Systems datenschutzrechtliche Verbesserungen vornehmen würden. Der HmbBfDI hielt Rücksprache mit den Kolleginnen und Kollegen der Aufsichtsbehörde in Berlin und es zeichnete sich ab, dass die erhofften Verbesserungen der Luca-App erheblich mehr Zeit in Anspruch nehmen würden. Daher wandte sich der HmbBfDI an die Senatorin für Arbeit, Gesundheit, Soziales, Familie und Integration und führte aus, dass die Gesamtschau der bekannt gewordenen Mängel zu dem Schluss geführt habe, dass die Luca-App nicht dem Stand der Technik entspräche und mit einer zeitnahen Beseitigung der wesentlichen Schwachstellen nicht zu rechnen sei. Gesundheitsämter müssten als datenschutzrechtlich verantwortliche Stellen dafür Sorge tragen, nicht auf unsichere technische Infrastrukturen zurückzugreifen.

Der HmbBfDI verwies wiederholt auf die vorzugswürdige Nutzung der Corona-Warn-App (CWA) des Robert-Koch-Instituts als eine sichere und datensparsame Lösung zur dezentralen Kontaktnachverfolgung.

Diese bietet eine mit der Luca-App vergleichbare Clustererkennung, bei der ebenfalls QR-Codes in Einrichtungen abgescannt werden können. Sie kann Nutzer bei möglichen Kontakten ohne Mitwirkung der Gesundheitsämter direkt und ohne weitere zeitliche Verzögerung warnen. Die 64. HmbSARS-CoV-2-Eindämmungsverordnung ermöglichte den Einsatz der CWA nicht. Der Senat hat sich dagegen entschieden, weil die CWA keine für Quarantäneanordnungen notwendigen Adressdaten liefern kann, diese jedoch zwingend nach § 7 HmbSARS-CoV-2-Eindämmungsverordnung anzugeben sind, soweit bereichsspezifisch die Verordnung zum Zweck der behördlichen Kontaktnachverfolgung die Pflicht zur Datenerhebung vorschreibt. Den Gästen, Kundinnen und Kunden sowie und Besucherinnen und Besuchern liefert die CWA gleichwohl die entscheidenden Informationen. Hier gilt es abzuwägen: Es wird zweifellos Einzelne geben, die sich trotz Warnung ihrer App nicht in Isolation begeben. In der Gesamtschau dürfte die Corona-Warn-App aber mehr Infektionsketten unterbrechen, da die Betroffenen direkt und ohne verzögerten Umweg über die Gesundheitsämter informiert werden.

Vor diesem Hintergrund bat der HmbBfDI die Senatorin zu prüfen, in Hamburg durch eine Änderung der HmbSARS-CoV-2-Eindämmungsverordnung den Einsatz der CWA für diesen Zweck zu eröffnen.

Der Senat hat sich zunächst nicht für eine Änderung der HmbSARS-CoV-2-Eindämmungsverordnung entschieden.

In den letzten Monaten des Berichtszeitraums hat sich die pandemische Lage dergestalt geändert, dass nunmehr nach der Erforderlichkeit einer flächendeckenden Erhebung von Kontaktdaten zu fragen ist. Aufgrund der massiven Überlastung der Gesundheitsämter findet keine bzw. nur noch in Einzelfällen – etwa in Pflegeheimen oder Krankenhäusern – eine Kontaktnachverfolgung durch die Gesundheitsämter statt. Es bietet sich insofern an, zumindest in allen anderen Bereichen des öffentlichen Lebens auf die CWA als probates Mittel zu setzen.

Erst im Februar 2022 wurde mit der 65. Änderungsverordnung die bereichsspezifische Streichung der Pflicht zur Kontaktdatenerhebung beschlossen.

3.3 Schule in Zeiten von Corona

Mit dem Fortgang der Pandemie und veränderten Schutzmaßnahmen und Unterrichtskonzepten stellten sich laufend neue datenschutzrechtliche Fragen, die auch von Gerichten zu beantworten waren.

Auch im zweiten Jahr der COVID-19 Pandemie führte diese im Schulbereich zu einer steigenden Anzahl an Eingaben beim HmbBfDI, da es pandemiebedingt zu einer Vielzahl von neuen Verarbeitungen personenbezogener Daten der am Schulbetrieb beteiligten Personen kam.

Formate zum Distanzunterricht führten zu Datenverarbeitungsvorgängen im Rahmen der Verwendung von Videokonferenzsystem und digitalen Lerntools. Durch Maßnahmen zur Vermeidung von gesundheitlichen Risiken und Vorbeugung vor Ansteckungen kam es zu verschiedenen Datenverarbeitungssituationen, auch von Gesundheitsdaten, die dem besonderen Schutz des Art. 9 Datenschutz-Grundverordnung (DSGVO) unterliegen und Gegenstand verschiedener Eingaben beim HmbBfDI wurden.

Die Frage der datenschutzrechtlichen Zulässigkeit der Verarbeitung von personenbezogenen Daten durch die Hamburger Schulen und die Behörde für Schule und Berufsbildung (BSB) im Rahmen von pandemiebedingten Schutzmaßnahmen spitzte sich insbesondere bei der Frage der Zulässigkeit der verpflichtenden Corona-Testung der Schülerinnen und Schüler, die im Klassenverband durchgeführt werden, zu. Während das Testergebnis unstreitig als Gesundheitsdatum

im Sinne von Art. 9 DSGVO einzuordnen ist, stellte sich die Frage, ob die mit der Testung im Klassenverband zwangsläufig verbundene Offenlegung dieses Datum gegenüber Dritten datenschutzrechtlich zulässig sein kann. Diese Frage wurde parallel zu den hier vorgenommenen Prüfungen durch das Verwaltungsgericht Hamburg entschieden. Das Verwaltungsgericht stellte in seinem Urteil vom 29.04.2021 zum Aktenzeichen 2 E 1710/21 zunächst grundsätzlich fest, dass die in § 23 Abs. 1 Satz 3 Nr. 3 HmbSARS-CoV-2-EindämmungsVO geregelte Beschränkung des Zugangs zu Präsenzangeboten an der Schule durch die verpflichtende Teilnahme an einem Corona-Test als eine notwendige Schutzmaßnahme im Sinne des Infektionsschutzgesetzes zulässig ist und die daraus folgenden Datenverarbeitungsvorgänge mit den Vorschiften der DSGVO vereinbar sind. Daran anschließend ist die Selbsttestung der Schülerinnen und Schüler im Klassenverband nach den Ausführungen des Verwaltungsgerichts dann zulässig, wenn den Schülerinnen und Schülern die Möglichkeit gegeben wird, sich diesem Testverfahren im Klassenverband durch Vorlage eines Testergebnisses aus einem Test bei einem Testanbieter § 6 Abs. 1 Satz 1 Coronavirus-Testverordnung zu entziehen, um damit eine Offenlegung des Testergebnisses gegenüber Mitschülerinnen und Mitschüler vermeiden zu können. Diese Möglichkeit war durch die Musterhygienepläne der BSB vor dieser gerichtlichen Entscheidung nicht eingeräumt worden. Die Musterhygienepläne wurden aber aufgrund dieses Urteils durch die BSB angepasst.

Zum Einsatz von Videokonferenzsystemen wurde bereits im 29. Tätigkeitsbericht des HmbBfDI (dort Kapitel II 5) berichtet. Das von der Behörde für Schule und Berufsbildung für den Distanzunterricht geschaffene Lernmanagementsystem „Lernen Hamburg“ wurde im Jahr 2021 weiter ausgebaut. Es wurden seitens der Behörde weitere Serverkapazitäten geschaffen, um der wachsenden Nachfrage bei den Schulen zur Anwendung dieses Systems Rechnung zu tragen und einen belastbaren Betrieb des Systems zu ermöglichen. Da dieses System auch für alle beruflichen Schulen zur Verfügung gestellt wurde und dort zum Einsatz kam, sorgte eine beim HmbBfDI eingehende Eingabe zur geplanten Einführung von Microsoft 365 an allen beruf-

lichen Schulen in Hamburg durch das Hamburger Institut für berufliche Bildung (HIBB) für Überraschung. Der HmbBfDI wurde bei der Planung dieses großflächigen Projektes nicht beteiligt. obwohl es sich bei Microsoft 365 um ein bundesweit datenschutzrechtlich höchst umstrittenes Produkt handelt. Im Rahmen eines Modellprojektes zum Einsatz von Microsoft 365 an beruflichen Schulen in Baden-Württemberg, bei dem eine Zusammenarbeit des dortigen Kultusministeriums mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit stattfand, wurde beispielsweise ein hohes datenschutzrechtliches Risiko beim Einsatz dieses Dienstes festgestellt (https://www.baden-wuerttemberg.datenschutz.de/lfdi-raet-aufgrund-hoher-datenschutzrechtlicher-risiken-von-der-nutzung-der-geprueften-version-von-microsoft-office-365-an-schulen-ab/). Deswegen ist auch auf Ebene der KMK eine AG eingesetzt worden, die unter Einbindung der DSK prüft, ob MS 365 überhaupt im Schulbereich eingesetzt werden kann. Unsere Bedenken wurden nun zumindest insoweit aufgegriffen, als das HIBB die flächendeckende Einführung zunächst ausgesetzt hat, bis wir belastbare Unterlagen, die uns mittlerweile vorliegen, geprüft haben.

3.4 Hochschulländerungsgesetz

Nach einem längeren Abstimmungsprozess wurde eine Anpassung der datenschutzrechtlichen Vorschriften im Hamburgischen Hochschulrecht an einen pandemiebedingt veränderten Lehrbetrieb beschlossen.

Im Hochschulbereich machte die COVID-19-Pandemie zur Vermeidung von Infektionsrisiken und dadurch notwendige Distanzformate eine Umstellung des Lehrbetriebs notwendig und stellte die Hamburger Hochschulen und die Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke (BWFGB) vor tatsächliche, technische und damit auch rechtliche Herausforderungen.

Die dadurch vorangetriebene Digitalisierung der Lehre warf durch den Einsatz von Videokonferenzsystemen, Lernplattformen und anderen digitalen Lernformaten verschiedene datenschutzrechtliche Fragen auf, die durch die BWFGB mit einem unter dem Titel „Digitalisierung von Lehre und Prüfungen“ zusammengefassten Gesetzesvorhaben gelöst werden sollten.

In die Diskussion, Anpassung und Veränderung des Gesetzentwurfs wurde der HmbBfDI von Seiten der BWFGB umfassend einbezogen und seine Einwände umfänglich erörtert. Die Gesprächsrunden auch unter Einbeziehung von Hochschulvertreter:innen zeigten, dass dem Spannungsfeld aus hochschulseitig pädagogisch begründeten, weit gewünschten Datenverarbeitungsbefugnissen auf der einen Seite und datenschutzrechtlich einzuhaltenden Verarbeitungsgrundsätzen, wie Rechtmäßigkeits-/Verhältnismäßigkeitserwägungen und Datenminimierungsgesichtspunkten auf der anderen Seite eine besondere Bedeutung zukam.

Dieses Spannungsfeld wurde an bestimmten Eckpunkten, wie der Frage nach der Zulässigkeit der Aufzeichnung von digitalen Lehrveranstaltungen und der Zulässigkeit der Überwachung von Studierenden im Rahmen von digitalen Prüfungen einschließlich deren Aufzeichnung, besonders deutlich. Bei der Aufzeichnung von digitalen Lehrveranstaltungen kann es zu einer Aufzeichnung von Ton- und Bilddaten von Studierenden kommen, die nicht nur einen personenbezogenen Charakter, sondern je nach Format und Thema der Veranstaltung auch einen besonders persönlichen, schutzwürdigen und sensiblen Inhalt haben können. Gleiches gilt für die Aufzeichnung der Videoaufsicht einer Online-Prüfung, die ggf. Bilder von und aus dem engsten Privatbereich der Studierenden, nämlich ihrer Privatwohnung, festhält. Dieser Eingriffsintensität galt es bei der Formulierung gesetzlicher Regelungen ausreichend Rechnung zu tragen.

Am Ende des Abstimmungsprozesses stand ein Entwurf, der Änderungen im Hamburgischen Hochschulgesetz (HmbHG), insbesondere in § 111 Abs. 2-4 HmbHG und in § 3 des Gesetzes zur Bewältigung

der Auswirkungen der COVID-19-Pandemie im Hochschulbereich, vornahm.

Die Vorschrift in § 111 Absatz 2 HmbHG sollte nun eine Rechtsgrundlage für die Hochschulen enthalten, digitale Lehrveranstaltungen durchzuführen und die dafür erforderlichen personenbezogenen Daten von Teilnehmerinnen und Teilnehmern verarbeiten zu dürfen. Für § 111 Absatz 3 HmbHG wurde eine Regelung zur Verarbeitung von personenbezogenen Daten im Rahmen von digitalen Prüfungen zur Videoaufsicht und Authentifizierung der zu prüfenden Studierenden entworfen. Da eine Videoaufsicht im Rahmen einer digitalen Distanzprüfung unter Umständen eine eingriffsintensive Maßnahme darstellt, weil sie Einsicht in die privaten Räumlichkeiten und damit in die Privatsphäre als Schutzbereich der Studierenden ermöglicht, wurden auf Einwände des HmbBfDI Beschränkungen dieses Eingriffs aufgenommen. Insbesondere sollten danach eine Aufzeichnung der Videoaufsicht und eine automatisierte Auswertung nicht zulässig sein. Zudem sollte die Teilnahme einer digitalen Prüfung unter Videoaufsicht nur freiwillig möglich sein.

Die entworfene Regelung in § 3 des Gesetzes zur Bewältigung der Auswirkungen der COVID-19-Pandemie im Hochschulbereich enthielt zwar eine Befugnis für die Hochschulen, Online-Veranstaltungen durch Bild- und Tonaufnahmen aufzuzeichnen, die aber durch verschiedene Zusätze eine Beschränkung in der Weiterverarbeitung des Aufzeichnungsergebnisses beinhaltete. Zudem wurde durch die Aufnahme dieser Befugnisse in dieses Gesetz und dessen zeitliche Befristung der pandemiebedingte Ausnahmecharakter dieser Datenverarbeitungsbefugnis betont.

Der Gesetzentwurf wurde aus der Mitte der Bürgerschaft beschlossen und als Gesetz vom 17.06.2021 am 18.06.2021 im Hamburgischen Gesetz und Verordnungsblatt Nr. 43 bekannt gegeben. Im Ergebnis liegt eine gesetzliche Regelung vor, die ernsthaft und sichtlich bemüht ist, datenschutzrechtliche Einschränkungen zum Schutz der Rechte und Freiheiten Betroffener zu formulieren und diese in

Einklang mit an praktischen Bedürfnissen orientierten Forderungen der Hochschulen zu bringen.

3.5 Zensus 2022

Der Zensus 2022 ist in Sichtweite. Der HmbBfDI wird die laufenden Vorbereitungen und die Durchführung der Volkszählung intensiv und kritisch begleiten und auch nach Abschluss der Befragungen die Einhaltung der gesetzlichen Löschfristen überwachen.

Nach geltendem EU-Recht müssen die Mitgliedstaaten alle zehn Jahre eine Volkszählung (Zensus) durchführen. Da der letzte Zensus 2011 stattfand, war die aktuelle Volkszählung zunächst für 2021 vorgesehen. Aufgrund der Auswirkungen der Corona-Pandemie und der aufwändigen Vorbereitung musste der Zensus auf das Jahr 2022 verschoben werden. Neuer Stichtag ist der 15. Mai 2022.

Der Zensus dient der Ermittlung von Basisdaten zur Bevölkerung, Erwerbstätigkeit und Wohnsituation als Grundlage der amtlichen Statistik. Eine zentrale Aufgabe ist die statistische Ermittlung der amtlichen Einwohnerzahlen. Der Zensus 2022 ist erneut als registergestützte Bevölkerungsbefragung angelegt. Das bedeutet, dass nicht alle Bürgerinnen und Bürger befragt werden, sondern in großem Umfang bestehende Datenbestände der staatlichen Verwaltungsregister, wie etwa der Melderegister, als Basisinformation genutzt werden. Dadurch kann die sogenannte Haushaltebefragung auf eine Stichprobe von etwa 10% der Bevölkerung begrenzt werden. Zusätzlich werden an Anschriften mit Sonderbereichen die Bewohnerinnen und Bewohner von Wohnheimen befragt. In Gemeinschaftsunterkünften sind die Einrichtungsleitungen auskunftspflichtig. Bei der Gebäude- und Wohnungszählung (GWZ) werden die Eigentümerinnen und Eigentümer, Verwaltungen sowie sonstige

verfügungs- oder nutzungsberechtigte Personen aller Wohngebäude bzw. Wohnungen befragt.

Das Bundesverfassungsgericht (BVerfG) hat in seiner Entscheidung vom 19. September 2018 (2 BvF 1/15; 2 BvF 2/15) über die Normenkontrollanträge der Länder Berlin und Hamburg diese Methode als verfassungskonform bestätigt.

Für die datenschutzrechtliche Begleitung des Zensus 2022 wurde durch den Arbeitskreis Statistik der Datenschutzkonferenz eine Arbeitsgruppe gebildet, welcher der HmbBfDI angehört. Diese Arbeitsgruppe hat im Rahmen der Beteiligung an den Gesetzgebungsverfahren zum Zensusvorbereitungsgesetz 2022 und zum Zensusgesetz 2022 datenschutzrelevante Bedenken vorgebracht und Änderungsvorschläge erarbeitet, welche jedoch nicht in vollem Umfang Berücksichtigung fanden. Wesentliche Kritikpunkte am Zensusgesetz betreffen die nicht anonyme Erhebung in sensiblen Sonderbereichen, wie z.B. Justizvollzugsanstalten, die weiterhin vorgesehene Vollerhebung bei der GWZ, die verpflichtende Erhebung der Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft – zumal der deutsche Gesetzgeber hier die EU-Vorgaben überschreitet.

Neu beim Zensus 2022 ist die erstmals zentral dem Statistischen Bundesamt obliegende Verwaltung des Gesamtdatenbestandes. Daher war hinsichtlich der Zusammenarbeit der Statistischen Ämter des Bundes und der Länder im sogenannten statistischen Verbund eine eindeutige und trennscharfe Regelung der datenschutzrechtlichen Verantwortung gefordert worden.

Beim Zensusvorbereitungsgesetz steht der später eingefügte § 9a in der Kritik. Dieser regelt die Übermittlung bestimmter Daten sämtlicher zu einem angegebenen Stichtag in den deutschen Melderegistern gespeicherten Personen an die Statistischen Ämter. Dies sollte der Überprüfung der Übermittlungswege und der Qualität der übermittelten Datensätze und der Weiterentwicklung der Programme zur Zensusdurchführung dienen. Ein gegen diesen Test mit Echt-

daten beim BVerfG gestellter Eilantrag wurde mit Entscheidung vom 6. Februar 2019 (1 BvQ 4/2019) abgelehnt. Der Ausgang des Verfassungsbeschwerdeverfahrens ist jedoch noch offen.

Im Zuge der laufenden praktischen Vorbereitungen für die Durchführung des Zensus 2022 hat der HmbBfDI in mehreren Informations- und Beratungsgesprächen mit dem Statistischen Amt für Hamburg und Schleswig-Holstein datenschutzrechtliche und –technische Fragestellungen erörtert und wird dies auch weiterhin tun.

Nach Umsetzung der geplanten Verwaltungsregistermodernisierung in Deutschland sollen zukünftige Zensen ausschließlich registerbasiert durchgeführt werden und gänzlich ohne Befragungen der Bevölkerung auskommen. Die dafür erforderlichen Verknüpfungen von Informationen aus bestehenden und noch neu zu errichtenden Verwaltungsregistern unterschiedlicher Bereiche werden den Datenschutz vor neue Herausforderungen stellen.

3.6 Löschung von Bewerbungsunterlagen

Wann Bewerbungsunterlagen nach einem erfolglosen Auswahlverfahren zu löschen sind, hängt maßgeblich davon ab, ob die ausschreibende Stelle eine öffentliche oder nicht-öffentliche Stelle ist.

Im Berichtszeitraum erreichten dem HmbBfDI immer wieder Fragen sowohl von Arbeitgeberinnen und Arbeitgebern als auch von Bewerberinnen und Bewerbern zur Löschung von Bewerbungsunterlagen nach Beendigung des Auswahlverfahrens. In der überwiegenden Anzahl der Fälle stellte sich die Frage der Speicher- bzw. Löschfristen der Bewerbungsunterlagen nach Abschluss eines Bewerbungsverfahrens.

Sofern das Bewerbungsverfahren mit einer positiven Auswahlentscheidung endet, sind die Bewerbungsunterlagen in die Personalakte (wenn vorhanden) zu überführen. Endet das Bewerbungsverfahren hingegen mit einer Ablehnung (sog. Negativentscheidung), sind die Bewerbungsunterlagen der unterlegenen Bewerberinnen und Bewerber zu löschen (beziehungsweise an die Bewerberin oder den Bewerber zurückzugeben).

Art. 88 Abs. 1 DSGVO i.V.m. § 26 BDSG als Rechtsgrundlage für die Verarbeitung von Bewerberdaten im nicht-öffentlichen Bereich schweigt hierzu. Datenschutzrechtlich ergibt sich diese Verpflichtung daher aus den Grundsätzen der Datenminimierung und der Speicherbegrenzung. Personenbezogene Daten sind folglich unverzüglich zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Der Zweck ist hier das Bewerbungsverfahren, das mit dem Ablehnungsschreiben endet, sodass die Bewerbungsunterlagen nach Absenden des Ablehnungsschreibens gelöscht werden müssen. Beide Grundsätze können sich aber sowohl für die ausschreibende Stelle als auch für die unterlegenen Bewerberinnen und Bewerber nachteilig auswirken und zu einer Beweisnot führen, nämlich dann, wenn Rechtsansprüche aus dem Bewerbungsverfahren von unterlegenen Bewerberinnen und Bewerbern geltend gemacht werden. Daher ist es datenschutzrechtlich vertretbar, dass die ausschreibende Stelle die Bewerbungsunterlagen und/oder eine Dokumentation über das Bewerbungsverfahren für einen gewissen Zeitraum aufbewahrt, um sich gegen Rechtsansprüche der unterlegenen Bewerberin bzw. Bewerber zu verteidigen. Entscheidend für die Länge der Frist ist die Frage, innerhalb welchen Zeitraums nach Zugang eines Ablehnungsschreibens Rechtsansprüche von unterlegenen Bewerberinnen und Bewerbern eingehen können.

Als Maßstab wird hier die Frist von sechs Monaten gesehen. Diese Frist ergibt sich aus dem Allgemeinen Gleichbehandlungsgesetz (AGG) bei einem etwaigen Verstoß gegen das Benachteiligungsverbot. Diese Frist berechnet sich wie folgt: Nach dem AGG müssen Schadensersatz- oder Entschädigungsansprüche innerhalb einer Zweimo-

natsfrist nach Zugang des Ablehnungsschreibens geltend gemacht werden (§ 15 Absatz 4 AGG). Nur wenn innerhalb dieses Zeitraums Ansprüche gegenüber der Arbeitgeberin oder dem Arbeitgeber erhoben werden, schließt sich die dreimonatige Frist des § 61b Absatz 1 Arbeitsgerichtsgesetz an, die mit der schriftlichen Geltendmachung des Anspruchs gegenüber dem Arbeitgeber nach § 15 Absatz 4 Satz 1 AGG beginnt. Im Ergebnis führt dies zu einer Aufbewahrungsfrist von fünf Monaten plus einem Monat für die Abwicklung.

Verantwortliche Stellen dürfen jedoch nicht auf die starre Speicherfrist von sechs Monaten beharren, wenn die betroffene Person spätestens zwei Monate nach Erhalt des Ablehnungsschreibens die Löschung ihrer personenbezogenen Daten begehrt und in der Zwischenzeit keine Schadensersatz- oder Entschädigungsansprüche geltend gemacht wurden. In diesen Fällen entfällt die Erforderlichkeit der weiteren Speicherung und die Daten sind umgehend zu löschen.

Möchte ein Arbeitgeber die personenbezogenen Daten darüber hinaus speichern (zum Beispiel zum Zwecke einer zukünftigen Berücksichtigung bei weiteren Stellenangeboten), bedarf es der ausdrücklichen und schriftlichen oder elektronischen Information und Einwilligung der Bewerberinnen und Bewerber. Diese sollte im Idealfall mit der Absendung des Ablehnungsschreibens oder – abhängig von der Ausgestaltung des Bewerbungsverfahrens – zu Beginn des Bewerbungsverfahrens eingeholt werden.

Anders sieht es jedoch im öffentlichen Bereich aus. Hier hat der Gesetzgeber in § 10 Abs. 6 HmbDSG zwar eine ausdrückliche und unverzügliche Löschverpflichtung bei erfolglosen Bewerbungsverfahren vorgesehen. Eine Einschränkung dieses Grundsatzes enthält jedoch Satz 2 bei Vorliegen überwiegender berechtigter Interessen der Daten verarbeitenden Stelle.

Überwiegende berechtigte Interessen können auch hier Ansprüche nach dem AGG sein. Allerdings besteht auch die Möglichkeit, Bewerbungsunterlagen für einen längeren Zeitraum als sechs Mona-

te zu speichern und zwar dann, wenn Ablehnungsbescheide nicht mit einer Rechtsbehelfsbelehrung versehen werden. In diesen Fällen müssen Bewerbungsunterlagen aufgrund der Notwendigkeit zur Beweisführung bei potentiellen Konkurrentenklagen mindestens für die Dauer von einem Jahr gespeichert werden.

Der HmbBfDI erfuhr im Rahmen der Prüfung der Digitalisierung des Bewerbungsverfahrens und der Einführung des Bewerbungsmanagement Systems in der FHH (BMS-Verfahren), dass die FHH personenbezogene Daten unterlegener Bewerberinnen und Bewerbern regelhaft für die Dauer von 400 Tagen speichert. Eine daraufhin eingeholte Stellungnahme vom Personalamt ergab, dass Absageschreiben an die unterlegenen Bewerberinnen und Bewerber in der FHH üblicherweise nicht mit einer Rechtsbehelfsbelehrung versehen werden, sodass zumindest theoretisch etwaige Rechtsmittel noch bis zu einem Jahr nach der Absage eingelegt werden könnten. Daher müssen die Bewerbungsdaten nach Abschluss des Auswahlverfahrens regelmäßig noch mindestens 400 Tage (Jahresfrist + 35 Tage für die Abwicklung) aufbewahrt werden.

Die Speicherdauer ist datenschutzrechtlich nicht zu beanstanden, denn gem. § 37 HmbVwVfG besteht keine Pflicht, Verwaltungsakte mit einer Rechtsbehelfsbelehrung (RBB) zu versehen (anders im Bundesrecht gem. § 37 Abs. 6. VwVfG, wonach schriftliche oder elektronische Verwaltungsakte, die der Anfechtung unterliegen, mit einer RBB versehen werden müssen). Eine Pflicht zur Erteilung einer RBB ergibt sich auch nicht aus § 58 VwGO, ebenso wenig aus dem Rechtsstaatsprinzip des Art. 20 GG, dem Recht auf effektiven Rechtsschutz des Art. 19 Abs. 4 GG oder dem Gleichheitsgrundsatz des Art. 3 GG. Es existieren auch keine anderweitigen gesetzlichen Vorschriften, die eine derartige Pflicht statuieren, sodass die ausschreibenden Behörden demgemäß nicht verpflichtet sind, ihre – anfechtbaren – Entscheidungen mit einer RBB zu versehen.

Überwiegende berechtigte Interessen können bei mehrstufigen Bewerbungsverfahren mitunter auch zu verhältnismäßig langen

Speicherfristen führen. Diese langen Speicherfristen können datenschutzrechtlich erforderlich und damit vertretbar sein, wenn sich das Bewerbungsverfahren durch Besonderheiten und mehrere Prüfungsetappen auszeichnet. So sind z.B. bei der Polizei die gesundheitlichen Voraussetzungen eingehend geregelt. Ansonsten geeignete Bewerberinnen und Bewerber können zunächst aus behebbaren Gründen (z.B. fehlender Nachweis der Schwimmbefähigung oder fehlende erforderliche Bildungsvoraussetzungen) scheitern. Bei einer größeren Zahl von Wiederholungsbewerbungen kann es auch sachgerecht sein, das Einstellungsverfahren nicht wiederholt in allen Stufen durchzuführen, wenn eine erhebliche Anzahl solcher Bewerbungen schon durch einen Rückgriff auf frühere Unterlagen ausgeschlossen werden kann, so z.B. wenn die Bewerberin oder Bewerber als absolut ungeeignet für den Polizeivollzugsdienst eingestuft wurden. Gerade bei diesen Bewerberinnen und Bewerbern, ist jedoch zu beachten, dass die Speicherfristen dabei nicht als absolute und starre Speicherfristen ausgerichtet sein dürfen, sondern als Prüffrist angelegt werden müssen, um das Recht auf informationelle Selbstbestimmung zu wahren.

Unter Umständen sind nämlich auch bei als absolut ungeeignet eingestuften Bewerberinnen und Bewerbern Konstellationen denkbar, die bei einer Neubewertung zu einer anderen Einstufung führen können. Dies kann Bewerberinnen und Bewerber betreffen, die sich als Jugendliche oder Heranwachsende bei der Polizei bewerben und Ermittlungsverfahren verschweigen, weil sie die betreffenden Risiken, Folgen und Garantien nicht einschätzen können. Längst vergangene „Jugendsünden“ würden so zu einer Stigmatisierung führen, die bis zum Ablauf des Einstellungsalters (bis zum 35. Lebensjahr) andauern kann. Hierauf hat der HmbBfDI die Polizei Hamburg im Rahmen der Prüfung einer Beschwerde aufmerksam gemacht. Die Polizei Hamburg konnte die Argumentation des HmbBfDI nachvollziehen und hat Ende November dem HmbBfDI einen Entwurf vorgelegt, wonach die absolute und starre Speicherfrist bei absolut ungeeigneten Bewerberinnen und Bewerbern um eine Prüffrist ergänzt wurde. Vorgesehen ist nunmehr eine zwischengeschaltete Prüffrist von drei

Jahren. Sofern der Status „absolut ungeeignet“ weiterhin vergeben werden soll, müssen die Gründe, die zu einer längeren Speicherung im Einzelfall führten, hinsichtlich ihres Fortbestands überprüft und dokumentiert werden. Die diesbezüglichen Prozesse in der Polizeiakademie wurden bereits angepasst.

3.7 IT-Forensik und datenschutztechnische Prüfungen beim HmbBfDI

Der HmbBfDI hat eine standardisierte Vorgehensweise für forensische Prüfungen etabliert.

Im Zuge von Prüfungen und Beschwerden muss zunächst festgestellt werden, welche Daten auf einem Gerät, etwa einem Smartphone oder USB-Stick gespeichert und verarbeitet wurden. Auch zuvor gelöschte und dann rekonstruierte Daten können für die Sachverhaltsaufklärung von Interesse sein. Bei diesen technischen Prüfungen des HmbBfDI ist es von hoher Relevanz, aussagekräftige und belastbare Informationen über den jeweiligen Prüfgegenstand zu gewinnen, die letztlich eine gerichtsfeste Qualität aufweisen. Die daraus gewonnenen Erkenntnisse bilden die Grundlage für die Beurteilungen, ob datenschutzrechtliche Verstöße vorliegen und ob und welche Sanktionen verhängt werden. Dabei war in den vergangenen Jahren ein Anstieg solcher technischen Prüfungen zu verzeichnen, die der HmbBfDI zum Anlass genommen hat, für bestimmte Teilbereiche standardisierte Prozesse zu etablieren. Insbesondere anlassbezogene Prüfungen, in denen Speichermedien auszuwerten waren, stellen zunehmend einen solchen Bereich dar.

Für die bisherige aufsichtsbehördliche Praxis beim HmbBfDI waren Auswertungen von Speichermedien wie u.a. (externe) Festplatten, USB-Sticks, SD-Karten und auch Speicher von Smartphones für die Aufklärung von Sachverhalten im Rahmen technischer Prüfun-

gen von Bedeutung. Um solche Speichermedien und die auf ihnen gespeicherten personenbezogenen Daten beurteilen und würdigen zu können, ist es wichtig, einheitliche und abgestimmte Analyseprozesse zu definieren, die von externen Stellen – wie etwa Gerichten – nachvollzogen und evaluiert werden können. Der HmbBfDI hat daher zum Zwecke der Datenträgeruntersuchung ein standardisiertes Vorgehen definiert: Zunächst werden diese Datenträger/Speichermedien gesichert, ohne dass die Speichermedien verändert werden. Erst dann folgt die Analyse, die lückenlos dokumentiert wird.

Die Vorgehensweise basiert auf dem Leitfaden IT-Forensik des Bundesamtes für Sicherheit in der Informationstechnik (BSI), mit der die Vollständigkeit und Integrität sowie Authentizität sichergestellt wird. Sie umfasst dabei u.a. die integritätsgesicherte Erstellung forensischer Duplikate mittels sog. WriteBlocker sowie eine Auswertung auf Basis von Werkzeugen, die dem aktuellen Stand der Technik entsprechen. In der Regel sind die genutzten Programme quelloffen in der IT-Security-Community entwickelt worden. Der Untersuchungsumfang wird dabei stets zu Beginn der jeweiligen Überprüfung festgelegt und alle Schritte dieses Prozesses dokumentiert. Die notwendige Hardwareausstattung wurde in den vergangenen Jahren stets zielgerichtet beschafft, sodass die benötigten Ressourcen zur Verfügung stehen. Durch externe Schulungen konnte das notwendige Know-how bei den zuständigen Mitarbeiterinnen und Mitarbeitern ausgebaut werden. Der HmbBfDI geht davon aus, dass sich die geschilderte Entwicklung zur Notwendigkeit solcher technischen Untersuchungen im Laufe der kommenden Jahre weiter fortsetzen und sogar erhöhen wird. Auch ist davon auszugehen, dass zukünftig im Rahmen anlassloser Prüfungen sowie Meldungen der verantwortlichen Stellen über Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO (Data Breaches) ebensolche Methodiken durch den HmbBfDI zunehmend genutzt werden. Der Austausch mit anderen Datenschutzaufsichtsbehörden wird dabei einerseits die Bewertung deutschlandweit und auch auf europäischer Ebene vereinheitlichen und andererseits durch den fachlichen Austausch

auch bezüglich der Qualität datenschutztechnischer Prüfungen zu Mehrwerten in der aufsichtsbehördlichen Praxis führen.

An dieser Stelle sei deutlich betont, dass der unberechtigte Zugang zu Daten, die besonders gesichert sind, oder gar die Nutzung von Backdoors im Rahmen dieser technischen Prüfungen eine klare Grenze darstellen und zu keinem Zeitpunkt geplant waren. Im Gegenteil positioniert sich der HmbBfDI seit etlichen Jahren klar dafür, dass IT-Sicherheitslücken schnellstmöglich zu schließen sind, damit alle Personen sicher sein können, dass ihre personenbezogenen Daten nur ihnen und ausdrücklich Berechtigten zugänglich gemacht werden. Im Rahmen der o.g. Prüfungen findet außerdem stets eine Abwägung zwischen den durchzuführenden Eingriffen – teilweise bei privaten Endgeräten – und dem im Raum stehenden datenschutzrechtlichen Verstoß statt.

3.8 Beschwerden der Organisation NOYB

Im August 2021 wurden von der Nichtregierungsorganisation NOYB mehrere Beschwerden wegen der Verwendung von „Dark Patterns“ und „Nudging“ in Cookie-Bannern eingereicht. Weitere Beschwerden richteten sich gegen den Einsatz von „Bezahlmodellen“ auf Medien-Websites.

3.8.1 Beschwerden wegen „Dark Patterns“ und „Nudging“

Mit 422 Beschwerden wendet sich NOYB gegen Betreiber von Websites. Gegenstand der Beschwerden ist der Einsatz von Consent-Bannern, durch die, nach Auffassung von NOYB, die unzulässige Beeinflussung von Nutzerinnen und Nutzern bei der Erteilung ihrer Einwilligung zum Tracking erfolgt. Im Rahmen seiner Zuständigkeit prüft der HmbBfDI fünf dieser Beschwerden.

Personenbezogene Daten sind aus Sicht vieler Betreiber von Telemedien erst interessant, wenn diese Daten wirtschaftlich verwertbar

sind. Die Datenverarbeitung zur – in der Regel geräteübergreifenden – Nachverfolgung des individuellen Verhaltens von Nutzerinnen und Nutzern (Tracking) ist ein wichtiger Faktor im Wettbewerb, um beispielsweise personalisierte Werbung ausspielen zu können. Bevor personenbezogene Daten zu Zwecken eines Nutzertracking auf Websites oder in mobilen Apps verarbeitet werden, ist es jedoch zwingend erforderlich, dass von den jeweiligen Betreibern eine diesbezügliche vorherige Einwilligung der Nutzerinnen und Nutzer eingeholt wird.

Um eine möglichst hohe Einwilligungsrate zu erreichen, wird daher zunehmend versucht, die Rate der Erteilung einer Einwilligung durch den Einsatz von fragwürdigen Mechanismen wie beispielsweise dem „Nudging“ oder der Verwendung von „Dark Patterns“, zu erhöhen.

Unter diesen Begriffen können grafische Gestaltungen von Benutzeroberflächen und sonstige Mechanismen gefasst werden, mit denen das Verhalten von Nutzerinnen und Nutzern in eine bestimmte Richtung gelenkt werden soll.

Als Nudging (to nudge = anstupsen) werden im Kontext der Cookie-Bannergestaltung grafisch umgesetzte Steuerungseffekte bezeichnet. Derartige „Anstupser“ dienen dazu, Nutzerinnen und Nutzern bei ihrer Entscheidung in Richtung einer von verschiedenen Auswahloptionen zu lenken.

Kommen „Dark Patterns“ zum Einsatz, sollen Nutzerinnen und Nutzer darüber hinaus zu Handlungen verleitet werden, die nicht ihren wahren Interessen entsprechen und diesen sogar zuwiderlaufen können. Erreicht werden derartige interessenswidrige Entscheidungen, indem etwa Benutzeroberflächen geschaffen werden, die sich über Nutzerpräferenzen hinwegsetzen. Dies kann u. a. mit unzureichenden Informationen zu eingesetzten Cookies, Falschbezeichnung von Cookie-Funktionen, bereits vorausgewählten Häkchen in den Einstellungen oder auch durch verwirrende Farbgestaltungen von Auswahlfeldern erfolgen.

Eine eindeutige Abgrenzung beider Methoden ist nicht möglich und auch nicht erforderlich, da beide Methoden in ihrer rechtlichen Betrachtung die Frage der Wirksamkeit eingeholter Einwilligungen betreffen.

In den dem HmbBfDI vorliegenden Beschwerden macht NOYB geltend, dass in diesem Sinne täuschende Cookie-Banner eingesetzt würden, welche nicht den datenschutzrechtlichen Anforderungen an „freiwillige für den bestimmten Einzelfall, in informierter Weise und unmissverständlich abgegebenen" Einwilligungen entsprächen.

Gegenstand der Beschwerden sind dabei der Einsatz von „Dark Patterns" in Form von fehlender bzw. versteckter Ablehnungs-Funktionen auf der ersten Ebene des Cookie-Banners. Als weitere Ausgestaltung der unzulässigen Steuerung durch „Dark Patterns" oder „Nudgings", enthalten die Beschwerden Angaben zu irreführenden Buttonfarben für die verschiedenen Optionen im Banner. Schaltflächen des Akzeptierens sind farblich und schriftbildlich deutlich hervorgehoben. Demgegenüber sind die Schaltflächen zum Ablehnen nur in kontrastarmen Farben gehalten und zudem vom Fließtext kaum unterscheidbar.

Die 422 NOYB-Beschwerden sind in der Folge einer unionsweiten Sichtung von Websites erfolgt. Dementsprechend fällt die Zuständigkeit zur Überprüfung der behaupteten DSGVO-Verstöße in die Zuständigkeit unterschiedlicher europäischer Aufsichtsbehörden (vgl. 29 TB, IV 6). Da die Beschwerden inhaltlich identische Beschwerdegegenstände aufweisen, wurde auch für diesen Themenkomplex durch den europäischen Datenschutzausschuss (EDSA) eine Task Force eingerichtet. Hierdurch soll ein bestmöglicher harmonisierter Ansatz zur Bearbeitung der Beschwerden durch die jeweils zuständigen Aufsichtsbehörden gewährleistet werden. Die Erarbeitung abgestimmter Prozesse dauert derzeit noch an.

3.8.2 NOYB-Beschwerden gegen Abo-Modelle

Weitere Beschwerden der Organisation NOYB betreffen Websites der sieben größten Nachrichtenmagazine. Zwei dieser Beschwerden fallen in die Zuständigkeit des HmbBfDI.

Inhaltlich befassen sich die Beschwerden mit sogenannten „Abo-Modellen" oder auch „Bezahlmodellen" auf Medienwebsites.

Diese Modelle stellen ein Geschäftsmodell dar, welches Nutzerinnen und Nutzer einer Website vor die Wahl stellt, entweder in das Setzen und Auslesen von Cookies oder vergleichbarer Technologien (uneingeschränkt) einzuwilligen oder im Rahmen eines Abonnements für die datenschutzfreundliche Variante des Anbieters zu bezahlen. Durch die allgemeine Zustimmung ermöglichen Nutzerinnen und Nutzer den Betreibern der Medienwebsites sowie deren Marketingpartnern ein umfassendes – oftmals websiteübergreifendes – Nachverfolgen ihres Nutzungsverhaltens (Tracking). Nutzerprofile, die durch ein solches Tracking erstellt werden, dienen wiederum als Grundlagen personalisierter Werbung.

NOYB wendet sich mit den eingereichten Beschwerden gegen das Geschäftsmodell der sogenannten Pur-Abos. Bei deren Einsatz fehle es bereits an einer echten Wahlfreiheit dahingehend, ob Nutzerinnen und Nutzer ihre personenbezogenen Daten preisgeben wollen oder nicht.

Möchten sie keine Einwilligung zum Tracking erteilen, entstünden erhebliche Aufwände. In zeitlicher Hinsicht müsste Aufwand betrieben werden, das Abo abzuschließen. In finanzieller Hinsicht erfolgten z.T. hohe Belastungen durch unverhältnismäßig hohe Preise. Dies führe dazu, dass Nutzerinnen und Nutzer, die z.B. nicht über ausreichend finanzielle Mittel verfügten, nur die Möglichkeit hätten, ihre Daten „zu verkaufen", wenn sie Zugang zu den Websites erlangen möchten.

Der Verstoß gegen die Anforderungen der DSGVO liege daher in dem Umstand, dass es an einer wirklich freiwillig erteilten Einwilligung zum Tracking fehle.

Da von den Beschwerden verschiedene Websitebetreiber betroffen sind, für welche unterschiedliche deutsche Aufsichtsbehörden zuständig sind, wurde im Rahmen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) der Unterarbeitskreis „Abo-Modelle" gegründet, an dem der HmbBfDI mitwirkt. Hierdurch soll eine einheitliche Beschwerdebearbeitung gewährleistet werden.

Der HmbBfDI teilt die in diesem Forum erarbeitete Annahme, dass „Abo-Modelle", bei welchen die Nutzerinnen und Nutzer die Wahl haben, entweder die Einwilligung zum Einsatz von Cookies und vergleichbaren Technologien zu akzeptieren oder die Websites mit dem kostenpflichtigen „Abo-Vertrag" zu nutzen (z.B. Abo-Vertrag), nicht von vornherein durch datenschutzrechtliche Vorgaben ausgeschlossen sind. Voraussetzung hierfür ist jedoch, dass für Nutzerinnen und Nutzer eine echte Wahlmöglichkeit besteht und dementsprechend deren Einwilligung zum Tracking tatsächlich freiwillig erteilt wird.

Hinsichtlich der Frage der freiwilligen Erteilung einer Einwilligung führt der EDSA aus:

„Der Verantwortliche könnte argumentieren, dass seine Organisation den betroffenen Personen eine echte Wahl bietet, wenn diese zwischen einer Dienstleistung, die die Einwilligung in die Verwendung personenbezogener Daten für zusätzliche Zwecke umfasst und einer ***vergleichbaren Dienstleistung, die von demselben Verantwortlichen angeboten wird und keine Einwilligung in die Verwendung von Daten für zusätzliche Zwecke beinhaltet****, wählen können. Solange die Möglichkeit besteht, dass der Verantwortliche den Vertrag erfüllt oder die Dienstleistungen erbringt, die Gegenstand des Vertrags sind, ohne dass in die fragliche andere oder zusätzliche Datennutzung eingewilligt werden muss, bedeutet dies, dass es nicht länger eine an Bedingungen geknüpf-*

te Dienstleistung ist. ***Die beiden Dienstleistungen müssen jedoch wirklich gleichwertig sein."*** *(Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Rn. 37, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf)*

Weitere Fragestellungen wie beispielsweise, ob eine Einwilligung derart pauschal erteilt werden kann, wie es derzeit über die Funktion des Zustimmungs-Buttons bei Pur-Angeboten erfolgt, befinden sich ebenso in der Abstimmung wie die Frage, welcher vergleichende Maßstab bei der Bewertung herangezogen werden kann, ob die Bezahlmöglichkeit eine geeignete Alternative zur Einwilligung darstellt.

3.9 Anpassung der Orientierungshilfe Werbung

Die überaus praxisrelevante Orientierungshilfe zur Direktwerbung wurde nach umfänglicher Überarbeitung der DSK als Beschlussentwurf vorgelegt.

Nachdem die Datenschutzkonferenz (DSK) am 7. November 2018 bereits eine „Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung unter der Geltung der Datenschutz-Grundverordnung (DSG-VO)" veröffentlicht hatte, ergeht nach Beschluss der DSK aktuell eine Anpassung der Orientierungshilfe, die dem Arbeitskreis der DSK „Werbung und Adresshandel" übertragen wurde.

Als Mitglied des Arbeitskreises „Werbung und Adresshandel" hat sich der HmbBfDI an der Überarbeitung und Aktualisierung dieser Orientierungshilfe umfangreich beteiligt. Die praktische Relevanz des Themas Direktwerbung in Bezug auf die Einhaltung der datenschutzrechtlichen Vorgaben und damit die Notwendigkeit einer Aktualisierung der Orientierungshilfe lässt sich anhand der hohen Anzahl der beim HmbBfDI im Bereich Werbung eingehenden Be-

schwerden nachvollziehen. Umso wichtiger war es daher, den auf dem Geschäftsfeld der Direktwerbung handelnden Akteuren eine aktualisierte fachliche Anwendungshilfe zur Verfügung zu stellen, um der stetig wachsenden Zahl an Beschwerden vorbeugen zu können.

Im Rahmen der Abstimmungen unter den Aufsichtsbehörden zur Anpassung der Orientierungshilfe zeigte sich die Komplexität des Themas, die sich insbesondere aus der Struktur des Geschäftsfeldes „Direktwerbung" ergibt, in dem an einer Werbemaßnahme oftmals verschiedene verantwortliche Stellen zusammenwirken. Ein werbendes Unternehmen verfügt häufig nicht über die für eine Werbemaßnahme notwendigen personenbezogenen Daten möglicher Adressaten und ist somit auf ein anderes Unternehmen angewiesen, das sich als Verkäufer oder Vermieter von Adressbeständen betätigt. Die Beurteilung der datenschutzrechtlichen Verantwortlichkeit der einzelnen Akteure hat damit ganz unterschiedliche tatsächliche Aspekte zu berücksichtigen, z.B. ob nur der Adresshändler tatsächlich Kenntnis von den personenbezogenen Daten der Werbeadressaten im Einzelnen hat und welche Rolle dem werbenden Unternehmen in Bezug auf die Auswahl von zu verwendenden personenbezogenen Daten zukommt. Die Zuordnung der handelnden Unternehmen zu den unterschiedlichen Verantwortlichkeiten der DSGVO stellt damit eine Aufgabe dar, die einer vielschichtigen und aufwendigen rechtlichen Prüfung bedarf, um die Rollen als eigenständig verantwortliche Stelle, als Auftragsverarbeiter gemäß Art. 28 DSGVO oder als gemeinsam verantwortliche Stellen im Sinne von Art. 26 DSGVO zuordnen zu können. Vor diesem Hintergrund wurde im Rahmen der Abstimmung unter den Aufsichtsbehörden zu der Anpassung der Orientierungshilfe beschlossen, das Thema Adresshandel einer gesonderten Beratung zu widmen, um eine Überfrachtung und Unübersichtlichkeit der Orientierungshilfe zur Direktwerbung zu vermeiden.

Damit entstand Raum, um sich im Rahmen der Orientierungshilfe mit weiteren komplexen Fragen, die sich beispielsweise aus den unterschiedlichen Wegen der Direktwerbung bzw. den unterschiedlichen

Werbemitteln bei Direktwerbung in Form von Briefwerbung, Werbung per E-Mail oder als Werbeanruf ergeben, befassen zu können. Da für die einzelnen Werbemittel ganz unterschiedliche Datenkategorien verarbeitet werden, ging es bei der Orientierungshilfe in Bezug auf die Zulässigkeit der Verarbeitung um eine übersichtliche und verständliche Darstellung der Zulässigkeitsvoraussetzungen für einzelne Verarbeitungsszenarien.

Im Ergebnis ist damit eine Orientierungshilfe entstanden, die die Voraussetzungen für eine datenschutzkonforme Verarbeitung personenbezogener Daten durch werbende Unternehmen übersichtlich darstellt, soweit diese ohne Hinzuziehung Dritter als eigenständig verantwortliche Stelle tätig werden. Zum Zeitpunkt des Redaktionsschlusses war die Anpassung der „Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung unter der Geltung der Datenschutz-Grundverordnung (DSG-VO)“ inhaltlich abgeschlossen, die förmliche Beschließung und Veröffentlichung durch die DSK stand allerdings noch aus.

3.10 Google Suchmaschine

Der HmbBfDI kann Google zur Auslistung von Suchergebnissen der Google Suchmaschine auffordern und diese anordnen. Dies erfolgt, wenn Betroffene die Google LLC zur Auslistung beeinträchtigender Suchergebnisse aufgefordert haben und der Suchmaschinenbetreiber die Auslistung zu Unrecht nicht vornimmt.

Legt eine betroffene Person der Google LLC hinreichend konkret und nachvollziehbar begründet dar, dass durch ein bestimmtes Suchergebnis ihre Persönlichkeitsrechte in nicht gerechtfertigter Weise beeinträchtigt werden, so ist die Google LLC zur Entfernung des Suchergebnisses bei Suchanfragen in Bezug auf die Person verpflichtet.

Die Google LLC erkennt in aller Regel einen vorliegenden Rechteverstoß an und listet das Suchergebnis aus. Im Berichtszeitraum hat der HmbBfDI allerdings in zwei Fällen gegenüber der Google LLC die Auslistung von Suchergebnissen angeordnet.

In einem Fall wurden bei Eingabe des Namens des Beschwerdeführers Entscheidungen eines EU-Gerichts zu einem Verfahren in den Suchmaschinenergebnissen angezeigt, das der Beschwerdeführer gegen seinen Dienstherrn geführt hatte. Das Europäische Gericht hatte die Entscheidungen aus 2012 und 2013 ohne eine Anonymisierung des Klägernamens veröffentlicht. Der HmbBfDI hatte in der Anzeige der Suchergebnisse zunächst keine Verletzung von Art. 17 Abs. 1 DSGVO durch die Google LLC gesehen, diese Entscheidung jedoch revidiert und die Auslistung bei einer namensbezogenen Suche gegenüber der Google LLC angeordnet. Die Gerichtsentscheidung enthielt die Information, dass und wegen welcher Umstände aus dem Dienstverhältnis der Beschwerdeführer seinen Arbeitgeber verklagt hatte, und wie das Gericht diese Umstände bei seiner Entscheidung berücksichtigt hat. Diese Informationen waren geeignet, den Beschwerdeführer etwa bei einer zukünftigen Arbeitssuche zu behindern. Dies insbesondere deshalb, weil sie bei bloßer Namenssuche des Klägers in den Suchergebnissen angezeigt wurden. Die Google LLC ist der Anordnung des HmbBfDI unmittelbar nachgekommen.

Es entspricht seit Jahrzehnten der deutschen Rechtsprechung, dass Gerichtsurteile nur anonymisiert veröffentlicht werden dürfen. Der Europäische Gerichtshof (EuGH) hat seine Praxis, Entscheidungen ohne Anonymisierung der Namen beteiligter Personen zu veröffentlichen, erst nach Inkrafttreten der DSGVO 2018 für Veröffentlichungen in Vorabentscheidungsverfahren geändert. Für in der Vergangenheit ohne Anonymisierung veröffentlichte und weiterhin im Internet abrufbare Gerichtsentscheidungen besteht daher die Möglichkeit, deren Auffindbarkeit über eine Namenssuche der betroffenen Prozesspartei in der Suchmaschine auszuschließen.

Eine weitere Anordnung gegen die Google LLC im Berichtszeitraum bezieht sich auf die Anzeige einer berufsbezogenen Meldung zu einem Beschwerdeführer in den Suchergebnissen zu dessen Namen. Die Meldung betrifft einen Jobwechsel des Beschwerdeführers im Jahr 2009, wobei auch ein von seinem Arbeitgeber herausgegebenes Foto von ihm veröffentlicht wurde. Die Anordnung ist nicht rechtskräftig, sondern wurde von der Google LLC gerichtlich angegriffen. Daher hat das Verwaltungsgericht (VG) Hamburg zu entscheiden, ob die Suchergebnisse auszulisten sind.

Nicht nur Anordnungen des HmbBfDI gegenüber der Google LLC, sondern auch Entscheidungen des HmbBfDI, eine Anordnung nicht zu erlassen, sind gerichtlich angreifbar (s. auch Kapitel IV 7). Das VG Hamburg urteilte im Juni 2021, dass für Beschwerdeführerinnen und Beschwerdeführer ein gerichtlich durchsetzbarer Anspruch auf ermessensfehlerfreie Entscheidung der Aufsichtsbehörde über ein Einschreiten besteht (Urteil v. 01.06.2021, 17 K 2977/19). Diese Auffassung wird mittlerweile von der überwiegenden Rechtsprechung vertreten. Die Frage liegt auch bereits dem EuGH zur Vorabentscheidung vor (s. VG Wiesbaden, Beschluss v. 31.08.2021, 6 K 226/21.WI). Im konkreten Fall entschied das Gericht aber, dass ein Recht auf Erlass einer Anordnung gegen die Google LLC nicht besteht. Der vormals als Privatagent tätige Kläger wendet sich u.a. gegen ein Suchergebnis, in dem die Kopie eines seiner Tarnpässe abgebildet ist. Das VG Hamburg konnte, ebenso wie der HmbBfDI, kein Geheimhaltungsinteresse an den Angaben zur früheren Tarnidentität des Klägers erkennen. Es sah vielmehr das öffentliche Interesse an der Person des Klägers als überwiegend an. Der Kläger hat Antrag auf Zulassung der Berufung gestellt.

Ein anderes Verfahren, in dem der Kläger die Anordnung der Löschung eines Suchergebnisses gegenüber der Google LLC begehrt, ist weiterhin vor dem VG Hamburg anhängig. Hier wird das Gericht möglicherweise darüber zu entscheiden haben, ob für den Auslistungsanspruch auch die in der Quelle weiterverlinkten Unterseiten (sog. Deep Links) zu berücksichtigen sind, auf denen Fotos des Klägers abgebildet sind.

Zwei weitere vor dem VG Hamburg anhängige Verfahren betreffen (z.T. ehemals) für die AfD tätige Kläger. Hier wird sich das VG mit der Frage auseinandersetzen, ob eine rein kommunale Betätigung für die AfD als Bürgervertreter aus einem Suchergebnis hervorgehen darf bzw. ob in einem Suchergebnis neben der Betätigung des Klägers für die AfD auch eine neunjährige Haftstrafe wegen in den 90-er Jahren begangener Delikte erwähnt werden darf.

3.11 Akkreditierung für Datenschutz-Zertifizierungen

Gemäß Art. 42 und 43 DSGVO müssen Unternehmen, die Zertifizierungen im Bereich Datenschutz-Grundverordnung vergeben, geprüft und zugelassen werden. In Deutschland erfolgt dies durch die Deutsche Akkreditierungsstelle gemeinsam mit der zuständigen Aufsichtsbehörde.

Im Tätigkeitsbericht Datenschutz 2020 hat der HmbBfDI berichtet, dass ein Unternehmen aus Hamburg ein Programm für die Zertifizierung von Datenverarbeitungsprozessen nach der DSGVO entwickelt und hierfür eine Akkreditierung bei der Deutschen Akkreditierungsstelle (DAkkS) beantragt hat (siehe 29. TB, IV 4). Die Akkreditierung ist notwendig, bevor auf Grundlage eines solchen Programms Datenverarbeitungen die Konformität zur DSGVO bescheinigt werden kann. Auch die ausstellende Organisation muss für eine Zertifizierung formell begutachtet und zugelassen sein. Die Feststellung der Tauglichkeit für eine Zertifizierung heißt Akkreditierung, abgeleitet von dem lateinischen Wort *„accredere“* – *„Glauben schenken“*.

Die DAkkS akkreditiert als beliehene Stelle des Bundes in Deutschland in einer Vielzahl von Bereichen und Tätigkeiten, z.B. bei technischen Prozessen, Laboren oder Dienstleistungen. Hierbei setzt sie

eigene oder externe Gutachter ein, die regelmäßig ihre Kompetenz gegenüber der DAkkS nachweisen müssen. Für den Bereich Datenschutz sieht die DSGVO eine enge Einbindung der Datenschutzaufsichtsbehörden vor.

Da Anträge auf Akkreditierung nicht nur den HmbBfDI, sondern eine Reihe von Aufsichtsbehörden betreffen, wurde auf Ebene der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine enge Zusammenarbeit vereinbart. Dabei stehen sowohl die Fragen der praktischen Zusammenarbeit mit der DAkkS als auch die Gewährleistung eines einheitlichen Prüfniveaus sowie der Austausch unter den akkreditierenden Behörden im Fokus.

In diesem Rahmen hat der HmbBfDI an dem Kriterienkatalog mitgewirkt, mit dem national ein einheitlicher Prüfmaßstab für Akkreditierungen und Programmprüfungen festgelegt wird. (Download unter https://datenschutzkonferenz-online.de/media/ah/DSK_Anwendungshinweis_Zertifizierungskriterien.pdf).

Auf dieser Grundlage hat der HmbBfDI die Antragsunterlagen des Programms des Hamburger Unternehmens geprüft und bewertet. Die notwendigen Anpassungen und erneuten Prüfungen waren bei Redaktionsschluss weit fortgeschritten, aber noch nicht abgeschlossen. Der fachlichen Bewertung durch den HmbBfDI folgt eine Befassung auf europäischer Ebene, bevor schließlich formal eine Akkreditierung durch die DAkkS erteilt werden kann.

Für alle Beteiligten ist ein DSGVO-Akkreditierungsverfahren ein aufwändiger Prozess. Dies liegt zum einen daran, dass das Verfahren neu ist und eine Menge von grundlegender Vorarbeit erfordert. Hinzukommt, dass es sich um ein wirkmächtiges Instrument handelt, mit dem auf dem Markt erhebliche Effekte erzielt werden können. Ein akkreditiertes Programm kann von dem beantragenden Unternehmen selbst oder auch von Dritten genutzt werden, um damit entsprechende Datenverarbeitungsprozesse auf DSGVO-Konformität zu prüfen und zu zertifizieren. Das vom europäischen Verordnungs-

geber gewünschte Moment der Selbstregulierung kann sich nur dann entfalten, wenn dies auf hohem fachlichem Niveau und ohne wesentliche Konflikte mit den Aufsichtsbehörden gelingt.

BUSSGELDER, ANORDNUNGEN, GERICHTSVERFAHREN 4.

4. Bußgelder, Anordnungen, Gerichtsverfahren

4.1 Bußgeld Hamburger Energieversorgungsunternehmen

Der HmbBfDI hat gegen einen Hamburger Energieversorger ein Bußgeld in Höhe von 901.388,84 Euro verhängt. Der Bußgeldbescheid ist rechtskräftig.

Der Energieversorger hatte zwischen August 2018 und etwa Dezember 2019 Vertragsanfragen von Neukunden routinemäßig daraufhin überprüft, ob diese ein sogenanntes „wechselauffälliges Verhalten" zeigten. Als wechselauffälliges Verhalten galt, dass für denselben Zählpunkt ein und derselbe Kunde zuvor bereits zwei Verträge abgeschlossen oder Bonuszahlungen von mehr als 500 Euro erhalten hatte. Um ein solches wechselauffälliges Verhalten festzustellen, wurden Stamm-, Vertrags- und Abrechnungsdaten sowie Zahlungsinformationen daraufhin überprüft, ob der Kunde bereits Vertragspartner war. Bei Feststellung eines solchen wechselauffälligen Verhaltens, kamen Vertragsabschlüsse nicht zustande.

Innerhalb des Antragsformulars zur Strombelieferung wurden Kunden lediglich darüber informiert, dass ein etwaiger Bonus nur gewährt werden konnte, wenn der Kunde nicht unmittelbar vor Lieferbeginn an der betreffenden Lieferstelle mit Strom beliefert wurde. Auch an anderer Stelle, wie insbesondere der Datenschutzerklärung, erfolgten keine konkreten Hinweise, aus denen Kunden auf die Prüfung von Vertragsanfragen nach dem eingangs beschriebenen Verfahren schließen konnten.

Ein solcher Abgleich erfolgte in rund 500.000 Fällen, ohne dass die betroffenen Personen hinreichend informiert wurden und damit unter Verstoß gegen die Transparenzpflichten nach Art. 5 Abs. 1 lit. a), 12 und 13 DSGVO. Danach müssen personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies setzt voraus, dass die verantwortliche Stelle bei

Erhebung der personenbezogenen Daten die in Art. 12, 13 DSGVO genannten Informationen mitteilt. Bestandteil der Informationspflichten ist auch die Nennung der Zwecke der Verarbeitung (Art. 13 Abs. 1 lit. c) DSGVO). Danach hätten die konkret durchgeführten Datenabgleiche offengelegt werden müssen.

Die Einleitung eines Bußgeldverfahrens war aufgrund der Vielzahl der Fälle und der systematischen Verstöße angezeigt. Bei der konkreten Zumessung des Bußgeldes wurde berücksichtigt, dass der Verstoß in qualitativer Hinsicht wenig gravierend, in quantitativer Hinsicht hingegen als Verstoß mittlerer Schwere einzuordnen war. Darüber hinaus handelte es sich um einen Erstverstoß des Unternehmens und es hat eine umfangreiche Zusammenarbeit mit der Aufsichtsbehörde stattgefunden.

4.2 Bußgeld wegen mangelhafter TOM im Gesundheitswesen

Bei der Verarbeitung von Gesundheitsdaten von Patientinnen und Patienten müssen Unternehmen geeignete technische und organisatorische Maßnahmen (TOM) ergreifen, um diese Daten angemessen zu schützen. Bei einer unzureichenden Umsetzung von TOM drohen empfindliche Bußgelder.

Im Berichtszeitraum hat der HmbBfDI ein Bußgeldverfahren gegen ein in Hamburg ansässiges Unternehmen durchgeführt, welches im Gesundheitswesen tätig ist.

Das Unternehmen hatte es zum einen unterlassen, geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um beim Versand von Arztbriefen (Transferdokument für die Kommunikation zwischen behandelnden Ärztinnen und Ärzten) durch Beschäftigte des Unternehmens ein dem Risiko angemessenes Schutzniveau zu gewährleisten. In der Folge wurden mehrfach Arztbriefe an eine

Person versandt, die zwar einem Heilberuf nachging, aber nicht die weiterbehandelnde Ärztin dieser Patientinnen und Patienten war. Die Arztbriefe waren vielmehr für eine gleichnamige Allgemeinärztin bestimmt. Erschwerend kam hinzu, dass das Unternehmen in der Vergangenheit von der unberechtigten Empfängerin mehrfach auf den Fehlversand hingewiesen wurde. Das Unternehmen hatte die Adressatin nach deren Hinweisen mit einem Sperrvermerk in dem verwendeten Datenverarbeitungssystem versehen. Es hatte es dabei aber unterlassen, durch organisatorische und technische Maßnahmen sicherzustellen, dass der Sperrvermerk auch bei Software-Updates übernommen wird. So wurde nach einem Update der Sperrvermerk nicht übernommen und die Empfängerin bekam erneut Arztbriefe über Personen, die nicht ihre Patientinnen und Patienten waren. Der Fehlversand beruhte somit auf dem fehlenden Sperrvermerk und einer nicht mit der notwendigen Sorgfalt durchgeführten Auswahl der Adressatin durch die Beschäftigten des Unternehmens. Dies stellt einen Verstoß gegen die Pflicht des Art. 32 Abs. 1 DSGVO dar.

Auch wenn die fehlerhaft adressierte Empfängerin selbst Berufsgeheimnisträgerin war und das Risiko einer schädigenden Verwendung der übermittelten Daten deswegen als eher gering einzustufen ist, ist das Risiko für die Rechte und Freiheiten bestimmter natürlicher Personen bei der Verarbeitung personenbezogener Daten in Arztbriefen derart erheblich, dass die Daten wirksam geschützt werden müssen. Es stellt ein zu erwartendes menschliches Fehlverhalten dar, dass Beschäftigte im hektischen Alltag bei der Auswahl von Adressaten für Arztbriefe nicht in jedem Fall die notwendige Sorgfalt walten lassen. Deswegen sind auch geeignete technische Schutzmaßnahmen wie die Einrichtung eines Sperrvermerks zu treffen und eine Übernahme dieser technischen Schutzmaßnahmen bei Aktualisierungen von Datenverarbeitungsanlagen sicherzustellen.

Zum anderen hatte das Unternehmen es an einem Standort für einen Zeitraum von über einem Jahr unterlassen, durch die Implementierung und Verwendung einer Protokollierungsfunktion für lesende Zugriffe auf Daten von Patientinnen und Patienten im genutzten

Informationssystem eine angemessene Sicherheit der Verarbeitung von Daten der Patientinnen und Patienten zu gewährleisten und hier insbesondere die Vertraulichkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen und nachzuweisen. In der Folge war es nicht möglich nachzuvollziehen, welche Beschäftigten lesend auf Daten von Patientinnen und Patienten zugegriffen haben.

Zum Schutz vor einer unbefugten oder unrechtmäßigen Verarbeitung bedarf es bei sensiblen Daten wie Gesundheitsdaten neben Vorkehrungen wie Zugangsbeschränkungen und Datenverschlüsselung auch geeigneter Maßnahmen mittels derer nachträglich überprüft und festgestellt werden kann, ob und wann personenbezogene Daten verarbeitet wurden. Eine Protokollierung von lesenden Zugriffen ist insbesondere erforderlich, um die in Art. 32 Abs. 1 lit. b) DSGVO genannte Integrität der im Informationssystem gespeicherten Daten zu gewährleisten. Die Gewährleistung der Vorgaben des Art. 32 DSGVO hat der Verantwortliche bei Bedarf gem. Art. 24 Abs. 1 DSGVO nachzuweisen. Ein Nachweis durch das Unternehmen darüber, durch wen zu welchem Zeitpunkt auf bestimmte Daten von Patientinnen und Patienten zugegriffen wurde, war nicht möglich, obwohl in einem Fall konkrete Hinweise auf einen unberechtigten, lesenden Zugriff vorlagen. Das Unternehmen verstieß somit gegen 32 Abs. 1 DSGVO.

Der HmbBfDI hat wegen dieser Verstöße ein Bußgeld im niedrigen sechsstelligen Bereich verhängt. Bei der Zumessung des Bußgelds wurde mildernd berücksichtigt, dass es sich um einen Erstverstoß des Unternehmens handelte und eine umfangreiche Zusammenarbeit mit der Aufsichtsbehörde stattgefunden hat, um den Verstößen abzuhelfen. Schärfend wurde der Umstand berücksichtigt, dass es sich bei den verarbeiteten Daten um Gesundheitsdaten handelte. Es wurden somit besondere Arten personenbezogener Daten verarbeitet, die ihrem Wesen nach sensibel sind und nach den Vorschriften der DSGVO einem besonderen Schutz unterliegen.

Das Unternehmen hat die Geldbuße akzeptiert und auf einen Einspruch verzichtet.

4.3 Zwei Bußgeldverfahren gegen Energieversorger

Der HmbBfDI hat im Berichtszeitraum zwei Bußgeldbescheide, jeweils in Höhe von 12.500,00 Euro, gegen zwei in Hamburg ansässige Energieversorger erlassen. Die Bescheide sind rechtskräftig.

Hintergrund der Ordnungswidrigkeitenverfahren war die Ausgliederung der Heizenergiesparte eines großen deutschen Energieversorgers und die anschließende Veräußerung der ausgegliederten Sparte. Kundinnen und Kunden, die von dem Übergang betroffen waren, wurden über die Vertragsübergänge ihrer Strombelieferungsverträge informiert und ihnen wurde ein Widerspruchsrecht eingeräumt. Im Falle eines erklärten Widerspruchs sollten keine personenbezogenen Daten der Kundinnen und Kunden an das neue Unternehmen übermittelt werden.

Trotz ordnungsgemäß erklärtem Widerspruch von Kundinnen und Kunden kam es in einem relevanten Ausmaß zur Migration von Strombelieferungsverträgen auf den Erwerber der Heizenergiesparte. Dadurch waren Kundendaten auch in den Fällen an das neue Unternehmen übermittelt, in denen die Betroffenen ordnungsgemäß einen entsprechenden Widerspruch erklärt hatten. Ursächlich waren Fehler bei der Verarbeitung der Widersprüche durch den eingesetzten Auftragsverarbeiter des veräußernden Unternehmens. Aufgrund der Vielzahl der Verstöße war es angezeigt, Bußgeldverfahren gegen die Unternehmen einzuleiten.

Bei der Bemessung der Höhe der jeweiligen Bußgelder wurde insbesondere berücksichtigt, dass es sich um Erstverstöße handelte und

eine umfangreiche Zusammenarbeit mit der Aufsichtsbehörde stattgefunden hat.

4.4 Bußgeld wegen Anfertigung von Videos fremder Kinder und junger Frauen in Einkaufzentren

Der HmbBfDI hat wegen der rechtswidrigen Anfertigung von Videos fremder Personen das höchste Bußgeld gegen eine Privatperson seit Geltung der DSGVO verhängt. Ein Ende der Straßenfotografie droht dennoch nicht!

In seinem letzten Tätigkeitsbericht hat der HmbBfDI bereits über mehrere Fälle berichtet, in denen Privatpersonen mit dem Mobiltelefon oder einer Digitalkamera auf der Straße Aufnahmen von Fremden angefertigt haben, zu denen sie keinerlei Beziehung hatten (vgl. 29. TB 2019, Kapitel V 10). Auch in diesem Berichtszeitraum musste der HmbBfDI ein entsprechendes Bußgeldverfahren durchführen.

Der HmbBfDI erhielt den Vorgang von der Staatsanwaltschaft Hamburg zur Prüfung einer etwaigen von dem Ersteller der Videos begangenen Ordnungswidrigkeit nach der DSGVO. An einem Tag im August 2020 fiel einem Passanten in einem Einkaufszentrum ein Mann auf, der in verdeckter Weise junge, leicht bekleidete Mädchen filmte. Der Passant informierte einen Mitarbeiter des Sicherheitsdienstes des Einkaufszentrums über seine Beobachtung. Der Mitarbeiter des Sicherheitsdienstes verständigte daraufhin die Polizei. Bei einer Durchsuchung des Rucksacks fanden die Polizisten eine Digitalkamera und acht Speicherkarten. Diese wurden von der Polizei vor Ort sichergestellt.

Auf den sichergestellten Speicherkarten befanden sich insgesamt 156 Videodateien, die in den Jahren 2013 bis 2020 erstellt wurden. Eine Auswertung des Videomaterials ergab, dass Personen,

die sich in Hamburg auf öffentlichen Straßen oder Wegen sowie in Einkaufzentren aufgehalten haben, gezielt und heimlich gefilmt und die Videodateien auf mitgeführten SD-Karten gespeichert wurden. Auf den Aufnahmen waren vorwiegend junge, weibliche Personen in knapper Bekleidung zu sehen. Einige der aufgenommenen weiblichen Personen waren augenscheinlich jünger als 14 Jahre. Der Fokus der Aufnahmen lag in vielen Fällen auf dem Gesäßbereich/Unterleib der Gefilmten. Der Ersteller näherte sich den gefilmten Personen in mehreren Fällen bis auf wenige Zentimeter und verfolgte sie mit der Kamera bis zu 38 Minuten lang durch die Hamburger Innenstadt. Er überholte die Gefilmten zielgerichtet, um sie dann beim Vorbeigehen erneut filmen zu können. Ferner postierte er sich auch vor Geschäftsausgängen, um die Personen beim Verlassen des Geschäfts abermals filmen zu können.

Der Ersteller der Videos hat die personenbezogenen Daten der von ihm gefilmten jungen Frauen und Mädchen verarbeitet, obwohl ihm dies weder durch eine wirksame Einwilligung der Gefilmten noch durch eine Rechtsvorschrift erlaubt war. Die sog. Haushaltsausnahme nach Art. 2 Abs. 2 lit c) DSGVO zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten greift hier nicht. Der HmbBfDI hat wegen eines Verstoßes gegen Art. 83 Abs. 5 lit. a) i.V.m. Art. 5 Abs. 1 lit. a), 6 Abs. 1 DSGVO in 13 Fällen eine Geldbuße in Höhe von 5.000 EUR verhängt. Bei der Zumessung der Geldbuße wurde schärfend berücksichtigt, dass die jungen Frauen und Mädchen in diesen Fällen über einen langen Zeitraum verfolgt und an verschiedenen Orten heimlich gefilmt wurden. Ferner nahm der Ersteller mindestens billigend in Kauf, dass es sich bei den aufgenommenen Personen auch um Kinder handelte. Auch dies wurde schärfend berücksichtigt. Kinder sind von der Rechtsordnung besonders geschützt. Gerade sie müssen auf entsprechenden Schutz vertrauen können, da sie häufig noch nicht in der Lage sind, zwischen Privatsphäre und Sozialsphäre adäquat zu unterscheiden und sich daher nicht durchgehend an die jeweilige Sphäre angepasst verhalten. Der Ersteller der Videos hat die Geldbuße akzeptiert und keinen Einspruch eingelegt.

Die Entscheidung des HmbBfDI, derartige Fälle mit einem Bußgeld zu ahnden, bedeutet nicht das Ende der Straßenfotografie. Entsprechende Sorgen von Fotografinnen und Fotografen, die nach der Veröffentlichung des Tätigkeitsberichts 2020 in sozialen Medien geäußert wurden, sind unbegründet. Die vom HmbBfDI verfolgten Fälle haben keinen Bezug zur Straßenfotografie. Es handelt sich um Aufnahmen und Videos von leichtbekleideten Frauen und Kindern, die heimlich und allem Anschein nach ausschließlich aus sexuellen Motiven angefertigt wurden. Den Aufnahmen kommt kein künstlerischer Wert zu und sie dürften wohl nach keinem Verständnis unter den Sammelbegriff der Straßenfotografie fallen. Die rechtliche Bewertung des HmbBfDI zum Bereich Straßenfotografie ist in einem Vermerk festgehalten, der auf der Homepage des HmbBfDI veröffentlicht ist: https://datenschutz-hamburg.de/assets/pdf/Vermerk_Fotografie_DSGVO.pdf. Danach ist die Datenerhebung zum Zweck der Straßenfotografie in den meisten Fällen über Art. 6 Abs. 1 lit. f) DSGVO erlaubt.

4.5 Bußgeld wegen der Offenlegung der Krankheit eines Kundenberaters

Weil Gesundheitsdaten eines Mitarbeiters gegenüber dem Kundenstamm datenschutzwidrig offenbart wurden, hat der HmbBfDI ein Bußgeld in Höhe von EURO 10.100 gegen ein Autohandelsunternehmen aus Hamburg verhängt. Die Entscheidung ist rechtskräftig.

Der HmbBfDI hat ein Bußgeld in Höhe von 10.110 EURO verhängt, weil eine überregional tätige Autohandelsgruppe den Kundenstamm seiner Niederlassung außerhalb Hamburgs darüber informiert hat, dass Gründe für die dortige Umstrukturierung der krankheitsbedingte Ausfall des bisherigen Verkaufsleiters sei. Der genaue Zeitpunkt des Beginns der Arbeitsunfähigkeit sowie die Mitteilung,

dass die Situation noch auf unbestimmte Zeit anhalte, wurden an mehr als 3000 Stammkundinnen und -kunden an diesem Standort übermittelt. Diese Mitteilung führte zu einem besonders intensiven Eingriff in die Betroffenenrechte und hat das zum Zeitpunkt der Mitteilung bestehende Arbeitsverhältnis erheblich belastet. Da für diese Übermittlung von personenbezogenen Gesundheitsdaten keine Rechtsgrundlage bestand, hätte sie unterbleiben müssen. Das Unternehmen hat Vorkehrungen getroffen, dass sich ein solcher Fall nicht wiederholt.

Wie kommuniziert man also Umstrukturierungen im Unternehmen datenschutzkonform?
Ein Personalwechsel im Unternehmen will kommuniziert werden. Mitarbeiter, aber auch Geschäftspartner und Kunden wollen über eine Neubesetzung informiert werden, wenn zwischen Ihnen Kontakt besteht. Eine offene Kommunikation soll Klarheit verschaffen und Gerüchten vorbeugen. Doch wieviel Klarheit ist erforderlich und datenschutzrechtlich erlaubt? Gehört zu einer neutralen und sachlichen Kommunikation auch die Nennung von Gründen krankheitsbedingter Abwesenheit?

Wenn es darum geht, neue Mitarbeiter mit intensivem Kundenkontakt anzukündigen, dürfen bisheriger und neuer Ansprechpartner gegenüber Kundinnen und Kunden in der Regel benannt werden. Bei vorübergehender Vakanz sollten die Gründe der Abwesenheit grundsätzlich nicht nach außen kommuniziert werden, noch viel weniger, wenn dabei besonders sensible Daten betroffen sind. Sofern keine Einwilligung des bisherigen Mitarbeiters vorliegt besteht für die Übermittlung des Gesundheitszustandes, der den Kern der Privatsphäre betrifft, wegen des verschärften Erforderlichkeitsmaßstabes im Beschäftigtendatenschutz – mit Ausnahme von gesetzlich geregelten Ausnahmefällen – keine Rechtfertigung. Kundinnen und Kunden können auch ohne Mitteilung krankheitsbedingter Abwesenheit ausreichend informiert werden Für eine Bindung zum neuen Ansprechpartner im Unternehmen ist die Nennung dieser Gründe ebenfalls nicht erforderlich. Beim Datenschutz im Kundenservice

sind durch entsprechende Vorkehrungen auch personenbezogene Daten der Mitarbeiter zu beachten.

4.6 Warnung wegen des beabsichtigten Einsatzes der Videokonferenzsoftware Zoom

Im Jahr 2021 sprach der HmbBfDI gegenüber der Senatskanzlei der Freien und Hansestadt Hamburg eine förmliche Warnung gem. Art. 58 Abs. 2 lit. a DSGVO aus. Diese bezog sich auf den geplanten Einsatz der Videokonferenzsoftware Zoom. Der HmbBfDI kam in dieser zu dem Ergebnis, dass ein datenschutzrechtskonformer Einsatz der Software aufgrund der „Schrems II"-Entscheidung des Europäischen Gerichtshofs (EuGH) derzeit nicht möglich ist. Die Warnung wird von der Senatskanzlei vor dem Hamburgischen Verwaltungsgericht angegriffen.

Die Entscheidung des EuGH in der Sache Facebook Ireland und Schrems (Urt. v. 16. Juli 2020, C-311/18), besser bekannt als „Schrems II", hatte und hat gewichtige Auswirkungen auf datenschutzrechtliche Beurteilungen in der gesamten Europäischen Union. So wie alle Aufsichtsbehörden, hat auch der HmbBfDI die Ausführungen des EuGH bei datenschutzrechtlichen Prüfungen im Raum der Hansestadt Hamburg zu beachten. Der HmbBfDI führt parallel zahlreiche Prüfungen durch, welche diese Materie betreffen (s. Kapitel V 2.1 und V 2.2).

Drittlandtransfer personenbezogener Daten beim Einsatz von Zoom

Beim Einsatz von Zoom fallen zahlreiche personenbezogene Daten an. Bei Einrichtung eines Zoom-Kontos können hierunter ein natürlicher Name, ein Profilfoto, eine E-Mailadresse, Telefonnummern oder Zahlungsdaten fallen. Einige dieser Informationen sind zwingend notwendig anzugeben, wenn bspw. geplant ist, an einer Ende-zu-Ende-verschlüsselten Videokonferenz teilzunehmen. Dabei war bis zum

Abschluss der Ermittlungen des HmbBfDI nicht erkennbar, weshalb besondere Anforderungen an die Profilinformationen für besser verschlüsselte Konferenzen bestehen. Die Verwaltung und damit die zugehörige Datenverarbeitung der eingerichteten Nutzerkonten übernimmt beim Einsatz von Zoom stets die in den USA ansässige Zoom Video Communications, Inc.

Beim konkreten Einsatz fallen zahlreiche Konferenzinhalte als personenbezogene Daten an: Audio- und Videoübertragungen, Chatverläufe und zugehörige Meeting-Inhalte. Der Einsatz der – nur mit Einschränkungen zur Verfügung stehenden – Ende-zu-Ende-Verschlüsselung kann hier dafür sorgen, dass diese Daten nicht gegenüber der Zoom Video Communications, Inc. offengelegt werden.

Darüber hinaus werden aber Metadaten angelegt, d.h. Kommunikationen werden protokolliert und das Nutzungsverhalten bei Nutzung der Software sowie Informationen über die eingesetzte Hardware werden gesammelt. Diese Daten reichern zunehmend das Nutzer-Konto mit weiteren Informationen an und stehen der Zoom Video Communications, Inc. zur Verfügung.

Da also nicht verhindert werden kann, dass beim Einsatz von Zoom Daten an die Zoom Video Communications, Inc. fließen, müssen besondere Vorkehrungen zum Schutz der Daten getroffen werden. Diese Notwendigkeit ist eine direkte Folge der „Schrems II"-Entscheidung des EuGH. Nach Ansicht des HmbBfDI ist die Ende-zu-Ende-Verschlüsselungsfunktion von Zoom alleine nicht geeignet, den erforderlichen Schutz zu gewährleisten. Selbst wenn diese Funktion optimal genutzt würde, d.h. bei ausnahmslos jedem Meeting zum Einsatz käme, blieben die Profildaten übrig, die nicht hiervon erfasst werden können.

Für die Administration beim Einsatz steht daneben die Möglichkeit zur Verfügung, als Verarbeitungsstandorte ausschließlich Rechenzentren innerhalb der Europäischen Union zu bestimmen. Eine solche Vereinbarung soll verhindern, dass die personenbezogenen Da-

ten technisch auf Computersysteme in den USA übertragen werden. Die Verantwortung für diese Systeme verbleibt jedoch bei der in den USA ansässigen Firma. Aus diesem Grund ist nach Einschätzung des HmbBfDI auch damit kein wirksamer Schutz erreicht. Der HmbBfDI folgt hierbei einer verwaltungsgerichtlichen Entscheidung des französischen Conseil d'État. Da es sich bei der DSGVO um eine europäische Verordnung handelt, die eine Vereinheitlichung der Rechtsanwendung in der gesamten Europäischen Union zum Ziel hat, sind Entscheidungen aus anderen Mitgliedsstaaten ebenfalls zu beachten, jedenfalls solange keine eindeutige Linie der deutschen Rechtsprechung vorliegt, oder sogar eine weitere EuGH-Entscheidung.

Der französische Conseil d'État entschied, dass aufgrund des US-amerikanischen Gesetzes, des „Cloud Act", § 2713 Chapter 121, eine Standortvereinbarung nicht zur Erreichung des notwendigen Schutzes ausreicht. Der „Cloud Act" ermöglicht es US-amerikanischen Nachrichtendiensten, Daten von US-Unternehmen heraus zu verlangen, auch dann wenn diese ausschließlich in Cloud-Systemen außerhalb der USA gespeichert sind. Die Trennung von Unternehmenssitz und Standort der Daten ist demnach als unzureichende Schutzmaßnahme anzusehen. Der HmbBfDI kam daher zu dem Ergebnis, dass der Einsatz von Zoom zu einem Drittlandtransfer personenbezogener Daten führt, ohne dass diese Daten ausreichend geschützt wären.

Eine Warnung gegenüber der Senatskanzlei

Der HmbBfDI ist betreffend der öffentlichen Stellen in Hamburg zum einen Aufsichtsbehörde, zum anderen jedoch auch besonders zur Beratung verpflichtet. Dem HmbBfDI ist es ein wichtiges Anliegen, diese Beratungstätigkeit gegenüber öffentlichen Stellen gewissenhaft zu erfüllen. Nachdem er von Plänen zum Einsatz von Zoom erfahren hatte, war er daher sehr darum bemüht, frühzeitig die grundsätzlichen Bedenken gegen den Einsatz vorzubringen und darauf hinzuweisen, dass der Markt bereits zahlreiche Alternativen bietet, die datenschutzkonform eingesetzt werden können. Leider konnte sich der HmbBfDI mit diesen Bedenken nicht durchsetzen, so dass

schlussendlich im Wege eines förmlichen Verfahrens der Erlass einer Warnung gem. Art. 58 Abs. 2 lit. a DSGVO folgte. Mit dieser kann eine Aufsichtsbehörde eine verantwortliche Stelle davor warnen, dass eine geplante Datenverarbeitung voraussichtlich gegen die DSGVO verstoßen wird. Diese Voraussetzungen sah der HmbBfDI durch die geplante Einführung der Software als Ergänzung zu vorhandenen Videokonferenzlösungen als gegeben an.

Der HmbBfDI bedauert, dass dieser Schritt – und damit der Übergang von der Beratung hin zur Aufsicht – schlussendlich notwendig war. Jedoch muss letztlich vor allem der Schutz personenbezogener Daten vor drohenden Rechtsverletzungen gewährleistet werden.

Die Senatskanzlei lässt die Warnung des HmbBfDI nunmehr gerichtlich vor dem Hamburgischen Verwaltungsgericht überprüfen. Der HmbBfDI sieht hierin die Chance, wichtige Fragen im Zusammenhang mit dem Drittlandtransfer personenbezogener Daten bei dem Einsatz von Videokonferenzsystemen von einem deutschen Gericht zu klären. Insofern handelt es sich um ein Grundsatzverfahren von nationaler und europäischer Bedeutung.

4.7 Überblick Gerichtsverfahren

Auch im Berichtszeitraum war der HmbBfDI in gerichtliche Verfahren involviert. Dabei wurden Verfahren fortgeführt, die bereits vor dem Berichtszeitraum anhängig waren.

So wurde etwa das Verfahren um die beim G20-Gipfel in Hamburg 2017 von der Polizei eingesetzte Gesichtserkennungssoftware „Videmo“ fortgesetzt (s. hierzu die Darstellung im TB Datenschutz 2020, Kapitel V 4). Zur Erinnerung: Mangels einer Rechtsgrundlage hatte der HmbBfDI die Löschung der biometrischen Datenbank angeordnet. Die hiergegen gerichtete Klage beim Verwaltungsgericht

Hamburg war zunächst erfolgreich. Hiergegen hat der HmbBfDI einen Antrag auf Zulassung der Berufung gestellt. Dieser liegt zur Entscheidung beim Oberverwaltungsgericht Hamburg. Der Ausgang der Entscheidung ist insbesondere deswegen ungewiss, da die Polizei Hamburg zwischenzeitlich die in Streit stehende Datenbank gelöscht hat und damit prinzipiell der ursprünglichen Anordnung des HmbBfDI nachgekommen ist. Gleichwohl besteht aus Sicht des HmbBfDI ein dringendes Erfordernis die offenen Rechtsfragen einer obergerichtlichen Klärung zuzuführen, um Rechtssicherheit für zukünftige Einsätze vergleichbarer Datenverarbeitungssysteme für die Sicherheitsorgane der FHH zu schaffen und – im Idealfall – den Problemkreis biometrischer Gesichtserkennung der Legislative zu überantworten.

Darüber hinaus sah sich der HmbBfDI Klagen von Bürgerinnen und Bürgern auf ein Einschreiten gegenüber verantwortlichen Stellen ausgesetzt. Ein Schwerpunkt dabei sind Gerichtsverfahren, die einen Delisting-Anspruch gegen die Google LLC. nach Art. 17 DSGVO zum Gegenstand haben, die also eine Auslistung von Suchergebnissen innerhalb der Google-Suche verfolgen.

Hier hat das Verwaltungsgericht Hamburg in einem allerdings noch nicht rechtskräftigen Urteil die Rechte der Bürgerinnen und Bürger gestärkt. Es hat festgestellt, dass grundsätzlich ein Anspruch darauf besteht, dass der HmbBfDI Beschwerden dahingehend überprüft, ob die Google LLC. durch die Indexierung von Suchergebnissen, bzw. die darin liegende Verarbeitung der personenbezogenen Daten betroffener Personen gegen die DSGVO verstößt. Für den Fall, dass der HmbBfDI einen solchen Verstoß feststellt, besteht ein Anspruch der betroffenen Person auf ermessensfehlerfreie Entscheidung in Bezug auf den Erlass von Abhilfemaßnahmen nach Art. 58 Abs. 2 DSGVO, insbesondere ein Verbot der Verarbeitung.

Aber auch in anderen Konstellationen haben Bürgerinnen und Bürger ihre Rechte aus Art. 78 DSGVO wahrgenommen und Entscheidungen des HmbBfDI gerichtlich überprüfen lassen. Betroffene Perso-

nen nutzen insofern mehr und mehr die wirksamen Instrumentarien, die die DSGVO zur Verfügung stellt, um ihre Persönlichkeitsrechte selbstbewusst zu schützen. So richtete sich eine Klage gegen die Entscheidung des HmbBfDI, in einem im Beschäftigtendatenschutz angesiedelten Fall nicht tätig zu werden: Eine ehemalige Mitarbeiterin wandte sich an den HmbBfDI, da sie sich Überwachungsmaßnahmen durch ihren Arbeitgeber ausgesetzt sah. Tatsächlich hatte die Mitarbeiterin den ihr zur Verfügung gestellten Firmenwagen zweckwidrig für private Zwecke verwendet. Überdies wies die Stundenabrechnung erhebliche Unregelmäßigkeiten auf. Der Arbeitgeber fertigte von der Privatnutzung des Firmenwagens Videoaufzeichnungen an, welche der Arbeitgeber im Rahmen eines arbeitsrechtlichen Vergleichs zusicherte zu löschen. Das Verwaltungsgericht Hamburg bestätigte die Entscheidung des HmbBfDI, nicht tätig zu werden, da die Überwachungsmaßnahmen gerechtfertigt waren.

In einem anderen Fall begehrte eine Klägerin den Erlass einer Anordnung gegenüber einem E-Mail-Provider, mit der diesem zur Löschung eines E-Mail-Kontos verpflichtet werden sollte. Der HmbBfDI hatte zuvor ein Tätigwerden abgelehnt, da die Klägerin ihre Kontoinhaberschaft nicht hinreichend dargelegt hatte. Das Verwaltungsgericht Hamburg wies die Klage ab und urteilte, dass keine Pflicht der Aufsichtsbehörde bestehe, dass diese bei unvollständigen und unklaren Angaben verpflichtet wäre, weitreichende eigene tatsächliche Ermittlungen, insbesondere in der ureigenen Sphäre beschwerter Personen, anzustellen, um den Sachverhalt aufzuklären. Werden unvollständige oder unklare Angaben auch auf Nachfrage der Aufsichtsbehörde nicht vervollständigt oder klargestellt, obwohl dies möglich und zumutbar ist, ist es nicht zu beanstanden, wenn die Aufsichtsbehörde nicht selbstständig eigene Ermittlungen „ins Blaue hinein“ anstellt, sondern den Sachverhalt auf der Grundlage der vorgelegten Informationen bewertet und dabei unklare oder unvollständige Angaben zu Lasten beschwerter Personen wertet.

Demgegenüber hat der HmbBfDI nur einen Einspruch gegen ein erlassenes Bußgeld verhandelt. Gegenstand war hierbei ein Bußgeld

wegen rechtsgrundloser E-Mail-Werbung in 10 Fällen. Im Laufe der Verhandlung wurde der Einspruch auf die Bußgeldhöhe beschränkt. Der Großteil der vom HmbBfDI verhängten Bußgelder wurde von den Adressaten akzeptiert und sie verzichteten auf Einsprüche.

GRENZÜBERSCHREITENDE THEMEN 5.

5. Grenzüberschreitende Themen

5.1 Europäische Aktivitäten

5.1.1 Dringlichkeitsverfahren Facebook

Der HmbBfDI hat im Frühjahr 2021 eine Unterlassungsanordnung gegen Facebook im Wege eines sog. Dringlichkeitsverfahrens nach Art. 66 Abs. 1 DSGVO erlassen und anschließend nach Art. 66 Abs. 2 DSGVO den Europäischen Datenschutzausschuss um einen verbindlichen Beschluss ersucht.

Der HmbBfDI erließ am 10. Mai 2021 eine Unterlassungsanordnung gegen die Facebook Ireland Limited, in der er die Verantwortliche anwies, nicht ohne eine Rechtsgrundlage bestimmte Verarbeitungen vornehmen zu dürfen. Diese Anordnung war entsprechend der Ausnahmevorschrift des Art. 66 Abs. 1 DSGVO ausschließlich für das Gebiet der Bundesrepublik Deutschland und nur für die Dauer von drei Monaten gültig. Sie ist inzwischen bestandskräftig.

Hintergrund der Anordnung waren die aktualisierten Nutzungsbedingungen und die neue Datenschutzrichtlinie von WhatsApp, mit denen die Nutzer seit Anfang 2021 konfrontiert waren. Die Nutzer von WhatsApp wurden aufgefordert, den neuen Bestimmungen bis spätestens Mitte Mai 2021 zuzustimmen, andernfalls hätten sie WhatsApp nicht weiter sinnvoll nutzen können. Die verfahrensgegenständlichen WhatsApp-Bestimmungen sahen umfangreiche Passagen vor, mit denen sich die Verantwortliche, die WhatsApp Ireland Limited, das Recht einräumte, Daten der Nutzer mit anderen Facebook-Unternehmen zu teilen. Facebooks Datenschutzrichtlinie sieht ebenfalls eine allgemeine unternehmensübergreifende Nutzung und Auswertung von Daten verbundener Unternehmen vor.

Der HmbBfDI sah in den neuen Formulierungen die Gefahr, dass WhatsApp mit den neuen Bestimmungen neben den bereits bestehenden Austauschmöglichkeiten mit Facebook für die Bereiche Pro-

duktverbesserung, Analyse, Network/Security künftig weitere Verarbeitungsmöglichkeiten für Marketingzwecke und Direktwerbung schafft und somit Facebook noch umfassendere Datenverarbeitungen über die unterschiedlichen Dienste hinweg ermöglicht. Nach unserer Auffassung wäre eine solche Nutzung durch Facebook nur möglich, wenn die WhatsApp-Nutzer ihr explizit zugestimmt hätten. Das faktisch alternativlose Akzeptieren von Nutzungsbedingungen ersetzt nicht eine datenschutzrechtliche Einwilligung.

Der HmbBfDI ist in Deutschland für Facebook zuständig, da die deutsche Niederlassung von Facebook ihren Sitz in Hamburg hat. Die europäische Hauptniederlassung von Facebook befindet sich jedoch in Irland. Regulär sehen die Zuständigkeitsregelungen in Art. 55, 56 DSGVO und das Kooperationsverfahren nach Art. 60 ff. DSGVO vor, dass in erster Linie die federführende Aufsichtsbehörde, in diesem Fall die Irish Data Protection Commission (kurz IDPC), aufsichtsrechtlich tätig wird. Das war hier nicht der Fall, so dass der HmbBfDI einen dringenden Handlungsbedarf annahm und einstweilige Maßnahmen ergriff.

Abweichend zum regulären Verfahren der Kooperation und Kohärenz nach Art. 60, 64, 65 DSGVO konnte der HmbBfDI als betroffene Behörde auf Grundlage von Art. 66 Abs. 1 DSGVO einstweilige Maßnahmen gegen die in Irland ansässige Facebook Ireland Ltd. treffen, um die Rechte und Freiheiten deutscher Nutzer zu schützen. Aufgrund der zeitlichen und räumlichen Begrenzung der einstweiligen Anordnung entschied sich der HmbBfDI, zusätzlich zu den vorgenannten Maßnahmen den Europäischen Datenschutzausschuss (EDSA) um einen verbindlichen Beschluss zu ersuchen, der nach Art. 66 Abs. 2 DSGVO eine Dringlichkeitsanordnung nach Abs. 1 verlängern oder sogar ergänzen kann, beispielsweise durch eine Ausdehnung der Anordnung auf den gesamten EU-Raum oder durch endgültige Maßnahmen.

Dem EDSA stehen dabei weitgehende Befugnisse zu: Während Art. 66 Abs. 1 DSGVO klare Vorgaben für den Geltungsbereich vorläufi-

ger Maßnahmen macht (zeitlich und räumlich begrenzt), gibt es keine solchen Vorgaben für den Geltungsbereich endgültiger Maßnahmen nach Art. 66 Abs. 2 DSGVO. Der EDSA entscheidet in solchen Fällen anstelle der federführenden Aufsichtsbehörde, ob es über den begrenzten Geltungsbereich und Zeitraum hinaus weiterer, endgültiger Maßnahmen bedarf. Der EDSA hat dabei keine Kompetenz, über die Rechtmäßigkeit der einstweiligen Maßnahmen der betroffenen Behörde zu befinden. Dies obliegt den nationalen Gerichten. Beide Verfahren nach Art. 66 Abs. 1 und Abs. 2 DSGVO sind daher selbstständige Verfahrensarten mit unterschiedlichen Anforderungen und Zielrichtungen und können auch im Ergebnis sehr unterschiedlich ausgestaltet sein.

Für den EDSA war es das erste Dringlichkeitsverfahren nach Art. 66 Abs. 2 DSGVO. Auf der Grundlage der vorgelegten Nachweise kam der EDSA zu dem Schluss, dass Facebook Ireland Limited mit hoher Wahrscheinlichkeit Nutzerdaten von WhatsApp als (gemeinsam) für die Verarbeitung Verantwortlicher für den gemeinsamen Zweck der Sicherheit und Integrität von WhatsApp und den anderen Facebook-Unternehmen sowie für den gemeinsamen Zweck der Verbesserung der Produkte der Facebook-Unternehmen bereits verarbeitet. Angesichts einiger Widersprüche, Unklarheiten und Unsicherheiten, die in den Nutzerinformationen von WhatsApp einerseits und in einigen schriftlichen Verpflichtungserklärungen von Facebook Ireland Limited sowie in den schriftlichen Angaben von WhatsApp andererseits festgestellt wurden, kam der EDSA jedoch zu dem Schluss, dass er nicht in der Lage ist, mit Sicherheit festzustellen, welche Verarbeitungen tatsächlich durchgeführt werden und auf welche Art und Weise. Daher entschied er, dass die Voraussetzungen für den Nachweis des Vorliegens eines Verstoßes und einer Dringlichkeit nicht erfüllt gewesen seien.

Der EDSA beschloss daher, in diesem Fall keine endgültigen Maßnahmen gegen Facebook Ireland Limited zu erlassen. Er betonte jedoch die hohe Wahrscheinlichkeit von Verstößen, insbesondere im Hinblick auf die Sicherheit und Integrität von WhatsApp Ireland Limited

und der anderen Facebook-Unternehmen sowie im Hinblick auf die Verbesserung der Produkte der Facebook-Unternehmen.

Der EDSA war außerdem der Ansicht, dass diese Angelegenheit rasch weitere Untersuchungen erfordert. Insbesondere sollte überprüft werden, ob die Facebook-Unternehmen in der Praxis Verarbeitungen durchführen, die die Zusammenführung oder den Abgleich der Nutzerdaten von WhatsApp mit eigenen Datensätzen beinhalten, was nicht zuletzt durch die Verwendung von eindeutigen Kennungen erleichtert wird. Aus diesem Grund forderte der EDSA die IDPC auf, vorrangig eine Untersuchung durchzuführen, ob solche Verarbeitungstätigkeiten stattfinden oder nicht, und wenn dies der Fall ist, festzustellen, ob sie eine ordnungsgemäße Rechtsgrundlage gemäß Art. 5 Abs. 1 Buchstabe a und Art. 6 Abs. 1 DSGVO haben. Ferner forderte der EDSA die IDPC auf, die Rolle von Facebook Ireland Limited zu untersuchen, d.h. ob Facebook in Bezug auf diese Verarbeitungen als Auftragsverarbeiter oder als (gemeinsam) für die Verarbeitung Verantwortlicher handelt. Das Ergebnis dieser Untersuchungen steht noch aus.

Das erste Dringlichkeitsverfahren nach Art. 66 Abs. 2 DSGVO berührte eine Reihe von Fragen, auf die der EDSA noch keine abschließenden Antworten gefunden hat. So bleibt beispielsweise weiterhin unklar, welche Anforderungen an die vorzulegenden Nachweise in einem Dringlichkeitsverfahren nach Art. 66 Abs. 2 DSGVO konkret zu stellen sind, wenn eine betroffene, aber ansonsten nicht federführende Behörde ohne umfassende Untersuchungsbefugnisse den EDSA um einen verbindlichen Beschluss ersucht. Diese und weitere Fragen wird der EDSA voraussichtlich in einer neuen bzw. aktualisierten Leitlinie zum Dringlichkeitsverfahren nach Art. 66 DSGVO beantworten.

5.1.2 Einsprüche gegen Beschlussentwürfe nach Art. 60 DSGVO

Eine der Aufgaben der betroffenen Aufsichtsbehörden ist die Prüfung von Beschlussentwürfen der federführenden Aufsichtsbehörden. Soweit erforderlich, sind Einsprüche nach Art. 60 Abs. 4 DSGVO einzulegen. Der HmbBfDI hatte im Berichtszeitraum mehrfach als betroffene Aufsichtsbehörde einen gemeinsamen Einspruch der deutschen Aufsichtsbehörden gegen Beschlussentwürfe der Irish Data Protection Commission koordiniert, mit unterschiedlichem Ausgang.

Die Zahl der Durchsetzungsverfahren in der EU hat im Berichtszeitraum insgesamt zugenommen. Dennoch existieren auch nach vier Jahren seit Einführung der DSGVO nur wenige Entscheidungsentwürfe zu substanziellen Maßnahmen gegen marktmächtige IT-Konzerne wie Facebook oder Twitter, die in Irland ihre europäische Hauptniederlassung haben und grenzüberschreitend in der EU sowie EWR tätig sind.

Umso wichtiger war es für den HmbBfDI, als national federführende und betroffene Aufsichtsbehörde die lange erwarteten Entscheidungsentwürfe der Irish Data Protection Commission (kurz IDPC) zu prüfen. Dabei kam er bei fast allen Entscheidungsentwürfen der IDPC zum Ergebnis, dass ein maßgeblicher und begründeter Einspruch erforderlich war, um ein gleichhohes Schutzniveau bei der Durchsetzung und eine einheitliche Anwendung der DSGVO in Europa zu gewährleisten.

Die Einspruchseinlegung ist in Art. 4 Nr. 24, Art. 60 Abs. 3 und 4 DSGVO geregelt. Danach muss die federführende Aufsichtsbehörde den betroffenen Aufsichtsbehörden einen Entscheidungsentwurf vorlegen, gegen den diese innerhalb einer Frist von vier Wochen einen maßgeblichen und begründeten Einspruch erheben können. Die

Einspruchsfrist verkürzt sich in Art. 60 Abs. 5 DSGVO sogar auf zwei Wochen, wenn die federführende Aufsichtsbehörde einen überarbeiteten Entscheidungsentwurf vorlegt, der auch dann noch nicht konsensfähig ist.

Nach Erhalt eines maßgeblichen und begründeten Einspruchs stehen der federführenden Aufsichtsbehörde zwei Möglichkeiten offen: Sie kann dem maßgeblichen und begründeten Einspruch folgen und einen entsprechend überarbeiteten Entwurf vorlegen oder sie legt die Angelegenheit im Rahmen des Kohärenzverfahrens nach Art. 65 Abs. 1 lit. a DSGVO dem EDSA vor. Danach obliegt es dem Ausschuss, einen verbindlichen Beschluss darüber zu treffen, ob der Einspruch maßgeblich und begründet ist, und wenn ja, über alle Punkte, die Gegenstand des Einspruchs sind, zu entscheiden.

Die einzelnen Schritte und Anforderungen an die Einspruchseinlegung sind in Art. 4 Nr. 24 DSGVO nur grob festgelegt. Daher hat der Europäische Datenschutzausschuss (EDSA) im Berichtzeitraum eine umfassende Leitlinie zum maßgeblichen und begründeten Einspruch verabschiedet, an dessen Erstellung der HmbBfDI gemeinsam mit anderen deutschen Aufsichtsbehörden mitgewirkt hat.

Für deutsche Aufsichtsbehörden bringt die Einspruchseinlegung nach Art. 60 Abs. 4 DSGVO besondere nationalgesetzliche Herausforderungen mit sich: Grundsätzlich ist jede Aufsichtsbehörde berechtigt, sich beim Vorliegen der Voraussetzungen des Art. 4 Nr. 22 DSGVO als betroffene Aufsichtsbehörde zu melden und als solche einen formellen Einspruch einzulegen. Andererseits bedarf es nach § 18 Abs. 1 BDSG einer Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union sowie einer frühzeitigen Einbindung und Abstimmung unter den Aufsichtsbehörden. Nach § 19 Abs. 2 BDSG hat die innerdeutsch federführende Aufsichtsbehörde wiederum eine herausragende Rolle, sofern eine deutsche Niederlassung vorhanden ist, da nur sie die entsprechenden Beschwerden bearbeitet.

Auch wenn für einen Einspruch nach Art. 60 Abs. 4 DSGVO noch kein gemeinsamer Standpunkt im Sinne des § 18 Abs. 1 BDSG erreicht werden muss, haben deutsche Aufsichtsbehörden die Notwendigkeit eines gemeinsamen und koordinierten Auftretens auf der europäischen Ebene erkannt und stehen unter einem immensen Zeitdruck, sich über den vorgelegten Beschlussentwurf auszutauschen und gemeinsam einen maßgeblichen und begründeten Einspruch einzulegen. Die innerdeutsch federführende Aufsichtsbehörde übernimmt dabei die Koordination zwischen den betroffenen Aufsichtsbehörden. Diese Koordinationsaufgabe gilt, solange sie selbst einen Einspruch zu erheben beabsichtigt.

Da der HmbBfDI aufgrund einer deutschen Niederlassung von Facebook in Hamburg bei Entscheidungsentwürfen, die Facebook oder Instagram betreffen die innerdeutsche Federführung im Sinne des § 19 Abs. 2 BDSG innehat, hatte er im Berichtszeitraum mehrmals die Aufgabe, einen gemeinsamen Einspruch zu koordinieren.

Bei zwei Einsprüchen des HmbBfDI ging es in erster Linie um die Auslegung der Rechtsgrundlage für die Datenverarbeitung nach Art. 6 Abs. 1 lit. b DSGVO, die der HmbBfDI als fehlerhaft und nicht in Einklang mit den Richtlinien ansah, die der EDSA verfasst hat. Bei allen bisherigen Einsprüchen gegen die Entscheidungsentwürfe der IDPC wurden zudem die Berechnungsmethode bzw. die Bemessung der Bußgeldhöhe bemängelt. Bislang steht die Stellungnahme der IDPC aus, ob sie diesen gemeinsamen Einsprüchen folgt. Sollte dies nicht der Fall sein, werden auch diese Einsprüche in ein Kohärenzverfahren vor den EDSA nach Art. 65 Abs. 1 lit. a DSGVO getragen werden müssen.

Der HmbBfDI war im Frühjahr 2021 zudem intensiv an einem Einspruch beteiligt, der vom BfDI gegen den Entscheidungsentwurf der IDPC bzgl. der damals neuen Datenschutzerklärung von WhatsApp eingelegt worden ist. Hier befindet sich der BfDI in der koordinierenden Rolle innerhalb Deutschlands, da WhatsApp als Telekommunikationsdienst dessen sachlichem Zuständigkeitsbereich zugeordnet

ist. Aufgrund der Verbindung mit anderen Diensten des Facebook- bzw. Meta-Konzerns haben diese Fälle auch für den HmbBfDI eine hohe Relevanz. Er argumentierte u.a. gegen die Einschätzung der IDPC zum sog. Lossy Hashing-Verfahren und sprach sich für die Bewertung des verwendeten Hashwerts als personenbeziehbares Datum aus. Der EDSA bestätigte diese Auffassung in seinem verbindlichen Beschluss, der von der IDPC entsprechend berücksichtigt und umgesetzt werden musste.

Die kritische Prüfung von Entscheidungsentwürfen federführender Aufsichtsbehörden bei globalen Anbietern mit einer großen Nutzerbasis in Deutschland ist ein wichtiges Element zur Gewährleistung eines der zentralen Ansprüche der DSGVO: die Herstellung eines gleichmäßigen und hohen Datenschutzniveaus in der Europäischen Union. Über die Aufsichtsmaßnahmen der federführenden Behörden wird daher nicht unabhängig von den anderen betroffenen Behörden und letztlich kollektiv entschieden. Dies gilt im umgekehrten Fall ebenso, wenn der HmbBfDI oder eine andere deutsche Aufsichtsbehörde bei grenzüberschreitender Verarbeitung federführend zuständig ist.

5.1.3 Europäischer Datenschutzausschuss

Durch Wahl des Bundesrats wurde ein neuer Ländervertreter im Europäischen Datenschutzausschuss bestimmt und der HmbBfDI damit in dieser Rolle entlastet.

Gemäß § 17 Bundesdatenschutzgesetz (BDSG) obliegt es dem Bundesrat, den Stellvertreter des Gemeinsamen Vertreters im Europäischen Datenschutzausschuss (EDSA) durch Wahl zu bestimmen. Dies hat er im Berichtsjahr getan und in seiner 1006. Sitzung den Bayrischen Landesdatenschutzbeauftragten in diese Funktion gewählt. Damit endet eine längere Phase, während derer der Län-

dervertreter nicht durch eine gesetzlich festgelegte Wahl, sondern aufgrund Ernennung durch die Datenschutzkonferenz (DSK) besetzt war. Der HmbBfDI, der diese Rolle auf Bitten der DSK bereits seit Oktober 2015, damals noch im europäischen Vorgängergremium, der sog. Artikel-29-Gruppe wahrgenommen hat, wurde damit entlastet.

Die Wahrnehmung der Länderinteressen und Vertretung von deren Zuständigkeitsbereichen im EDSA ist eine wichtige Ergänzung der Tätigkeit des Bundesbeauftragten als Gemeinsamem Vertreter. Aufgrund der in Deutschland föderal organisierten Datenschutzaufsicht ist dabei eine enge Abstimmung unter den Landesdatenschutzbeauftragten wichtig. Die vom HmbBfDI bis Mitte 2021 organisierten Vorbereitungskonferenzen und Ergebnisrückmeldungen aus dem EDSA werden von den bayerischen Kollegen dankenswerterweise fortgeführt.

Für den HmbBfDI besteht damit mehr Raum für die inhaltliche Arbeit auf europäischer Ebene. Dies ermöglicht die Bewältigung einer anwachsenden Zahl von Stellungnahmen zu Beschlussentwürfen (siehe Kapitel V 1.2) und die Übernahme zusätzlicher Aufgaben im Rahmen der Ländervertretung in der Social Media Expert Subgroup des EDSA.

Der HmbBfDI hat im Berichtszeitraum seine diesbezüglichen Aufgaben fortgesetzt und intensiviert. Zusätzlich zum laufenden EDSA-Mandat zum Thema „dark patterns“ hat der HmbBfDI im Juli 2021 die Hauptberichterstattung zum Thema Nutzung sozialer Netzwerke durch öffentliche Stellen übernommen. Dieses trägt der EuGH-Rechtsprechung „Wirtschaftsakademie“ in Sachen Facebook Fanpages und der besonderen Vorbildfunktion sowie Aufgaben der öffentlichen Stellen Rechnung. Zudem haben Betroffene gegenüber öffentlichen Stellen erhöhte Erwartungen an Transparenz und sichere Datenverarbeitung als an private Stellen, die soziale Netzwerke nutzen. Mit dem neuen Arbeitspaket will die Social Media Expert Subgroup eine Orientierungshilfe für praktische Vorkehrungen geben, die öffentliche Stellen treffen können, um die Einhaltung der

Rechtsvorschriften zu gewährleisten. Dazu gehört auch die Klärung, ob und wenn ja, wie sie soziale Medien in einer Weise nutzen können, die mit der DSGVO vereinbar ist.

5.1.4 EDSA-Guidelines zur Zusammenarbeit im One-Stop-Shop-Mechanismus

Nur wenn eine starke Regulierung marktmächtiger IT-Konzerne gelingt, erfüllt die DSGVO den ihr zugedachten Zweck auf wirksame Weise. Dieses Ziel ist gefährdet durch eine Zuständigkeitskonzentration in Mitgliedstaaten, in denen nur überschaubare Ergebnisse erzielt werden. Der HmbBfDI hat sich erfolgreich im Europäischen Datenschutzausschuss (EDSA) für umfassende Einwirkungsmöglichkeiten der übrigen Aufsichtsbehörden eingesetzt.

Bei der Durchsetzung der DSGVO-Anforderungen bei grenzüberschreitenden Fällen kommt der federführenden Behörde am Ort der Hauptniederlassung des Verantwortlichen eine Schlüsselposition zu. Nur diese Datenschutzbehörde kann Aufsichtsmaßnahmen mit Außenwirkung erlassen. Hier entscheidet sich das Gelingen des vor vier Jahren eingeführten harmonisierten Datenschutzrechts. Ausgerechnet die IT-Unternehmen von globaler Marktmacht haben ihre Europazentralen zumeist in denselben EU-Mitgliedstaaten angesiedelt. Es ist somit von unionsweiter Bedeutung, dass dort eine schlagkräftige Aufsicht ausgeübt wird. Dies hat der Gesetzgeber mitgedacht in Form des Kooperationsverfahrens nach Art. 60 DSGVO. Die federführende Aufsichtsbehörde hat sich danach bei der Bearbeitung grenzüberschreitender Fälle mit den übrigen betroffenen Behörden anderer Mitgliedstaaten abzustimmen. Diese können unter Umständen die Einleitung von Prüfverfahren durch die federführende Behörde erzwingen und auch gegen deren Ergebnisse ein Veto einlegen.

In der Praxis ist die Rechtsdurchsetzung gegenüber internationa-

len Großkonzernen aus zwei Gründen wenig zufriedenstellend. Zum einen kennt die DSGVO keine Zeitvorgabe für die Beendigung von Prüfverfahren. In der Folge existieren auch vier Jahre nach Einführung der DSGVO nur wenige Entscheidungsentwürfe zu substanziellen Maßnahmen gegen marktmächtige IT-Konzerne. Zum anderen bestanden bislang Meinungsverschiedenheiten darüber, in welchen Fällen das Kooperationsverfahren des Art. 60 DSGVO greift, sodass die federführenden Behörden zu einer Tätigkeit gezwungen werden können. Für Beschwerden, in denen eine betroffene Person geltend macht, in ihren eigenen Rechten verletzt zu sein, war dies zwar seit jeher unstreitig. Weniger eindeutige Fälle betrafen jedoch beispielsweise Medienberichte oder auch Informationen von Whistleblowern über geplante Geschäftsmodelle mit Kundendaten, bei denen noch nicht bekannt war, ob sie schon umgesetzt waren. Entsprechende Hinweise, die der HmbBfDI und andere betroffene Behörden den jeweiligen federführenden Aufsichtsbehörden zur Kenntnis gegeben haben, wurden dort bisweilen nicht durchgehend verfolgt. Da die Entscheidung, keine Ermittlungen einzuleiten, auch nicht per Entscheidungsentwurf zurückgemeldet wurde, bestand keine Handhabe der übrigen Behörden, mittels eines Einspruchs eine Untersuchung zu erzwingen.

Zur Klärung der internen Verfahren war der HmbBfDI einer der Berichterstatter mehrerer umfassender interner Papiere des EDSA. Dies betrifft zunächst ein noch in Bearbeitung befindliches Dokument zur Zusammenarbeit nach Art. 60 DSGVO, dessen Teile zu den Absätzen 1 und 3 im März 2021 vom EDSA Plenum mit nur einer Gegenstimme angenommen wurden. Die vorangegangenen Verhandlungen im EDSA hatten gezeigt, dass nie zuvor eine Thematik in dem Gremium derart umkämpft gewesen war.

Der EDSA hat sich in diesen prozeduralen Leitlinien für einen weiten Anwendungsbereich des Kooperationsverfahrens ausgesprochen. Alle grenzüberschreitenden Fälle, in denen eine federführende und mindestens eine betroffene Aufsichtsbehörde existieren, sind demnach nach Art. 60 DSGVO zu behandeln. Dies beinhaltet neben

Konstellationen mit von der betroffenen Person zurückgezogener Beschwerde auch explizit solche, in denen das nationale Verfahrensrecht keinen Abschluss mittels eines Beschlusses vorsieht. Auch Medienberichte oder Informationen von Whistleblowern, die keine Beschwerden im Sinne des Art. 77 DSGVO sind, lösen das Kooperationsverfahren aus, wenn sie konkret und substantiiert sind. Nicht ausreichend ist es nach der Einschätzung des EDSA in der Regel, wenn ein wenig detaillierter Zeitungsartikel unkommentiert weitergeleitet wird. Es bedarf insofern weiterer einordnender Erläuterungen der übersendenden Behörde. Nicht notwendig ist es hingegen, dass die betroffene Aufsichtsbehörde einen Beweis vorlegt, dass die in dem Zeitungsartikel beschriebene Datenverarbeitung tatsächlich stattfindet oder dass sie gar die Identitäten konkreter Betroffener benennen kann. Es ist schließlich Aufgabe der federführenden Behörde im Rahmen des Verfahrens nach Art. 60 DSGVO zu ermitteln, ob ein Verstoß vorliegt. Ob und in welchem Umfang die federführende Behörde Ermittlungen einleitet, entscheidet sie bei derartigen Fällen, die keine Beschwerden sind, zunächst selbst im eigenen Ermessen. Wenn das Kooperationsverfahren eröffnet ist, hat sie die Entscheidung, nicht tätig zu werden, jedoch den übrigen betroffenen Behörden vorzulegen, die ein Veto dagegen einlegen können. Wird dem Einspruch nicht abgeholfen, kann der EDSA dann gegebenenfalls ein Prüfverfahren durch die federführende Behörde erzwingen.

Bei aller prozeduraler Autonomie betont der EDSA den Vorrang des Unionsrechts und die Pflicht aller Aufsichtsbehörden, die praktische Wirksamkeit der DSGVO zu gewährleisten. Dazu gehört auch ein hohes Maß an Kommunikation und Transparenz. Der EDSA hat dafür die Anforderungen an frühzeitigen und umfassenden Informationsaustausch nach Art. 60 Abs. 1 und 2 DSGVO konkretisiert und auch Form, Inhalt und Umfang der Entscheidungsentwürfe federführender Behörden so beschrieben, dass sich betroffene Behörden optimal in die Fallbearbeitung einbringen können.

Neben dem einstimmig beschlossenen Internal EDPB Document 02/2021 zu Pflichten bei der Beschwerdebearbeitung hat der EDSA

noch ein weiteres internes Dokument zur praktischen Umsetzung der sog. gütlichen Einigung (Internal EDPB Document 06/2021 on on the practical implementation of amicable settlements) verabschiedet, bei denen der HmbBfDI ebenfalls Berichterstatter war.

Das interne EDPB Document 06/2021 beschreibt praktische Umsetzungsmöglichkeiten der gütlichen Einigung bei der Bearbeitung grenzüberschreitender Fälle unter Berücksichtigung des One-Stop-Shops-Mechanismus (kurz OSS). Gütliche Einigung stellt nach allgemeinem Verständnis eine alternative Vorgehensweise zur Streitbeilegung dar. Wenn also bei der Aufsichtsbehörde eine Beschwerde über einen mutmaßlichen Verstoß gegen die DSGVO, insbesondere über die Rechte der betroffenen Personen, eingereicht wird, kann die betroffene Aufsichtsbehörde diese Beschwerde mit Einverständnis des Betroffenen beschleunigt im Rahmen einer gütlichen Einigung bearbeiten und den Fall zu Gunsten der betroffenen Personen lösen, ohne dass es einer formellen Abhilfemaßnahme gegenüber dem Verantwortlichen bzw. Auftragsverarbeiter bedarf. Das Dokument richtet sich sowohl an die betroffenen als auch an die federführenden Aufsichtsbehörden, da das Instrument der gütlichen Einigung je nach nationalen Verfahrensregeln in jedem Stadium der Beschwerdebearbeitung Anwendung finden kann. Gütliche Einigung findet sich beispielsweise im Erwägungsgrund 131 DSGVO, der sich vor allem auf Fälle mit Auswirkungen in einem Mitgliedsstaat richtet, oder auch in einigen nationalen Verfahrensvorschriften. Wie die einzelnen Schritte im Kontext des One-Stop-Shops aussehen können, wird im Dokument praxisnah anhand von Fallbeispielen erläutert. Der Schwerpunkt der Fallbeschreibung liegt auf den Merkmalen der Fälle (d. h. relativ einfache Beschwerden über die Rechte der betroffenen Person), die sich besonders für eine gütliche Einigung eignen. Zudem werden die rechtlichen Folgen, einschließlich der Annahme eines Beschlussentwurfes der federführenden Aufsichtsbehörde durch betroffene bzw. unterrichtete Behörden, näher erläutert.

5.2 Internationaler Datenverkehr

5.2.1 Drittlandtransfer beim Einsatz von Tracking

Durch den Einsatz von Cookies und vergleichbaren Technologien kann das Nutzungsverhalten von Besucherinnen und Besuchern einer Website geräteübergreifend verfolgt werden. Oftmals werden bei einem solchen Tracking personenbezogene Daten in Drittländer übermittelt, ohne dass die Datentransfers datenschutzrechtlichen Anforderungen genügen. Im Rahmen seiner Zuständigkeit kann der HmbBfDI die Aussetzung von solchen Drittlandtransfers anordnen.

Durch Anbieter von Telemedien kommen Cookies oder vergleichbare Technologien (z. B. auf einer Website oder in Apps) zum Einsatz, so dass damit auch personenbezogene Daten der Nutzerinnen und Nutzer gewonnen und verarbeitet werden.

Bei den durch die Websitebetreiber eingebundenen Anbietern handelt es sich dabei oft um Unternehmen, die ihren Sitz außerhalb der Europäischen Union (also in einem Drittland) haben. Problematisch ist dies derzeit insbesondere bei der Übermittlung in die USA, da für eine derartige Übermittlung kein Angemessenheitsbeschluss der europäischen Kommission besteht. Im Juli 2020 hat der Europäische Gerichtshof in seiner Entscheidung zu „Schrems II“ (EuGH, Aktenzeichen: C-311/18) den ungehinderten Datenfluss zwischen der EU und den USA für ungültig erklärt. (https://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18). Werden daher beim Tracking, insbesondere durch den Einsatz von Cookies personenbezogene Daten in Drittländer übermittelt, ohne dass die datenschutzrechtlichen Anforderungen der DSGVO vorliegen, ist dagegen die Beschwerde beim HmbBfDI möglich.

Im Rahmen der Bearbeitung von Beschwerden wegen eines Drittlandtransfers durch den Einsatz von Tracking-Technologien, hört der

HmbBfDI die Websitebetreiber zu Art und Umfang des Drittlandtransfers an. Sie erhalten dabei Gelegenheit, den erforderlichen Nachweis zu erbringen, dass bei jedem Transfervorgang die Anforderungen – geeignete Garantien, wie z. B. Standarddatenschutzklauseln, oder bei Vorliegen eines Ausnahmetatbestandes für bestimmte Fälle gemäß Art. 49 DSGVO – an eine rechtmäßige Datenübermittlung ins Drittland erfüllt sind.

Zur Übermittlung personenbezogener Daten an Drittländer hat sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zudem im Rahmen der überarbeiteten Orientierungshilfe für Telemedienanbieter im Dezember 2021 ausdrücklich geäußert. Insbesondere kann eine Einwilligung im Zusammenhang mit Webtracking gerade nicht auf Art. 49 Abs. 1 lit. a) DSGVO gestützt werden (https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf, S. 32):

„Zu beachten ist, dass der reine Abschluss von Standarddatenschutzklauseln wie den von der EU-Kommission beschlossenen Standardvertragsklauseln nicht ausreicht. Es ist darüber hinaus im Einzelfall zu prüfen, ob das Recht oder die Praxis des Drittlandes den durch die Standardvertragsklauseln garantieren Schutz beeinträchtigen und ob ggf. ergänzende Maßnahmen zur Einhaltung dieses Schutzniveaus zu treffen sind. Eine detaillierte Anleitung zum Vorgehen bei der erforderlichen Prüfung hat der Europäische Datenschutzausschuss veröffentlicht.48 Gerade im Zusammenhang mit der Einbindung von Dritt-Inhalten und der Nutzung von Tracking-Dienstleistungen werden allerdings oft keine ausreichenden ergänzenden Maßnahmen möglich sein. In diesem Fall dürfen die betroffenen Dienste nicht genutzt, also auch nicht in die Webseite eingebunden werden. Personenbezogene Daten, die im Zusammenhang mit der regelmäßigen Nachverfolgung von Nutzerverhalten auf Webseite oder in Apps verarbeitet werden, können grundsätzlich nicht auf Grundlage einer Einwilligung nach Art. 49 Abs. 1 lit. a DSG-VO in ein Drittland übermittelt werden. Umfang und Regelmäßigkeit solcher Transfers widersprechen regelmäßig dem Charakter des Art. 49 DSG-VO als Ausnahmevorschrift und den Anforderungen aus Art. 44 S. 2 DSG-VO."

Liegt somit beim Einsatz von Tracking-Technologien ein Drittlandtransfer vor und können die Verantwortlichen die hierfür nötigen zusätzlichen Schutzmaßnahmen nicht nachweisen, handelt es sich um eine unzulässige Datenübermittlung. Nach den Vorgaben der Schrems II-Entscheidung hat der HmbBfDI die Übermittlung auszusetzen oder zu verbieten (s. hierzu 29. TB, Kapitel IV 5).

5.2.2 Koordinierte Prüfung der Taskforce Schrems II

Der Europäische Gerichtshof hat in seiner Schrems-II-Entscheidung einen klaren Handlungsauftrag an die Aufsichtsbehörden kommuniziert. Zur Durchsetzung des Urteils hat die DSK eine Taskforce eingesetzt, die eine gemeinsame Prüfaktion koordiniert.

Die Schrems-II-Entscheidung des Europäischen Gerichtshofs aus dem Jahr 2020 hat die Datenschutzlandschaft nachhaltig geprägt. Datenübermittlungen in Drittstaaten mit anlassloser Massenüberwachung sind seitdem nur noch mit besonderen Sicherungsmaßnahmen zulässig. Nicht bei allen Geschäftsmodellen können diese ohne Änderung der technischen bzw. standortpolitischen Ausgestaltung umgesetzt werden (zum Urteil und dessen Auswirkungen siehe 29. TB, Kapitel IV 5).

Neben den rechtlichen Anforderungen für verantwortliche Stellen hat der Gerichtshof die klare Erwartung an die Aufsichtsbehörden formuliert, diese auch verbindlich und flächendeckend umzusetzen. Im Fall von Beschwerden Betroffener hat er das Entschließungsermessen der zuständigen Behörden reduziert. Um sowohl Marktgleichheit herzustellen als auch eine breite Durchsetzung zu erzielen, hat die DSK eine Taskforce zum Umgang mit der Schrems-II-Entscheidung eingesetzt. Sie hat die Aufgabe, eine gemeinsame, bundesweite Vollzugsstrategie zu entwickeln und umzusetzen, die auch gegenüber den europäischen Aufsichtsbehörden kommuniziert wird. Die Lei-

tung der Taskforce obliegt dem HmbBfDI sowie der Berliner Beauftragten für Datenschutz und Informationsfreiheit. Die Berliner Kollegen konzentrieren sich dabei auf die rechtlichen Auslegungsfragen, die aus dem Urteil folgen, während der HmbBfDI die bundesweite Prüfaktion koordiniert.

Die rechtliche Analyse beinhaltet unter anderem eine Auseinandersetzung mit den Sicherheitsgesetzen der USA, um die Reichweite der Ausführungen des Gerichtshofs auf andere Unternehmen zu ermitteln. Die Taskforce hat zu diesem Zweck ein Gutachten bei Prof. Stephen Vladeck von der Universität Texas in Auftrag gegeben. Der Rechtsexperte war zuvor in den Schrems-Verfahren für Facebook gutachterlich tätig gewesen. Nach seinen Erkenntnissen ist der Anwendungsbereich der US-amerikanischen Überwachungsgesetze wesentlich weiter als bislang in Europa zumeist angenommen. So können dem Tatbestandsmerkmal des electronic communication service je nach Einzelfall auch Unternehmen aller Branchen unterfallen, wenn sie entsprechende interne Softwareprodukte nutzen. Es ist vorgesehen, das Gutachten Anfang 2022 zu veröffentlichen.

An der vom HmbBfDI geleiteten Prüfaktion nehmen zehn Landesdatenschutzbehörden sowie eine kirchliche Aufsichtsbehörde teil. In gemeinsamer Abstimmung hat sich die Taskforce auf fünf Fallgruppen geeinigt, die im jeweiligen Zuständigkeitsbereich überprüft werden. Zu jeder Fallgruppe wurden einheitliche Fragebögen entwickelt, die unter www.datenschutz-hamburg.de/pages/fragebogenaktion/ veröffentlicht wurden. Dabei obliegt es jeder teilnehmenden Behörde, selbst zu entscheiden, welche der Fragebögen sie verwendet und wie viele Adressaten sie damit anschreibt. Die Fallgruppen des Webhosting und des Mailhosting wurden ausgewählt, weil dafür häufig Dienstleister aus Drittstaaten eingesetzt werden, während adäquate europäische Alternativen existieren und ein Wechsel relativ unkompliziert und zeitnah möglich ist. Aufgrund der besonderen Schutzbedürftigkeit von Bewerberinnen und Bewerbern werden zudem Bewerberverwaltungssysteme betrachtet. Ein weiterer Fragebogen betrifft das Webtracking in Anbetracht der Praxisrelevanz des The-

mas. Neben dem Einsatz der genannten externen Dienstleister wird zudem der konzerninterne Austausch von Kundendaten innerhalb einer Unternehmensgruppe als weitere Fallgruppe überprüft, da die Schrems-Entscheidungen des Europäischen Gerichtshofs auf eine solche Konstellation zurückgehen.

Die teilnehmenden Aufsichtsbehörden würdigen jeden Fall individuell anhand seiner Einzigartigkeit und üben selbständige Ermessensentscheidungen aus. Damit dies in koordinierter Weise erfolgt, tauschen sie sich in regelmäßigen Terminen über den Stand der Verfahren und den Umgang mit den Antworten der verantwortlichen Stellen aus. Zum einen können auf diese Weise rechtliche Fragestellungen einheitlich bewertet werden, zum anderen werden auch verfahrensleitende Fragen wie die Gewährung von Umsetzungsfristen für Nachbesserungen auf diesem Wege abgestimmt.

Der HmbBfDI hat im ersten Schritt 23 Hamburger Unternehmen angeschrieben. Bei sieben Verfahren hat er den Fragebogen zum Webhosting verwendet. Dabei hat er sich auf die Internetseiten von marktrelevanten Onlineshops konzentriert. In Anbetracht der Bedeutung Hamburgs als wichtiger, überregionaler Versandhandelsstandort werden alle wesentlichen Akteure der Branche überprüft. Zwölf Unternehmen haben den Fragebogen zum konzerninternen Datenverkehr erhalten und viermal wurde der Fragebogen zur Bewerberverwaltung verwendet. Zur Auswahl der Adressaten beider Fallgruppen wurden Erkenntnisse einer vergleichbaren Aktion aus dem Jahr 2015 nach der Schrems-I-Entscheidung ausgewertet (zur damaligen Prüfung 25. TB, Kapitel X 1; 26. TB, Kapitel IV 4). Damit konnten gezielt verantwortliche Stellen angeschrieben werden, bei denen Grund zur Annahme besteht, dass sie die zu überprüfenden Datenverarbeitungen tatsächlich durchführen.

Aufgrund der großen Komplexität der meisten Antworten dauern die Prüfungen in Hamburg noch an. Erste Erkenntnisse zeigen ein differenziertes Bild. Während die Antworten teilweise zu erkennen geben, dass bislang noch nicht einmal eine zufriedenstellende Aus-

einandersetzung mit den neuen rechtlichen Anforderungen stattgefunden hat, präsentieren andere Verantwortliche mitunter gut durchdachte und effektive Lösungen zur Umsetzung der Vorgaben des Europäischen Gerichtshofs. Wo noch Defizite bestehen, soll zunächst im kooperativen Dialog eine Beendigung des Datenschutzverstoßes erwirkt werden. Gelingt dies nicht, sind gegebenenfalls verwaltungsrechtliche Maßnahmen angezeigt.

BERATUNGEN ÖFFENTLICHER STELLEN 6.

Beratungen öffentlicher Stellen

6.1 Gesundheitsdaten im IT-Verfahren „Beihilfe digital"

Das Authentisierungsverfahren von „Beihilfe digital" erfüllt nicht die Anforderungen nach dem Stand der Technik.

Die Datenschutz-Grundverordnung stellt im Art. 9 Abs. 1 klar, dass Gesundheitsdaten zu den besonders schützenswerten Daten gehören. Das ist in weiten Bereichen Konsens, so zum Beispiel in der Patientenakte und im Praxisinformationssystem. Dies gilt aber nicht nur im Gesundheitsbereich, sondern immer dann, wenn Gesundheitsdaten verarbeitet werden.

Große Mengen von Gesundheitsdaten werden auch im Verwaltungsbereich bei der Beihilfesachbearbeitung verarbeitet. In diesem Verfahren werden sensible Gesundheitsdaten wie z.B. Kopien von Rezepten und Arztrechnungen übertragen und gespeichert, die nicht nur aus der Behandlung durch einen Arzt stammen, sondern aus den verschiedenen Behandlungszusammenhängen einer Person. Im Laufe der Zeit kommen hier die Daten aus mehreren Jahren zusammen. Auch können bereits elektronisch eingereichte Daten im Verfahren „Beihilfe digital" über das Internet wieder abgerufen werden.

Der HmbBfDI hat das Zentrum für Personaldienste (ZPD) der FHH von Anfang an darauf hingewiesen, dass ein solcher Abruf insbesondere eine 2-Faktor-Authentisierung unter Nutzung eines Hardwaretokens erfordert. Hierfür kommt vor allem die Online-Ausweisfunktion in Frage, die bereits bei anderen Verfahren der hamburgischen Verwaltung als Authentisierungsmittel genutzt wird.

Im Zuge der weiteren Beratung hat der HmbBfDI bei „Beihilfe digital" geprüft, ob und falls ja unter welchen Bedingungen auch mit einer 2-Faktor-Authentisierung unter Nutzung eines Software-Tokens ein angemessenes Schutzniveau erreicht werden kann. Nach

Auffassung des HmbBfDI kann ein Softwaretoken nur dann genutzt werden, wenn bei „Beihilfe digital" den Betroffenen diese Möglichkeit als zusätzliche Möglichkeit neben der Authentisierung mit einem Hardwaretoken, die dem Stand der Technik entspricht, angeboten wird. Die Betroffenen können dann auf der Grundlage einer ausführlichen Information über die unterschiedlichen Möglichkeiten entscheiden, welches Mittel sie für sich im Einzelfall nutzen möchten. Diese Position des HmbBfDI berücksichtigt auch die im Herbst 2020 erfolgte Änderung des § 336 SGB V, mit der der Zugriff auf eine elektronische Patientenakte für die Betroffenen in der Weise geregelt wurde, dass neben dem Authentisierungsverfahren mit der Gesundheitskarte (Hardwaretoken) den Betroffenen parallel auch ein Authentisierungsverfahren mit einem Softwaretoken angeboten kann, wenn man ihn über die damit verbundenen zusätzlichen Risiken aufklärt. Diese Möglichkeit hat der Gesetzgeber für den Zugriff auf die elektronische Pateientenakte geschaffen, in der vergleichbar sensible Gesundheitsdaten verarbeitet werden wie bei „Beihilfe digital" (vgl. 26. TB, Kapitel VI 2).

Um zu gewährleisten, dass wirklich nur berechtigte Personen diese Daten abrufen, ist eine dem hohen Vertrauensniveau entsprechende Registrierung und Anmeldung an dem Verfahren eine angemessene technische Maßnahme, die dem Stand der Technik entspricht. Hierzu kann insbesondere auf die Technische Richtlinie TR-03107-1 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwiesen werden. Ziel dieser Technischen Richtlinie ist es, Verfahren zu elektronischen Identitäten und Vertrauensdiensten für verschiedene Prozesse des E-Government zu bewerten und Vertrauensniveaus zuzuordnen. Diese Lösungen decken unterschiedliche Prozesse des Identitätsmanagements auf unterschiedlichen Sicherheitsniveaus ab. Auch der IT-Planungsrat zieht diese Richtlinie heran, um die Anforderungen an Authentisierungsmittel abzuleiten (siehe Tabelle nächste Seite).

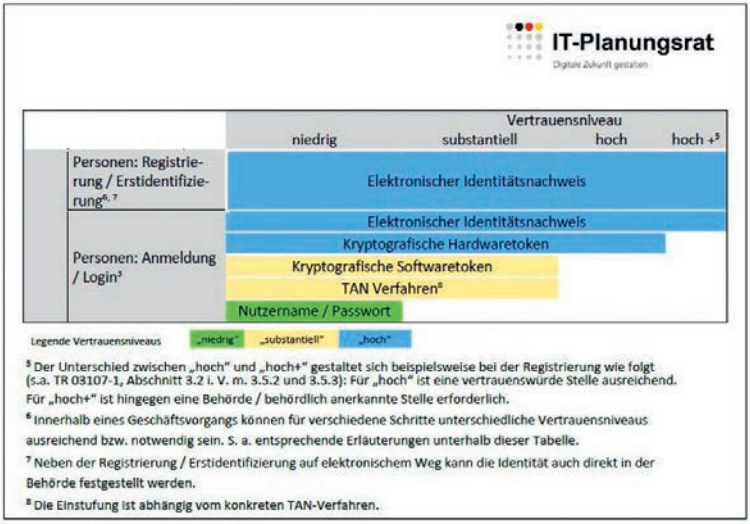


Tabelle: Einordnung der Prozesse in die jeweiligen Vertrauensniveaus Einordnung der Prozesse in die jeweiligen Vertrauensniveaus (Ausschnitt; Quelle: Empfehlungen für die Zuordnung von Vertrauensniveaus in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern bzw. der Wirtschaft Handreichung, Stand: 24.02.2020, Version 4.00 ; IT-Planungsrat)

Als kryptografischer Hardwaretoken kommt insbesondere die Online-Ausweisfunktion des Personalausweises in Frage: Der Personalausweis wird an das Smartphone oder den Kartenleser gehalten und nach PIN-Eingabe können die erforderlichen Daten sicher ausgelesen werden. Besitz (des Personalausweises) und Wissen (der PIN) sind erforderlich.

Auch in diesem Berichtszeitraum hat das ZPD die Auffassung vertreten, dass seine Lösung dem Stand der Technik gem. Art. 32 und 25 DSGVO entspricht, ohne eine Quelle zu benennen, aus der hervorgeht, dass auch mit einem Softwaretoken die erforderlichen Anforderungen gewährleistet werden. Das ZPD hält die Einbindung eines Hardwaretokens nicht für erforderlich. Warum die sensiblen Gesundheitsdaten der Beschäftigten der FHH nicht in gleichem Maße geschützt werden wie Gesundheitsdaten der Bürgerinnen und Bürger bei Online-Diensten nach dem Online-Zugangsgesetz, bleibt somit immer noch offen.

Mit diesem Dissens zwischen dem ZPD und dem HmbBfDI haben wir die Phase der Beratung beendet. Da der Betreiber der App und das ZPD mitgeteilt haben, dass sie „die Entwicklungen zum Stand der Technik im Blick behalten" werden, sieht der HmbBfDI auch weiterhin die Chance, dass beim Anmeldeverfahren zu „Beihilfe digital" ein hohes Sicherheitsniveau erreicht werden kann. Gerade bei Krankenkassen zeichnen sich bei vergleichbar sensiblen Anwendungen entsprechende Entwicklungen ab. Diese wird der HmbBfDI zum Anlass neben, weiterhin mit dem ZPD auch zu „Beihilfe digital" im Gespräch zu bleiben.

6.2 Digitale Personalakte

Nach der flächendeckenden Einführung einer elektronischen Aktenführung für die Sach- und Fachaktenführung der FHH (ELDORADO) soll nun auch eine Digitalisierung der Personalakten und der Bearbeitung von Personalprozessen erfolgen. Bei der Umsetzung der elektronischen Personalakte sind besondere datenschutzrechtliche Anforderungen zu beachten.

In der FHH ist die Personalverwaltung dezentral organisiert, d.h. die Behörden, Ämter, Landesbetriebe und Einrichtungen verfügen in der Regel über eigene Personalabteilungen. Bisher erfolgte die die dortige Personalaktenführung auf Papierbasis. Dies soll sich nun ändern.

Ziel des Projektes Digitale Personalakte ist die Digitalisierung in Papierform vorliegender Personalaktendaten und deren Weiterführung als digitale Personalakte (DigiPA). Dies umfasst die initiale Digitalisierung der vorhandenen Personalakten durch einen Scandienstleister einschließlich der Überführung in das Aktensystem sowie die Weiterführung durch Digitalisierung von Personalvorgängen für die DigiPA.

Die Grundsätze der Personalaktenführung, insbesondere die dafür geltenden rechtlichen Vorgaben, bleiben durch Einführung der

digitalen Personalaktenführung unberührt. Dies betrifft insbesondere die Grundsätze der Transparenz, der Vollständigkeit, der Richtigkeit, der Zulässigkeit und der Vertraulichkeit der Personalaktenführung. Das heißt, bei der Digitalisierung der Personalakten sowie der darauf aufsetzenden Prozesse sind diverse rechtliche Besonderheiten zu beachten, die durch technische und organisatorische Maßnahmen beim neuen IT-Verfahren umzusetzen sind.

Voraussetzung für das Führen einer digitalen Personalakte ist neben der gegebenen rechtlichen Zulässigkeit einer automatisierten Verarbeitung von Personalakten zunächst eine qualitätsgesicherte Digitalisierung der Bestandsakten. Ebenso wie beim nachgelagerten Scannen in der Bearbeitung von Personalprozessen muss geregelt und festgelegt werden, wie mit den Originalunterlagen umgegangen wird, d.h., ob und wann diese vernichtet werden. Hierbei sind die Anforderungen aus der technischen Richtlinie des Bundesamtes für Informationssicherheit BSI TR-03138 „Ersetzendes Scannen (RESISCAN) zu beachten. Ebenso wie eine qualitätssichere Digitalisierung muss vor einer Digitalisierung von Personalvorgängen auch die Möglichkeit einer rückstandslosen Löschung von Unterlagen aus der Personalakte geschaffen werden. Nach dem aktuellen Stand von Eldorado 2.0 ist ein solches Löschen noch nicht möglich, soll aber nun zeitnah umgesetzt werden. Wir werden uns dafür einsetzen, dass ein Rollout erst beginnt, wenn diese Erweiterung in Eldorado produktiv nutzbar ist.

Die nach den Vorgaben des Hamburgischen Beamtengesetzes standardisierte Aktenstruktur insbesondere die Gliederung in eine Grund- und mehrere Teilakten muss entsprechend umgesetzt werden.

Die digitale Personalakte der FHH wurde auf Basis des Dokumentenmanagementsystems ELORADO 2.0 entwickelt, in der die personalaktenführende Schriftgutverwaltung erfolgen soll. Da die Einsichtnahme in Personalakten nur für bestimmte Personengruppen zulässig ist, ist u.a. auch das Berechtigungs- und Rollenkonzept und dessen Umsetzung von maßgeblicher Bedeutung. So wird der Aufruf

der DigiPA ausschließlich über das führende Personalmanagement der FHH (KoPers) erfolgen und den dortigen Zugriffsrechten gefolgt.

Der HmbBfDI wurde frühzeitig vom Projekt informiert und eingebunden und befindet sich laufend in einem sehr konstruktiven Austausch mit diesem Projekt.

6.3 IT-Verfahren „MeinePersonaldaten“

Das Verfahren „MeinePersonaldaten“ soll Beschäftigten und Versorgungempfangenden der FHH den Zugriff auf die eigenen Personaldaten ermöglichen und perspektivisch Abläufe der Personalverwaltung vereinfachen. Die Sensibilität der Daten erfordert angemessene Schutzmaßnahmen für die Daten.

Im Rahmen der Personalverwaltung werden personenbezogene Daten unterschiedlicher Sensibilität verarbeitet, deren Angabe für die Bediensteten verpflichtend ist. Hierzu gehören z.B. Namen, Beschäftigungsdienststelle, private Anschrift, Geburtsdatum, Personalnummer, Steuernummer, Sozialversicherungsnummer, Kirchenzugehörigkeit, Besoldungsgruppe, Familienstand, Kontonummer, aber ggf. auch besonders sensible Daten wie Einträge zur Schwerbehinderung und Gehaltspfändungen. Während bislang nur Mitarbeiterinnen und Mitarbeiter innerhalb der personalverwaltenden Stellen Zugriff auf die im Personalmanagementsystem (KoPers) gespeicherten Daten hatten, werden diese durch MeinePersonaldaten erstmalig Personen außerhalb der Personalverwaltung über das Internet sowie das Intranet zugänglich sein.

„MeinePersonaldaten“ ist eine Plattform, über die die Beschäftigten und Versorgungempfangenden der FHH in der 1. Phase ihre Verdienstabrechnungen bzw. Versorgungsmitteilungen sowie Steuer- und Sozialversicherungsdokumente über das Internet bzw. das Intranet einsehen und herunterladen können. In der 2. Phase sollen

zudem Änderungen (bspw. Adressänderungen oder Änderungen der Kontonummer) sowie das Hochladen von Dokumenten ermöglicht werden.

Das Schutzniveau dieser Daten stellt entsprechende Anforderungen an die einzusetzende Identifizierungs- und Authentisierungslösung. Es muss sicher gewährleistet werden, dass nur die Beschäftigten und Versorgungsempfangenden auf ihre eigenen Verdienstabrechnungen zugreifen können.

Der HmbBfDI begleitet das Verfahren seit ca. 2 Jahren und hat sich aufgrund der Sensibilität der Daten sehr früh für eine 2-Faktor-Authentisierung eingesetzt. Erfreulicherweise wurde diese durch das Projekt für den Zugriff über das Internet auch umgesetzt.

Der Zugriff von Arbeitsplätzen der FHH über das Intranet/FHH-Net wurde konzeptionell nun nachträglich stark „vereinfacht". So soll ein Zugriff ohne explizite Registrierung durch die Nutzerinnen und Nutzer und ohne erforderliche zusätzliche Anmeldung an dem Verfahren ermöglicht werden (Single-Sign-On). Damit ist der Zugriff ausschließlich durch Benutzerkennung und Password des Windows-Accounts abgesichert. Hier setzt sich der HmbBfDI weiter für ergänzende technische-organisatorische Maßnahmen ein. Dies könnte wenigstens ein verfahrensspezifisches Passwort sein, das die Betroffenen vergeben, statt der Nutzung des Single-Sign-On.

Die Nutzungsbedingungen des Verfahrens sehen bislang vor, dass die Teilnehmenden ihre Einwilligung zum Datenabruf und damit die Verarbeitung durch MeinePersonaldaten erklären müssen, wenn sie den digitalen Zugang zum Service MeinePersonaldaten selbst nutzen möchten und sich dafür registrieren. Hierbei handelt es sich jedoch nicht um eine bedingte Freischaltung der Personalfälle für den Abruf von außen durch Setzen eines entsprechenden Kennzeichens (Flags) erst nach Einwilligung des Betroffenen (opt-in), sondern um die Zustimmung zur tatsächlichen Verarbeitung durch das Verfahren „MeinePersonaldaten". Vielmehr werden sämtliche Datenbestände

bereits vor der individuellen Registrierung an das Verfahren angebunden und dann durch die jeweilige Registrierung der Beschäftigten aktiviert.

Für den Online-Zugriff der Beschäftigten und Versorgungsempfangenden wurde auch kein gesonderter „Online-Datenbestand" vorgesehen, in dem idealerweise nur die Daten derer vorgehalten werden, die dieses Verfahren nutzen wollen und in die Online-Verfügbarkeit ihrer Daten eingewilligt haben. Die Freischaltung der Daten und die damit verbundenen Risiken betreffen stattdessen grundsätzlich zunächst einmal sämtliche Beschäftigte und Versorgungsempfangenden der FHH – unabhängig von ihrer tatsächlichen Nutzungsabsicht.

Wer mit der Freischaltung der individuellen Personaldaten für einen Online-Zugriff nicht einverstanden ist, kann diese momentan nur über die Personalsachbearbeitung sperren lassen (opt-out). Hierfür soll künftig eine technische Funktion geschaffen werden. Diese Sperrung bezieht sich jedoch immer auf die in KoPers hinterlegte Person und das dazugehörige Beschäftigungsverhältnis, unabhängig von der Art des Zugriffs. Dies bedeutet, dass man entweder beide Zugriffswege akzeptiert oder keinen. Somit kann bspw. ein auf hohem Schutzniveau abgesicherter Zugriff aus dem Internet mittels Online-Ausweisfunktion des Personalausweises nicht exklusiv aktiviert werden, ohne dass die schwächere Zugriffsmöglichkeit aus dem Intranet in Kauf genommen werden muss.

Der HmbBfDI wird sich weiter für datenschutzfreundliche Lösungen einsetzen.

6.4 Aktuelles zu Nutzerkonten und EfA-Diensten

Mit einem Nutzerkonto können Bürgerinnen und Bürger zukünftig auch die Online-Dienste aller anderen Bundesländer und des Bundes nutzen. Gleichzeitig hat die Senatskanzlei angekündigt, dass die Standards für die länderübergreifende Nutzung nicht für die innerhamburgische Nutzung gelten sollen.

Aktueller Stand bei den Nutzerkonten:
In kleinen Schritten schreitet die bundesweite Digitalisierung der öffentlichen Verwaltung voran. Dazu wurde im Dezember 2020 das Online-Zugangsgesetz (OZG) fortgeschrieben. Ein Ziel dieser Fortschreibung ist es, dass Bürgerinnen und Bürger mit einem Nutzerkonto eines Bundeslandes oder des Bundes auch alle Online-Dienste der anderen Bundesländer und des Bundes nutzen kann. So muss man sich nur einmal registrieren. Die Daten werden auf der Grundlage von Art. 6 Abs. 1 e) DSGVO, in Verbindung mit § 8 Online-Zugangsgesetz (OZG), § 4 Hamburgisches Datenschutzgesetz (HmbDSG) und § 25 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) verarbeitet. Diese Regelungen bilden die Rechtsgrundlage der Speicherung der personenbezogenen Daten im Nutzerkonto. Der vorgesehene Verwendungszweck der Daten wurde um die Speicherung für die länderübergreifende Nutzung erweitert. Eine solche Speicherung erfolgt jedoch nur, wenn ein Nutzer individuell dieser Speicherung zustimmt bzw., wie der Gesetztext formuliert, „einwilligt".

Auch für die Übermittlung der Daten aus dem Nutzerkonto zu einem Online-Dienst muss der Betroffene gemäß § 8 Abs. 5 Satz 1 OZG zustimmen. Der HmbBfDI hat sich dafür eingesetzt, dass diese Zustimmung immer nur für den jeweiligen Einzelfall gilt und dem Nutzer konkret angezeigt wird, welche Daten in diesem Einzelfall an den Online-Dienst übermittelt werden sollen. So kann er vor dem Absenden kontrollieren, ob diese Daten noch aktuell sind und ggf.

korrigierend eingreifen. Diese Regelung dient insbesondere der Transparenz. Die Projektgruppe des IT-Planungsrates, in der die Verantwortlichen für Nutzerkonten aller Länder und des Bundes vertreten sind, hat diesen Vorschlag aufgegriffen und für die länderübergreifende Nutzung der Daten im Nutzerkonto beschlossen.

Anders verhält es sich jedoch mit der Nutzung der im Nutzerkonto gespeicherten Daten für die Nutzung eines Online-Dienstes innerhalb des gleichen Bundeslandes. Für diese Fallkonstellation konnten sich die Verantwortlichen nicht auf ein einheitliches Vorgehen einigen. So vertrat die hamburgische Senatskanzlei in 2021 lange die Rechtauffassung, dass für eine landesinterne Übermittlung der Daten an einen hamburgischen Online-Dienst keine Zustimmung in jedem Einzelfall erfolgen muss. Ebenfalls ist sie der Auffassung, dass dem Nutzer der Übermittlung der Daten aus dem Nutzerkonto an den Online-Dienst diese Daten nicht angezeigt werden müssen. Aus Sicht des HmbBfDI bietet das OZG keinen Anhaltspunkt, der eine solche Benachteiligung bei der innerhamburgischen Anwendung rechtfertigen würde. Die unterschiedliche Vorgehensweise ist weder rechtlich begründbar, noch ist diese transparent für die Betroffenen. Kurz vor Redaktionsschluss hat der HmbBfDI auf Nachfrage eine Zuschrift der Senatskanzlei erhalten, in der ausgeführt wird, dass dem Nutzer auch dann eine Übersicht aller Daten angezeigt werden, die an einen hamburgischen Online-Dienst gesendet werden. Hierin liege eine konkludente Einwilligung, die den Anforderungen einer Einwilligung im Sinne des OZG und der DSGVO Rechnung trägt. Auch wenn die Erörterungen hierzu noch nicht abgeschlossen sind, zeichnet sich doch eine Verständigung in diesem Punkte ab.

Das Nutzerkonto enthält zukünftig auch ein Postfach, über das die Entscheidungen eines Online-Dienstes, etwa ein Bescheid eines Antrags, der betroffenen Person zugestellt werden kann. Dieser Aspekt wurde ebenfalls mit der Fortschreibung des OZG 2020 neu geregelt. Auch hier gilt, dass das Postfach des Nutzers nur dann für die Bescheid-Zustellung genutzt werden darf, falls er dieser Form der Bescheid-Zustellung explizit zustimmt. Dies ist in § 9 OZG geregelt.

Nach Auffassung des HmbBfDI muss auch diese Zustimmung in jedem Einzelfall erfolgen. Das Bundesministerium des Inneren, für Bau und Heimat vertritt diese Rechtsauffassung ebenfalls. Hintergrund ist, dass mit der Verabschiedung des neuen § 9 OZG dem Nutzer auferlegt wurde, dass er alleine dafür verantwortlich ist, regelmäßig zu kontrollieren, ob es einen neuen Eingang in seinem Postfach gibt. Im Regelfall wird der Nutzer zwar mit einer Mail über solch einen Neueingang im Posteingang seines Nutzerkontos informiert. Von großer Bedeutung ist jedoch, dass ein Bescheid auch dann als zugestellt gilt, wenn dieser im Posteingang des Nutzerkontos eingegangen ist, auch wenn der Nutzer über diesen Eingang nicht informiert wurde. Zudem beginnen mit der Zustellung sofort Fristen zu laufen, innerhalb derer der Nutzer z.B. Widerspruch einlegen muss. Es kann also gut sein, dass ein Nutzer zwar mit den Daten aus seinem Nutzerkonto einen Antrag stellen möchte, aber diese regelmäßige zusätzliche Kontrolle eines Einganges in seinem Postfach nicht übernehmen möchte oder kann. Die Bescheid-Zustellung würde in solchen Fällen über einen anderen Weg erfolgen, etwa mit der Briefpost.

Bezüglich dieser Frage besteht derzeit zwischen den Verantwortlichen der Länder und des Bundes noch kein Konsens. Die länderübergreifende Nutzung verzögert sich aufgrund dieser offenen Rechtsfrage voraussichtlich bis weit in das Jahr 2022. Auch bei diesem Thema hat die hamburgische Senatskanzlei angekündigt, dass sie eine Einzelfall-bezogene Einwilligung für die Bescheid-Zustellung nicht für erforderlich hält und diese zumindest für die innerhamburgische Anwendung nicht realisieren wird. Trotz mehrfacher Nachfragen hat der HmbBfDI noch keine Darlegung erhalten, auf welche Rechtsgrundlage die Senatskanzlei ihre Auslegung stützt.

Mit dem Nutzerkonto soll eine sichere, datenschutzgerechte und benutzerfreundliche Möglichkeit zur Verfügung gestellt werden. Je nach Dienst werden Daten mit sehr unterschiedlicher Sensibilität verarbeitet. Um diesen unterschiedlichen Anforderungen gerecht werden zu können, sehen die Rechtsgrundlagen unterschiedliche Vertrauensniveaus bei der Anmeldung vor. Zu begrüßen ist, dass

die Senatskanzlei für die Bürgerkonten seit langem die Online-Ausweisfunktion des Personalausweises als eine Option bei der Anmeldung am Nutzerkonto eingefügt hat. Doch weitere Varianten, die eine relativ große Verbreitung haben, werden derzeit noch nicht angeboten und sind auch für 2022 nicht eingeplant. Hier ist als Beispiel das Elster-Zertifikat zu nennen, das von der Einreichung der Steuererklärung auf elektronischem Wege bekannt ist. Seit der OZG-Fortschreibung 2020 kann dieses Zertifikat auch für den Authentifizierungs-Prozess bei der Anmeldung am Nutzerkonto zum Einsatz kommen. Noch liegen keine Planungen vor, ob und wann diese Variante 2022 für die Anmeldung im Nutzerkonto genutzt werden kann. Das gilt auch für die neuen Smart-eID und für eine 2-Faktor-Authentisierung mit einer Authenticator-App, die etwa aus dem Online-Banking bekannt ist und die Sicherheit bei der Anmeldung gegenüber der alleinigen Eingabe von Benutzerkennung und Passwort deutlich erhöht.

Zu den EfA-Diensten:

Das Onlinezugangsgesetz verpflichtet die deutsche Verwaltung, ihre Leistungen für Bürgerinnen, Bürger und Unternehmen bis Ende 2022 auch digital anzubieten. 575 OZG-Leistungen, bestehend aus mehr als 5.000 unterschiedlichen Einzelprozessen, müssen bis Ende 2022 nutzerfreundlich und medienbruchfrei digitalisiert werden. Diese große Anzahl wurde Themenfeldern zugeordnet. Jeweils ein Bundesland bzw. der Bund (**„Einer"**) übernimmt die Federführung für die Entwicklung der Online-Verfahren eines Themenfeldes. Die so entwickelten Programme stehen anschließend **„für Alle"** zur Weiternutzung zur Verfügung. „Einer für Alle" (EfA) ist ein nachvollziehbarer Ansatz in einer föderalen Struktur, der nicht zuletzt ein einheitliches Datenschutzniveau sicherstellt. Der Teufel steckt im Detail. Nach wie vor gibt es mehr Beschreibungen von offenen Rechtsfragen und gerade auch offenen datenschutzrechtlichen Aspekten als Antworten. Konzepte für die technische Umsetzung einer EfA-Nachnutzung wurden trotz Nachfragen dem HmbBfDI noch nicht zur Verfügung gestellt. Der HmbBfDI wird sich dennoch weiter konstruktiv an der datenschutzgerechten Digitalisierung des Ver-

waltungshandelns beteiligen. Auch wenn der Weg zum gesetzlich vorgegebenen Ziel, nach dem die Bundesländer bis Ende 2022 die Umsetzung abgeschlossen haben sollen, noch sehr lang ist.

6.5 Childhood-Haus

Im Spätsommer 2021 wurde der HmbBfDI an der Einführung einer Videovernehmungsanlage im sogenannten Childhood Haus (CHH) beratend hinzugezogen. Das CHH wurde am Universitätsklinikum Hamburg-Eppendorf (UKE) eingerichtet, um Kinder und Jugendliche, die Opfer oder Zeuge von Misshandlungen, sexualisierter Gewalt oder Vernachlässigung geworden sind, in kindgerechter Umgebung und interdisziplinär unter einem Dach untersuchen, beraten und befragen zu können. Die Behörde für Justiz und Verbraucherschutz (BJV) und die Polizei Hamburg übernehmen dabei die Konzeptionierung der Videovernehmungsanlage und baten den HmbBfDI um vorherige Einschätzung der technischen und rechtlichen Ausgestaltung.

In seiner Pressemitteilung vom 21.10.2021 stellt das UKE das neue Kompetenzzentrum für Kinderschutz vor. Darin betont Prof. Dr. Ondruschka, Direktor des Instituts für Rechtsmedizin des UKE:
„Kinderschutz geht uns alle an. Wir alle müssen den Schutz der Jüngsten und Schwächsten in unserer Gesellschaft sicherstellen. Es freut uns sehr, dass wir mit dem Childhood-Haus Hamburg als Kompetenzzentrum für Kinderschutz am UKE nun einen wichtigen weiteren Schritt für unsere Stadt gehen. Für alle Beteiligten ist es das oberste Ziel, eine Retraumatisierung der Kinder zu vermeiden und die Untersuchungsprozesse so kinderfreundlich und effizient wie möglich zu gestalten." (https://www.uke.de/allgemein/presse/pressemitteilungen/detailseite_112971.html)

Kinder und Jugendliche sollen in der vertrauten Umgebung des CHH im Rahmen von Ermittlungsverfahren durch die zuständigen Stellen

in kindgerechter Atmosphäre und Umgebung befragt werden können. Der Vernehmungsraum im CHH soll mit Kameras und Mikrofonen ausgestattet werden. Die polizeilichen und ggf. staatsanwaltlichen Vernehmungen sollen audiovisuell dokumentiert oder im Zuge von Gerichtsverfahren in Echtzeit in das Strafjustizgebäude übertragen werden können. Von einem Nebenraum aus kann die Übertragung gesteuert oder die Speicherung auf einen Datenträger vorgenommen werden. Das Projekt verfolgt das Ziel, die notwendigen Befragungen und Vernehmungen für Kinder und Jugendliche so schonend wie möglich zu gestalten.

Unter dieser Maßgabe wurde der HmbBfDI von der federführenden BJV im September 2021 zu einem Gespräch mit der Polizei Hamburg und den Beteiligten aus dem Bereich Justiz eingeladen, um über die grundsätzlichen datenschutzrechtlichen Anforderungen im Allgemeinen und im Speziellen die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten der Kinder im Rahmen der Videovernehmung im Childhood-Haus zu sprechen. Im Zuge dieser ersten Beratung wurden verschiedene Aspekte diskutiert, die insbesondere die installierten technischen (Videokonferenz-)Systeme und Arbeitsplätze betrafen.

Auch die Frage der datenschutzrechtlichen Verantwortlichkeit wurde intensiv besprochen. Die Verantwortung für die Einhaltung des Datenschutzes und den Schutz der Rechte der betroffenen Personen liegt bei dem sog. Verantwortlichen, dem durch Gesetz verschiedene Verpflichtungen zugewiesen werden. Aufgrund der Vielzahl von Beteiligen an dem Projekt – u.a. die Polizei, die Gerichte aber auch das UKE – und die unterschiedlich großen Beiträge und tatsächlichen Einwirkungs- und Einflussmöglichkeiten jedes einzelnen Beteiligten, ist die Bestimmung der datenschutzrechtlichen Verantwortlichkeit komplex. Sofern nämlich mehrere Parteien an einem datenschutzrechtlichen Projekt beteiligt sind, kommt es sowohl in Betracht, dass es mehrere Verantwortliche gibt und sich um sog. gemeinsame Verantwortliche (§ 63 BDSG) handelt, oder aber auch ein oder mehrere Beteiligte(r) als Auftragsverarbeiter

(§ 62 BDSG) für den/die (gemeinsamen) Verantwortlichen die Daten verarbeiten.

Verantwortlicher im datenschutzrechtlichen Sinne ist dabei jede Behörde, Einrichtung oder Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (§ 46 Nr. 7 BDSG). Auftragsverarbeiter ist jede Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Liegt eine gemeinsame Verantwortlichkeit vor, sind neben den gesetzlich zugewiesenen Pflichten auch die weiteren Vorgaben nach § 63 BDSG zu beachten; bei Auftragsverarbeitung die Vorgaben nach § 62 BDSG.

Aufgrund der zum Zeitpunkt der ersten Einbindung mitgeteilten Informationen war der HmbBfDI zunächst nicht in der Lage, eindeutig zu beurteilen, welche Rolle welche Partei einnimmt und welche datenschutzrechtlichen Fragestellungen noch einer weiteren Klärung zwischen den Beteiligten bedürfen. Der HmbBfDI übermittelte daraufhin Anfang Oktober nach Absprache mit den Parteien einen umfangreichen Fragenkatalog, der zum Ziel hatte, diese offenen datenschutzrechtlichen Fragen für die am Verfahren beteiligten Stellen greifbar zu machen und eine bessere Beurteilung und Abstimmung untereinander zu ermöglichen.

Neben der Klärung der Verantwortlichkeit, war dem HmbBfDI auch insbesondere die Frage einer hinreichenden Protokollierung wichtig, die die Zugriffe auf die Systeme und die damit verbundene Nutzung sowie Einsichtnahmen in die gespeicherten Videos dokumentiert. Dies ist zur Kontrolle der datenschutzrechtlichen Vorgänge gem. den Vorgaben des § 76 BDSG erforderlich. In einem Folgegespräch mit der BJV wurde dem HmbBfDI eine Protokollierungslösung vorgestellt, die eine Kontrolle dieser Vorgänge ermöglicht. Ein Protokollierungskonzept, welches auch die geplante Auswertung dieser Protokolleinträge einschließt, soll erarbeitet werden.

Der HmbBfDI hat zudem u.a. dazu angeraten, die verwendete Technik, die vorhandenen Schnittstellen sowie die regelhaft stattfindenden damit verbundenen Datenflüssen zu klären und ein detailliertes Löschkonzept für die personenbezogenen Daten zu erstellen.

Sowohl die Polizei als auch die BJV haben sich sehr intensiv mit den aufgeworfenen Fragen auseinandergesetzt und die Antworten dem HmbBfDI jeweils zur Verfügung gestellt. Im Ergebnis kann festgehalten werden, dass Maßnahmen ergriffen wurden, um den Schutz der Befragten zu gewährleisten: Der Zugang zu den Räumen wird vom Case Management des CHH kontrolliert, die Hardware befindet sich in verschlossenen Schränken, Datenträger sind verschlüsselt und eine Videokonferenz findet isoliert und transportverschlüsselt über das FHH-Netz statt. Für die Videokonferenzschalte wird das von Dataport betriebene Skype for Business eingesetzt, so dass keine weiteren externen Dienstleister in diese Kommunikation mit einbezogen werden. Die Übertragung der Aufzeichnung einer Vernehmung kann transportverschlüsselt über das FHH-Netz zur Justiz erfolgen. Polizeiliche Vernehmungen werden auf portable Datenträger übertragen, die zusammen mit Abschriften der Audioaufnahmen Eingang in die Ermittlungsakten finden.

Nach Bewertung der Rückmeldungen blieben jedoch noch verschiedene offene Fragen, die aus Sicht des HmbBfDI zwischen den Beteiligten zu klären sind zu. Klärungsbedürftig bleibt zum Redaktionsschluss beispielsweise noch, inwieweit das UKE selbst am Verfahren beteiligt ist, da es die Räumlichkeiten zur Verfügung stellt und zusätzlich das Zugangsmanagement übernimmt. Auch die konkrete technische Ausgestaltung der erforderlichen Mandantentrennung für eine Zugriffsbeschränkung auf die Videoaufzeichnung war noch Gegenstand von Diskussionen zwischen Polizei und BJV. Gleiches trifft auf die geplante automatisierte Löschung von Aufzeichnungen auf den Rechnern im CHH zu. Ein genaues Zeitfenster ist noch festzulegen und zu dokumentieren.

Der HmbBfDI begrüßt im Ergebnis die frühzeitige Einbindung ins Verfahren, da so noch Einfluss genommen werden konnte und datenschutzrechtliche Anforderungen in den Fokus der Planung gerückt wurden.

6.6 ITS-Kongress / Verkehrsprojekte

Der Berücksichtigung von Datenschutz und Datensicherheit ist rund um das Thema Intelligent Transport Systems / Intelligente Verkehrssysteme (ITS) eine besondere Bedeutung beizumessen. Im Berichtsjahr fand der ITS Weltkongress in Hamburg statt. Der HmbBfDI hat einzelne ITS-Projekte beratend begleitet und die Projektverantwortlichen dahingehend sensibilisiert, eine Balance zu schaffen zwischen dem Datenschutz und den Zielen einer effizienten, sicheren sowie auf „klügere" Weise nutzbaren und damit u.a. umweltfreundlicheren Mobilität.

Der Berücksichtigung von Datenschutz und Datensicherheit ist rund um das Thema Intelligent Transport Systems / Intelligente Verkehrssysteme (ITS) eine besondere Bedeutung beizumessen. Im Berichtsjahr fand der ITS Weltkongress in Hamburg statt. Der HmbBfDI hat einzelne ITS-Projekte beratend begleitet und die Projektverantwortlichen dahingehend sensibilisiert, eine Balance zwischen dem Datenschutz und den Zielen einer effizienten, sicheren sowie auf „klügere" Weise nutzbaren und damit u.a. umweltfreundlicheren Mobilität zu schaffen.

Der ITS Weltkongress ist die weltgrößte Veranstaltung für Innovationen in den Bereichen Mobilität, Logistik und IT. Jedes Jahr ist eine andere Stadt Gastgeber für den Kongress und im September 2021 wurde Hamburg eine Woche lang zum Ausstellungsort. Eine ausgiebige Presseberichterstattung begleitete die wichtigsten Veranstaltungen und Ankündigungen rund um den Kongress. Als Gastgeber bemühte sich Hamburg mit Innovation und Leuchtturmpro-

jekten hervorzutreten. In diesem Rahmen stand der HmbBfDI im Vorfeld beratend verschiedenen Projekten der Stadt zur Seite und konnte sich während des Kongresses Einblick in die Entwicklungen von Industrie und Forschung verschaffen. Viele der wissenschaftlichen Vorträge, Diskussionen und Produktpräsentationen zeigten, wie die Zukunft des Bereiches Verkehrswesen geschrieben werden kann. Für die Bürgerinnen und Bürger kann dies bspw. durch erhöhten Komfort bei automatisiertem Fahren und smarter Verkehrsführung spürbar werden. Auf der Kehrseite stehen neue Gefahren durch Überwachungsmöglichkeiten von Menschen und neue Wege für Cyberangriffe auf vernetzte Infrastruktur und Fahrzeuge. Neben vielen Ansätzen, Verkehr und Transport umweltfreundlicher zu gestalten, stehen vor allem das Erzeugen, Austauschen, Sammeln und Interpretieren von Daten im Vordergrund. Wenn ein Fahrzeug stetig Informationen zum Fahrer erhebt, beispielsweise Sitzposition, Aufmerksamkeit, Reaktionszeiten, Anspannung und Stressniveau, aber auch Daten zu weiteren Passagieren und der Umgebung aufzeichnet und mit anderen teilt, kann dies zu einer gesteigerten Sicherheit für alle Verkehrsteilnehmer führen. Durch die neugewonnene Datenmenge versprechen sich die Hersteller – aber auch Dritte wie bspw. Versicherungsunternehmen – diese Informationen anderweitig auswerten und u.U. lukrativ weiterverwenden zu können.

Zu vernehmen war von verschiedenen Seiten, erhobene Datensätze seien oftmals durch mangelnde Standards und geschlossene Systeme nicht für jeden zugänglich oder ließen sich nicht in Dienste integrieren. Berichtet wurde beispielsweise, wenn eine Stadt aufgrund von gemessenem Verkehrsaufkommen bestimmte Alternativrouten zur Förderung des Verkehrsflusses propagieren möchte, mangele es an Kooperationswillen der Hersteller von viel genutzten Autonavigationssystemen. Die Stadt müsse andere Möglichkeiten schaffen, um Verkehrsteilnehmer zu informieren.

Der HmbBfDI konnte sich mit verkehrsgestaltenden Behörden und Unternehmen austauschen. In weitestgehend allen Ballungszentren mit hohem Verkehrsaufkommen wird mit verschiedenen Konzepten

in den Bereichen Mobilität, Logistik und IT nach Lösungen gesucht. Dank des Messecharakters folgte dem Gespräch mit Herstellern von Hard- und Software oftmals eine aufschlussreiche Demonstration der Produkte und Dienste. Dies war vor allem im Hinblick auf die geplanten Einsätze dieser Produkte in Hamburg hilfreich für zukünftige Beratungen und Prüfungen.

Im Rahmen des ITS-Kongresses sind seitens der FHH 42 sog. Ankerprojekte zu den sechs in der ITS-Strategie benannten Handlungsfeldern Intelligente Fahrzeuge (automatisiertes und vernetztes Fahren), Daten und Informationen, Intelligente Verkehrssteuerung/-lenkung, Intelligente Infrastruktur, Intelligentes Parken sowie Mobilität als Service präsentiert worden.

Zu den nachfolgend angesprochenen Projekten hat es im Vorfeld einen umfangreichen Austausch zwischen den Projektverantwortlichen und dem HmbBfDI gegeben, der hier in beratender Funktion tätig geworden ist. Hinsichtlich der Projekte, die fortgesetzt werden oder noch in Umsetzung sind, wird die Beratung über den Berichtszeitraum hinaus fortgeführt.

6.6.1 Hamburg Electric Autonomous Transportation (HEAT)

Über das Projekt HEAT, einen automatisiert fahrenden Kleinbus in der Hafencity, hat der HmbBfDI aufgrund der in der Vergangenheit erfolgten grundsätzlichen Beratung schon berichtet (vgl. 27. TB, Kapitel V 2.2.1). Dabei handelt es sich um ein Forschungs- und Entwicklungsprojekt der Hamburger Hochbahn AG und weiterer Projektbeteiligter, im Rahmen dessen der Einsatz eines solchen Busses im öffentlichen Nahverkehr erprobt werden sollte. HEAT ist in der sogenannten dritten Integrationsstufe kurz vor und während des ITS-Kongresses im Fahrgastbetrieb unterwegs gewesen. Auch mit Blick darauf war aus datenschutzrechtlicher Sicht relevant, dass der Bus mit unterschiedlichen Kameras – nach außen sowie nach innen – ausgestattet ist, letzteres verbunden mit der Möglichkeit der anlassbezogenen Beobachtung durch die Leitstelle.

Bereits bei der Vorstellung des Projekts waren mit den Projektverantwortlichen, vor allem mit der Hamburger Hochbahn AG, Fragen insbesondere zu den Rechtsgrundlagen für die mit HEAT einhergehende Datenverarbeitung und zur Transparenz gegenüber Nutzerinnen und Nutzer sowie gegenüber passiv betroffenen Verkehrsbeteiligten erörtert worden. Das hat sich durch die unterschiedlichen Integrationsstufen hindurchgezogen und mündete in einen Vor-Ort-Termin im Juli 2021, bei dem die eingesetzte Technik in Augenschein genommen werden konnte und Mitarbeiter der Projektbeteiligten Fragen des HmbBfDI beantwortet haben. Außerdem wurden ergänzende Dokumente zur Verfügung gestellt, Dokumente überarbeitet und mehr Transparenz für Betroffene hergestellt – mittels weiterer Hinweise im und am Bus, an den Haltestellen sowie auf der Website der Hamburger Hochbahn AG.

Momentan ist der Betrieb von HEAT eingestellt. Über eine mögliche Fortführung des Projekts soll wohl im Frühjahr 2022 entschieden werden. Dann würde auch der HmbBfDI HEAT weiterhin beratend begleiten.

6.6.2 Check-in/Be-out – Funktion hvv Any in der hvv switch-App

Unter dem Titel Check-in/Be-out (CiBo) geht es um ein neues Verfahren, mit dem die Hamburger Hochbahn AG Nutzerinnen und Nutzern zukünftig ermöglichen möchte, für in Anspruch genommene Beförderungsleistungen den günstigsten Tarif ermitteln zu lassen und zu bezahlen. Das soll smartphonebasiert über die Funktion hvv Any in der hvv switch-App geschehen. Dafür werden Bluetooth-Signale, so genannte Beacons, von Haltestellen und Fahrzeugen ausgesendet und durch die Smartphones verarbeitet. Auch auf weitere Systemdienste, wie GPS und Bewegungssensoren, müssen die Nutzerinnen und Nutzer der Hamburger Hochbahn AG Zugriff gewähren.

Die Verarbeitung entsprechender Bewegungsdaten soll nur erfolgen, wenn die Nutzerinnen und Nutzer sich damit ausdrücklich und informiert einverstanden erklärt haben und ausschließlich zur Ver-

tragserfüllung. Die Erstellung von Bewegungsprofilen ist ausdrücklich nicht Zweck der Verarbeitung entsprechender Standort- und Bewegungsdaten. Das soll durch technische und organisatorische Maßnahmen sichergestellt werden, wie z.B. eine pseudonymisierte Verarbeitung und die zeitnahe Löschung der Bewegungsdaten nach Abrechnung.

Insbesondere zu diesen technischen und organisatorischen Maßnahmen sowie zum Umgang mit Abbrüchen der Mobilfunkverbindung oder Fehlern/Abstürzen von Software und Betriebssystemen hat der HmbBfDI Gespräche mit den Projektbeteiligten geführt. Auch im Zusammenhang mit diesem Projekt wird es, wenn das Verfahren ab Frühjahr 2022 zum Einsatz kommen soll, darum gehen, für Transparenz zu sorgen und den Nutzerinnen und Nutzer sämtliche notwendigen Informationen zur Funktionalität zur Verfügung zu stellen, damit diese informiert über den Einsatz der Funktion hvv Any entscheiden können. Dazu wird es weiteren Austausch zwischen dem HmbBfDI und der Hamburger Hochbahn AG geben.

6.6.3 Smarte Liefer- und Ladezonen (SmaLa)

Unter der Bezeichnung SmaLa hat die Behörde für Wirtschaft und Innovation (BWI) im Jahr 2021 ein Pilotprojekt gestartet, in dessen Rahmen erprobt werden soll, wie Liefer- und Ladezonen im städtischen Verkehr effizienter genutzt werden können. Über ein digitales Buchungssystem können Paketdienstleister, Kuriere oder Lieferanten in der ersten Projektphase vier Modelladezonen mit acht Stellplätzen im Bezirk Hamburg-Mitte reservieren. Bei diesen handelt es sich um Zonen im absoluten Halteverbot, das für den Buchungszeitraum, also den Zeitraum der voraussichtlichen Anlieferung, für kontrollierende Ordnungskräfte nachvollziehbar außer Kraft gesetzt ist.

Innerhalb der SmaLa-App können die registrierten (Test-)Nutzer ein oder mehrere Kfz-Kennzeichen in Kombination mit Angaben zur jeweiligen Fahrzeuglänge und zur durchschnittlichen Buchungsdauer hinterlegen. Wird für ein Kennzeichen eine Buchung getätigt, wird

eine Ticket-ID generiert, die in der App und in verkürzter Form auf den zur Kennzeichnung der Smarten Liefer- und Ladezonen aufgestellten digitalen Schilder angezeigt wird.

Als Zielgruppe von SmaLa und als Testnutzer des Buchungssystems stehen Paketdienstleister, Kuriere oder Lieferanten und somit im Regelfall Unternehmen im Fokus. Soweit die Fahrzeuge, deren Kennzeichen in der App hinterlegt werden, auf Unternehmen – und somit juristische Personen – zugelassen sind, fällt die Verarbeitung der entsprechenden Daten rund um die Buchung der Ladezonen nicht in den Anwendungsbereich der DSGVO. Denn die DSGVO gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person (s. Erwägungsgrund 14 zur DSGVO). Soweit die DSGVO doch zur Anwendung kommt, weil sich eine natürliche Person für die SmaLa-App registriert und ein ihr zuordenbares Kfz-Kennzeichen dort hinterlegt, erfolgt die Verarbeitung der damit im Zusammehang stehenden Daten zu Zwecken der Vertragserfüllung und auf der Basis des Art. 6 Abs. 1 lit. b DSGVO.

Eine Auswertung des Projekts erfolgt rein statistisch. Eine Zusammenführung mit den Registrierungscodes findet nicht statt, so dass keine Rückschlüsse auf das Buchungsverhalten einer konkreten Fahrerin bzw. eines konkreten Fahrers möglich sind.

In Phase 2 soll das Projekt auf bis zu 25 smarte Liefer- und Ladezonen ausgeweitet werden. Zusätzlich wird es um eine Ausstattung der Zonen z.B. mit absenkbaren Pollern gehen. Es wird darüber nachgedacht, eine solche Automatik mit Hilfe von Kameras zu realisieren, die die Kennzeichen der anfahrenden Kfz erfassen und mit dem Kennzeichen abgleichen, für das die Buchung der Liefer- und Ladezone erfolgt ist. Weil dabei voraussichtlich auch Kennzeichen unbeteiligter privater Kfz erfasst würden, hat der HmbBfDI angeregt, andere Möglichkeiten der Umsetzung, z.B. über die App, zu

erwägen. Dazu, wie sich diese Ausstattung datenschutzkonform realisieren lässt, wird der HmbBfDI auch im Jahr 2022 beratend zur Verfügung stehen.

6.6.4 Probe Vehicle Data (PVD) im Testfeld für Automatisiertes und Vernetztes Fahren

Die rund 9 km lange Teststrecke für die Erprobung des automatisierten und vernetzten Fahrens in der FHH war bereits Thema der Tätigkeitsberichte des HmbBfDI aus den Jahren 2018 und 2019 (vgl. 27. TB, Kapitel V 2.2.1 sowie 28. TB, Kapitel V 2.1). Zuletzt war es um die Ausstattung der Lichtsignalanlagen an der Teststrecke mit sog. Road Side Units gegangen, über die unidirektional die Ampelphasen an empfangsbereite Fahrzeuge ausgesendet werden (Infrastructure2Vehicle-Kommunikation). Dies ist aus Sicht des Datenschutzes in der Regel unproblematisch, da es hierbei nicht zu einer Verarbeitung personenbezogener Daten kommt.

Im Berichtszeitraum ging es nun darum zu testen, inwieweit die für die Kommunikation in diesem Bereich relevanten Cooperative Awareness Messages (CAMs), die moderne Fahrzeuge aussenden, von sog. Roadside ITS Stations empfangen und die darin enthaltenen Informationen zur Verbesserung der Verkehrslagenanalyse – in Ergänzung der bisher dafür eingesetzten Technik, wie u.a. Induktionsschleifen oder Wärmebildkameras – ausgewertet werden können (Vehicle2Infrastructure-Kommunikation). Bei durch Funk übertragenen CAMs handelt es sich um Statusinformationen unter anderem über den Verkehrsfluss, die Fahrzeugposition, die Fahrgeschwindigkeit, die Fahrtrichtung und den Fahrzeugzustand. Regelmäßig mit übermittelt wird auch die sog. ZertifikatsID, die das Fahrzeug und damit letztendlich den Halter identifizierbar macht.

Mit § 63e Straßenverkehrsgesetz (StVG) hat der deutsche Gesetzgeber im Sommer 2021 eine erste Rechtsgrundlage für die Verarbeitung entsprechender, in der Norm abschließend aufgezählter Daten durch den jeweils zuständigen Straßenbaulastträger zum Zweck des Verkehrsmanagements geschaffen. Die Norm schreibt eine an-

onymisierte Auswertung der mit den CAMs übermittelten Daten und eine anschließende unverzügliche Löschung vor.

Im Rahmen des Tests hat sich der für die Datenverarbeitung verantwortliche Landesbetrieb Straßen, Brücken und Gewässer (LSBG) für eine Einwilligungslösung entschieden. Verarbeitet werden nur CAMs einer beschränkten Anzahl an Testnutzern, im Wesentlichen Unternehmen, die der Auswertung zuvor zugestimmt haben. Technisch sichergestellt wird die Beschränkung auf die Testnutzer, indem die CAMs der Testfahrzeuge durch Schlüssel signiert werden, die mittels des von der FHH beantragten Manufacturer Certificats für die Hamburger Public Key Infrastructure erzeugt worden sind. Eine Zuordnung der CAMs zu konkreten Fahrern der Testfahrzeuge ist dem LSBG nicht möglich.

6.6.5 Verkehrsmengenerfassung

Die Umsetzung der automatisierten Verkehrsmengenerfassung wurde in der Vergangenheit bereits vom HmbBfDI begleitet (vgl. 28. TB, Kapitel V 2.2). Damals wurde der datensparsame Ansatz durch Wärmebildkameras gelobt und für unbedenklich eingestuft. Viele Weiterentwicklungen im Bereich Technik ermöglichen einen Ausbau der vorhandenen Infrastruktur. Die Behörde für Verkehr und Mobilitätswende (BVM) beauftragte die Hamburg Verkehrsanlagen GmbH (HHVA) mit dem Aufbau einer flächendeckenden automatisierten Verkehrsmengenerfassung und zusätzlich einer Reisezeitermittlung.

Hierfür wählte man den Hersteller aus, dessen Wärmebildkameras bereits für die Verkehrsmengenerfassung an den großen Knotenpunkten im Bereich der Lichtsignalanlagen installiert sind. Neuere Kameramodelle dieses Herstellers sind mit einem Wifi-Modul ausgestattet, welches die Wifi-Signale der von Verkehrsteilnehmern mitgeführten Smartphones empfangen kann. Dieser Ansatz macht sich die Eigenschaft zunutze, dass Wifi-fähige Geräte nach ihnen bekannten Wifi-Accesspoints suchen. Hierfür werden in regelmäßigen Zeitabständen „Wifi Probe Requests“ Signale gesendet, die

eine dem Gerät zugeordnete MAC-Adresse enthalten. Die durch die Lichtsignalanlagen empfangenen MAC-Adressen sollen gespeichert werden, so dass auf dieser Basis anschließend die Reisezeit für das Testgebiet ermittelt werden kann.

Weiterhin begleitet der HmbBfDI dieses Vorhaben und ist im regen Austausch mit den Verantwortlichen zu folgenden Problemen: Es ist noch nicht entschieden, auf welche Rechtsgrundlage sich die Verantwortlichen stützen können und ob der § 63e Straßenverkehrsgesetz (StVG) zur Anwendung kommen kann. Den Informationspflichten nach Art. 13 DSGVO müsste Genüge getan werden. Aktuell ist eine Website auf hamburg.de geplant, wobei offen ist, wie Betroffene auf diese Website hingewiesen werden sollen.

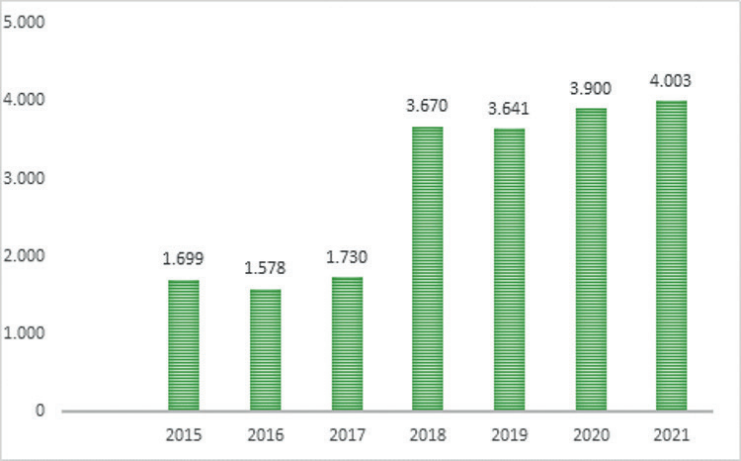
Aktuelle Smartphones verändern stetig ihre verwendeten MAC-Adressen für die beschriebenen Signale, um eine zuverlässige Wiedererkennung zu erschweren. Unklar ist, ob der Kameraherstellen über einen längeren Zeitraum mit dem angestrebten Verfahren aussagekräftige Ergebnisse erzielen kann und es sich somit überhaupt um ein geeignetes Mittel zur Zweckerfüllung handelt. Des Weiteren ist aus Sicht des HmbBfDI eine unnötig lange Speicherung der MAC-Adressen geplant. Problematisch erscheint auch die Verarbeitung in einer Cloud-Infrastruktur eines amerikanischen Anbieters. Mit dieser Lösung steht die Schrems-II-Problematik (vgl. 29. TB, Kapitel IV 5) im Raum, so dass eine Auswertung der MAC-Adressen durch amerikanische Dritte nicht unterbunden werden kann.

7. Informationen zur Behördentätigkeit

1. Statistische Informationen (Zahlen und Fakten)

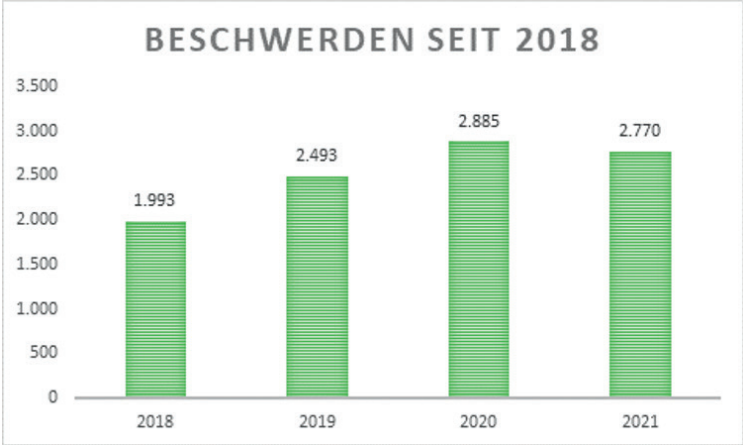
Alle Jahre wieder wird an dieser Stelle des Tätigkeitsberichts des HmbBfDI darüber berichtet, dass die Eingangszahlen im Berichtszeitraum so hoch sind wie nie. Das war auch im Jahr 2021 wieder der Fall, in dem den HmbBfDI 4.003 schriftliche Eingänge erreicht haben. Neben den 320 informationsfreiheitsrechtlichen Eingängen und den 12 Auskunftsanträgen an den HmbBfDI (Art. 15 DSGVO) sind es 3.671 schriftliche Eingänge, die an den HmbBfDI als Datenschutz-Aufsichtsbehörde gerichtet wurden. Dies ist ein neuer Rekord.

Schriftliche Eingänge beim HmbBfDI 2015 – 2021 (gesamt)



1.1 Beschwerden und Beratungen

Datenschutzrechtliche Beschwerden sind schriftliche Eingänge, mit denen Betroffene sich an den HmbBfDI wenden, wenn sie meinen, dass bei einer Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Regelungen der DSGVO verstoßen wurde (Art. 77 DSGVO). 2021 haben den HmbBfDI 2.770 solcher Beschwerden erreicht, das sind rund 69% der Gesamtzahl schriftlicher Eingänge. Das sind deutlich weniger datenschutzrechtliche Beschwerden als im Vorjahr (2.885 bzw. 76%), aber der zweithöchste Wert seit Inkrafttreten der DSGVO:



Betroffene, Unternehmen und Behörden wenden sich aber auch an den HmbBfDI, um in datenschutzrechtlichen Fragen beraten zu werden. Diese Anfragen erreichten den HmbBfDI auch 2021 wieder sowohl schriftlich als auch fernmündlich:

Beratungen 2021

	Betroffene	Unternehmen	Behörden	gesamt
schriftlich	331	171	35	537
telefonisch	461	125	56	642
gesamt	792	296	91	1.179

Die Zahl der schriftlichen Beratungen liegt etwas höher als im Vorjahr (537 zu 486 - 29. TB, Kapitel VII 1.1) und die Zahl der telefonischen Beratungen ist annähernd gleich geblieben (642 zu 634 - 29. TB, Kapitel VII 1.1), sodass insgesamt eine moderate Steigerung von rund 50 Fällen zu verzeichnen ist. Ob diese Zahlen den Trend, der bereits im vergangenen Jahr als Beobachtungsgegenstand avisiert wurde, bestätigen oder verneinen, kann nicht gesagt werden. Hierzu bedarf es der Auswertung der Zahlen der kommenden Jahre.

1.2 Stellungnahmen in Gesetzgebungsverfahren

Aufgrund der ‚Richtlinie zur Beteiligung der/des HmbBfDI' wird der HmbBfDI an der Abstimmung von Drucksachen beteiligt, bevor diese an den Senat und die Hamburgische Bürgerschaft gehen. 2021 erfolgte diese Beteiligung in 75 Fällen, von denen 44 Gesetzgebungs- und Rechtsetzungsvorhaben (einschl. dem Abschluss von Staatsverträgen) zum Inhalt hatten.

1.3 Abhilfemaßnahmen

Auch in diesem Berichtszeitraum hat der HmbBfDI wieder von seinen verschiedenen Abhilfebefugnissen (Art. 58 Abs. 2 DSGVO) Gebrauch gemacht. Im Einzelnen wurden im Jahr 2021 folgende Maßnahmen ergriffen:

Maßnahme	Rechtsgrundlage	Anzahl 2021
Warnungen	Art. 58 Abs. 2 lit. a	1
Verwarnungen	Art. 58 Abs. 2 lit. b	7
Anweisungen und Anordnungen	Art 58. Abs. 2 lit. c – g und j	3
Geldbußen	Art. 58 Abs. 2 lit. i	18
Widerruf von Zertifizierungen	Art. 58 Abs. 2 lit. h	0

1.4 Meldepflicht nach Art. 33 DSGVO

Hackerangriffe, Datenlecks und andere Verletzungen des Schutzes personenbezogener Daten sind der zuständigen Aufsichtsbehörde unverzüglich (möglichst binnen 72 Stunden nach Bekanntwerden) zu melden, wenn voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht.

Im Berichtszeitraum haben den HmbBfDI 871 solcher Meldungen erreicht, von denen allerdings 88 nach Prüfung als nicht meldepflichtige Vorfälle identifiziert wurden. Dennoch ist die Anzahl der Meldungen mit 783 im Vergleich zum Vorjahr um fast 100 Fälle deutlich gestiegen (686 - 29. TB, Kapitel VII 1.2).

Mit 269 Einzelmeldungen ist die häufigste gemeldete Verletzung des Schutzes personenbezogener Daten erneut der Falschversand, also der Versand von E-Mails und Postsendungen an falsche Empfängerinnen und Empfänger; mit 196 Einzelmeldungen sind aber auch Hackerangriffe auf einem sehr hohen Niveau und, im Vergleich zu 2020 (156 - 29. TB VII 1.2), nochmals deutlich gestiegen.

1.5 Europäische Verfahren

Wenn von einer Datenverarbeitung Bürgerinnen und Bürger mehrerer europäischer Staaten betroffen sind, wird dieser Sachverhalt in das Binnenmarkt-Informationssystem (Internal Market Information System, IMI) der Europäischen Kommission eingegeben. Für die Bearbeitung federführend ist dann die Aufsichtsbehörde, in deren Zuständigkeitsbereich der Verantwortliche seine europäische Hauptniederlassung hat, alle anderen Aufsichtsbehörden können sich im Verfahren als betroffen melden.

Im Jahr 2021 war der HmbBfDI an 21 europäischen Verfahren beteiligt:

Europäisches Verfahren	Anzahl 2021
Verfahren mit Betroffenheit (concerned)	16
Verfahren mit Federführung (lead)	5
Weitere Verfahren gem. Kap VII DSGVO (Art. 60 ff)	Keine statistische Erfassung

2. Presse- und Öffentlichkeitsarbeit

Im Berichtsjahr 2021 erreichten den HmbBfDI ca. 300 Presseanfragen. Wichtigste Themenbereiche waren hierbei Datenschutzfragen rund um WhatsApp und Facebook, die konzertierte Fragebogenaktion bezüglich der Umsetzung des Schrems II-Urteils sowie Datenschutzfragen im Kontext der Corona-Pandemie.

Die im Vergleich zum „Rekordjahr" 2020 reduzierte Zahl an Anfragen seitens der Presse und Medien lässt sich vermutlich auf die große mediale Fokussierung auf Themen wie die Corona-Pandemie und die Bundestagswahl zurückführen. Außerdem mag die mit dem Wechsel der Amtsleitung des HmbBfDI verbundene viermonatige Interimsphase ebenfalls ein Faktor gewesen sein.

Gleichwohl haben einige Themen, an denen bereits im Jahr 2020 großes Interesse bestand, weiterhin eine hohe Zahl von Anfragen nach sich gezogen. Hier ist insbesondere der gesamte Komplex um WhatsApp und Facebook zu nennen, also die Änderung der WhatsApp-Nutzungsbedingungen, die Frage des Datenaustauschs zwischen beiden Unternehmen, das Dringlichkeitsverfahren des HmbBfDI gegen Facebook sowie die damit verbundene Entscheidung des Europäischen Datenschutzausschusses. Ebenfalls großes Interesse generierten die Fragebogenaktion des HmbBfDI und anderer deutscher Datenschutzaufsichtsbehörden hinsichtlich der Umsetzung des Schrems II-Urteils in Unternehmen sowie die Prüfungen des HmbBfDI bezüglich der beiden US-Anbieter Clubhouse und Clearview. Wie schon in den Vorjahren sind gerade zu solch grenzüberschreitenden Themen zahlreiche Anfragen ausländischer Medien beim HmbBfDI eingegangen.

Weitere wichtige Themenbereiche waren – ebenfalls wie im Vorjahr – Datenschutzaspekte im Zusammenhang mit der Corona-Pandemie; hier beispielsweise die Diskussion um den Einsatz der Luca App, Fragen zur Datensicherheit in Corona-Testzentren und zum Upload von Impfpässen in Social Media.

Hinsichtlich speziell hamburgischer Themen sind das Bußgeld des HmbBfDI gegen ein Unternehmen eines Energieversorgungs-Konzerns sowie eine Warnung an die Senatskanzlei der Stadt Hamburg hinsichtlich der Nutzung der Videokonferenz-Plattform Zoom hervorzuheben. Des Weiteren ist der Amtswechsel beim HmbBfDI von Johannes Caspar zu Thomas Fuchs als stark angefragtes Thema zu nennen.

Anlässlich des dritten Jahrestages der DSGVO erreichten den HmbBfDI wie bereits in den Vorjahren mehrere statistische Anfragen zur Zahl der Beschwerden, der Data Breaches und der Sanktionen.

Im Berichtszeitraum 2021 haben den HmbBfDI insgesamt 297 Presseanfragen erreicht, das sind ca. 25% weniger als im Vorjahr 2020, das ein „Allzeithoch" von 398 Anfragen aufwies. Im Durchschnitt wurden im Berichtsjahr 2021 rund 25 Anfragen pro Monat bearbeitet.

Bezüglich der beiden großen Internet-Konzerne Facebook und Google lässt sich sagen, dass die Anfragen hierzu – insbesondere durch die Thematik rund um WhatsApp – deutlich zugelegt haben, von ca. 8% der Gesamtanfragenzahl in 2020 auf nun ca. 24% in 2021. Von den beiden Konzernen liegt Facebook (21%) hierbei weit vor Google (3%).

Mit Blick auf die örtliche Herkunft der anfragenden Medien ist wie im Vorjahr zu konstatieren, dass die mit Abstand meisten Anfragen von überregionalen deutschen Medien stammen. Anfragen ausländischer Medien sind im Vergleich zum Jahr 2020 auf gleichem Niveau geblieben, wie die nachstehende Tabelle zeigt:

Presseanfragen...	2020	2021
regionaler Medien:	107	83
überregionaler Medien:	219	143
ausländischer Medien:	72	71
Gesamt:	398	297

Tabelle1: Presseanfragen beim HmbBfDI 2020 und 2021

Neben dem vorliegenden Tätigkeitsbericht Datenschutz 2020 gab es im Berichtsjahr keine weiteren Veröffentlichungen im Printbereich. Das Internet-Angebot des HmbBfDI wird stets aktuell weiterentwickelt; im Berichtsjahr wurde hier zudem verstärkt die Thematik Barrierefreiheit in Angriff genommen. Im Berichtszeitraum hat der HmbBfDI 11 Pressemitteilungen veröffentlicht.

Zudem haben der Hamburgische Datenschutzbeauftragte sowie mehrere Mitarbeiterinnen und Mitarbeiter der Behörde erneut Vorträge und Präsentationen zu Aspekten der DSGVO sowie zu verschiedenen Themen des Datenschutzes durchgeführt und sich an Gesprächsrunden oder Podiumsdiskussionen beteiligt. Corona-bedingt fanden diese Veranstaltungen zumeist als Videokonferenzen statt. Im Rahmen der Datenschutz- und Medienkompetenzförderung des HmbBfDI gab es ebenfalls eine Beteiligung an zahlreichen entsprechenden Veranstaltungen und Aktionen (siehe hierzu ausführlich das nachfolgende Kapitel VII 3).

3. Datenschutzkompetenzförderung durch den HmbBfDI

Bildung und die Förderung von Medien- und Datenschutzkompetenz gehören zu den wichtigsten Aufgaben der modernen demokratischen Gesellschaft: Nur durch Bewusstseinsbildung, Aufklärung und gezielte Bildungsmaßnahmen kann eine aktive und informierte Teilhabe an Gesellschaft und Demokratie gelingen.

Die anhaltende Corona-Krise hat einmal mehr gezeigt, dass das Internet heutzutage allgegenwärtig ist. Wir erleben eine Digitalisierung der Gesellschaft, in der soziale Netzwerke, intelligente Geräte und künstliche Intelligenz immer mehr an gesellschaftlicher Bedeutung gewinnen. Die Gefahren des Identitätsdiebstahls, des Cybermobbings und der Beeinflussung der politischen und gesellschaftlichen Meinungsbildung durch soziale Medien sind längst Realität geworden.

Trotz der anhaltenden Corona-Krise hat der HmbBfDI auch im vergangenen Jahr 2021 Seminare und Workshops in Schulen und weiteren Bildungseinrichtungen zu Themen wie „Fake News & Datenschutz“, „Datenschutz & Demokratie“ oder „Datenschutz bei Messengern“ durchgeführt. Während diese zu Beginn des Jahres unter Einhaltung der damaligen Hygienevorschriften noch in Präsenz stattfinden konnten, fanden die Workshops und Veranstaltungen danach mehrheitlich digital statt.

Dabei stellte sich schnell heraus, dass die durch die FHH zur Verfügung gestellten Videokonferenzdienste „Skype for Business“ und „Cisco Webex“ für dieses Einsatz-Szenario nicht funktionieren. So können sich externe Teilnehmende nur mit einem zusätzlichen Aufwand an diesen Videokonferenzdiensten anmelden. Zudem bringen die beiden Systeme aus fachlicher und didaktischer Sicht einen Workflow mit sich, der aufgrund fehlender Funktionen wie Break-Out-Sessions, direkte visuelle Rückmeldungen („Handheben“, „Daumen hoch“) und Ad-hoc Umfragen nicht mehr zeitgemäß ist und auf zu geringe Akzeptanz bei den externen Teilnehmenden stößt. Daher wurde seitens des HmbBfDI BigBlueButton als Managed-Service beauftragt. BigBlueButton stellt eine datensparsame und transparente, da quelloffen entwickelte, Videokonferenzplattform dar. Die Gründe für die Beschaffung lagen insbesondere in der leicht nutzbaren Oberfläche, den oben genannten Features, kollaborativ nutzbaren Whiteboards und Screensharing-Funktionalitäten. Die Erfahrungen auf allen beteiligten Seiten mit BBB sind als durchweg positiv zu bewerten.

Im April partizipierte der HmbBfDI an dem deutschlandweiten Girls‘ Day und Boys‘ Day. Ziel des bundesweiten Aktionstages ist die klischeefreie Berufsorientierung. So soll der Girls‘ Day und Boys‘ Day Mädchen und Jungen die Möglichkeit bieten, Einblicke in Berufsfelder zu bekommen, die von traditionellen Berufsbildern abweichen. Unter dem Titel „Datenschutz ist langweilig? Von wegen!“ stellte der HmbBfDI die Berufsfelder der Rechtsanwältin und des Rechtsanwalts sowie das der Informatikerinnen und Informatiker vor. Bereits nach

kurzer Zeit waren die jeweils verfügbaren 20 Plätze ausgebucht, sodass insgesamt 40 Schülerinnen und Schüler an der Aktion des HmbBfDI teilnahmen.

Zwei Monate später veranstaltete der HmbBfDI im Rahmen des Digitaltages gemeinsam mit dem Jugendinformationszentrum (JIZ) eine Veranstaltungsreihe zum Themengebiet der Desinformation in den Sozialen Medien. Ziel des Digitaltages ist die Förderung der digitalen Teilhabe, denn alle sollen befähigt werden, sich sicher, souverän, selbstbewusst und selbstbestimmt in der digitalen Welt zu bewegen. So fand neben einem Seminar zum Thema Fake News und Datenschutz in einer Berufsbildenden Schule auch eine digitale Diskussionsrunde zum Thema „Eine Frage der Macht – Der Einfluss der Sozialen Medien auf unsere Demokratie“ mit Experten und Expertinnen statt. Die rege Teilnahme der Gäste zeugte davon, dass dieses Format und die diskutierten Fragestellungen auf großes gesellschaftliches Interesse stoßen.

Des Weiteren hat der HmbBfDI sich zum zweiten Mal in der Rolle der Fachberatung an einer Produktion der FWU Institut für Film und Bild in Wissenschaft und Unterricht gGmbH beteiligt. In dem zweiten Unterrichtsfilm „Social Media: Wie kann ich meine Daten schützen?“ lernen Schüler und Schülerinnen – in Anlehnung an die Ziele der Strategie „Bildung in der digitalen Welt“ der Kultusministerkonferenz (KMK) – beliebte Social Media-Plattformen kennen und werden zu möglichen Gefahren bei der Nutzung sensibilisiert. Außerdem wird zielgruppengerecht erläutert, warum Datenschutz auch im Alltag der Heranwachsenden relevant ist, und es werden Strategien zum Schutz der eigenen Daten im Film vorgestellt.

Der Film und das begleitende Unterrichtsmaterial stehen allen Hamburger Schülerinnen und Schülern über die Schulmediathek Hamburg zur Verfügung.

Der Link zum Film ist zudem in der FWU eigenen Mediathek abrufbar: https://www.fwu-mediathek.de/record?id=xfwu-5523058

Zudem beteiligte sich der HmbBfDI 2021 maßgeblich an der Überarbeitung des gemeinsamen Jugendportals der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sowie des Kantons Zürich, Youngdata.de. Ziel des Relaunches ist eine vollständige technische und inhaltliche Überarbeitung. Die Seite Youngdata wendet sich an Jugendliche im Alter von 13-16 Jahren mit dem Ziel, zum Thema Datenschutz zu informieren und für den sicheren Umgang mit personenbezogenen Daten zu sensibilisieren. Damit kommen die deutschen Datenschutzaufsichtsbehörden ihrem Bildungsauftrag nach Artikel 57 Abs. 1 b DSGVO nach. Auf Basis wissenschaftlicher Erkenntnisse wird die Bedienung der Seite den Gewohnheiten und Bedürfnissen der Zielgruppe angepasst. Auch die Inhalte werden zielgruppennah sowohl hinsichtlich der Auswahl der Themen wie auch der Ansprache der Jugendlichen in Texten und Videos neu gestaltet. Die Inhalte werden weiterhin unter einer freien Lizenz stehen, die eine Weiterverwendung ermöglicht. Auch Lehrkräfte, pädagogisch Tätige oder Eltern können über die Seite Informationen erlangen und didaktisch weiterverwenden.

Eine ausgeprägte Medienkompetenz ist auch für Eltern heute unverzichtbar. Eltern haben mit ihrer Mediennutzung eine Vorbildfunktion und sind damit der Schlüssel für die Medienerziehung der Kinder. Leider stehen Ihnen häufig nur wenige Informationsressourcen zur Verfügung: Zugängliches und unkompliziertes Informationsmaterial ist rar, ebenso wie kompetente Unterstützungs- und Beratungssysteme, an die sich Eltern bei Fragen wenden können. Daher haben sich die Datenschutzbehörden von Hamburg und Mecklenburg-Vorpommern mit dem Hamburger Bürgerrundfunk und Medienkompetenzzentrum TIDE zusammengeschlossen und sich mit dem Projekt D.E.A.P. (Data, Education, Awareness and Protection) auf EU-Fördergelder im Rahmen des Citizens, Equality, Rights and Values Programms (CERV) beworben. Das Projekt D.E.A.P. will Datenschutz für Eltern erlebbar und verständlich machen. Dazu soll in Online-Seminaren und (barrierefreien) Offline-Veranstaltungen das Bewusstsein für datenschutzrechtliche Erziehungsthemen gefördert werden. Darüber hinaus soll mehrsprachiges öffentlich zugängliches Bildungs-

material erstellt und der Aufbau lokaler Multiplikatoren-Strukturen unterstützt werden.

Der besondere Fokus von D.E.A.P. auf der Förderung der digitalen Kompetenz von sozioökonomisch benachteiligten Eltern ist nicht nur innovativ, sondern auch vielversprechend: Ein kritischer und informierter Umgang mit Medien stärkt die gesellschaftliche Teilhabe, den beruflichen Erfolg, die demokratische Bildung sowie die Persönlichkeitsentwicklung.

4. Aufgabenverteilung (Stand: 1.1.2022)

Der Hamburgische Beauftragte
für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22 (7. OG), 20459 Hamburg

Telefon: 040/42854-4040
Telefax: 040/42854-4000

E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.datenschutz-hamburg.de

Dienststellenleiter:	Thomas Fuchs
Stellvertreter:	Ulrich Kühn
Vorzimmer:	Heidi Niemann

Beauftragter für den Haushalt, Personal- und Organisationsleitung, Unternehmerpflichten, Controlling
Arne Gerhards

Haushaltsleitung, -planung und –bewirtschaftung, Berichtswesen, Controlling, Grundsatzfragen Gebührenrecht und Beschaffung
Robert Flechsig

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

Aus- und Fortbildung, Sachbearbeitung Reisekosten, Gebühren und Bußgelder, Gebäudeangelegenheiten und Beschaffung
Rolf Nentwig

Vorzimmer, Geschäftsstelle — Heidi Niemann

Registratur — Frau Vukšić

Registratur, Auskünfte
nach Art. 15 DSGVO — Ipek Sari

Datenschutzkompetenzförderung und Medienbildung, Öffentlichkeitsarbeit	Alina Feustel
Registratur	Komal Tariq
Grundsatzfragen DSGVO, BDSG, HmbDSG und HmbTG, VIG, HmbUIG, Vertretung des HmbBfDI in Gerichtsverfahren	Dr. Christoph Schnabel
Grundsatzfragen HmbVwVfG, VwGO, VwZG, Arbeits-, Dienst- und Disziplinarrecht, Sanktions- und Abhilfebescheide, Einzelfallbearbeitung	Richard Heyer
Grundsatzfragen Sanktionen und Aktenführung, Einzelfallbearbeitung, Sanktions- und Abhilfebescheide	Cornelia Goecke
Grundsatzfragen Art. 58 und Art. 32 f. DSGVO, Sanktions- und Abhilfebescheide, Einzelfallbearbeitung	Steffen Sundermann
Behörde für Inneres und Sport, Polizei, Verfassungsschutz, Behörde für Justiz und Verbraucherschutz, Staatsanwaltschaft, Gerichte, Strafvollzug	Anna-Lena Greve
Pass-, Ausweis- und Meldewesen, Personenstandswesen, Archivwesen, Statistik, Zensus, Mikrozensus	Uta Kranold
Behörde für Inneres und Sport, Polizei, Verfassungsschutz, Feuerwehr, Ausländerwesen, Friedhöfe, Waffenrecht, Hafensicherheitsrecht, Sicherheitsüberprüfungsgesetz	Dirk Pohl

Informationsfreiheit (HmbTG, UIG, VIG), presserechtliche Auskunftsansprüche	Swantje Wallbraun
Stellvertretender Hamburgischer Datenschutzbeauftragter, Akkreditierung und Zertifizierung	Ulrich Kühn
ePrivacy, Presse und Rundfunk, Telemedien und Telekommunikation, Werbung und Direktwerbung, Kultur, Akkreditierung und Zertifizierung	Katja Weber
Tracking und Cookies, themenübergreifende Sachbearbeitung	Amina Merkel
Bildung (Schulen und Hochschulen), Werbung und Direktwerbung, Forschung, Geodaten	Alexander Schiermann
Entwicklung von Prüftools, Smart Devices, Internet of Things, technische Unterstützung bei der Fall- und Sachbearbeitung	Roland Schilling
E-Mail- und Spieleanbieter, Cloud-Dienst eGovernment, Apps, Bewertungsportale	Felix Wagner
Grundsatzfragen Kap. VII DSGVO, Koordination der europäischen Verfahren sowie Verfahren der Zusammenarbeit und Kohärenz, Akkreditierung und Zertifizierung	Frau Jacobson
Suchmaschinen (insb. Google, NorthData)	Dr. Jutta Hazay

Soziale Netzwerke (insbes. Facebook, XING, Twitter), Datingportale	Simone Hoffmann
Akkreditierung und Zertifizierung, technische Unterstützung bei der Fall- und Sachbearbeitung	Herr Schneider
Technische Grundsatzfragen bei eGovernment, technisch-organisatorische Beratung und Prüfung	Dr. Sebastian Wirth
Technische Grundsatzfragen bei Biometrie, Künstliche Intelligenz, Videoüberwachung, Konzeption und Betrieb des Prüflabors, technisch-organisatorische Beratung und Prüfung	Eike Kleinfeld
Technisch-organisatorische Beratung und Prüfung	Jutta Nadler
Technische Grundsatzfragen bei Netzwerken und mobilen Geräten, Konzeption und Betrieb des Prüflabors, technisch-organisatorische Beratung und Prüfung	Herr Maka
Grundsatzfragen Wirtschaft, Internationaler Datenverkehr, Parlamente, Parteien, Fraktionen und Wahlen, Kammern	Dr. Jens Ambrock
Beschäftigtendatenschutz	Oksan Karakus
Kreditwirtschaft, Bauen und Wohnen, Umwelt, Landwirtschaft	Viola Büchl

Gewerbliche Dienstleistungen, Industrie, Versicherungswirtschaft, Rechtsanwälte, Sicherheitsdienste, Notare, Beschäftigtendatenschutz	Pieter Jauernig
Finanz- und Steuerwesen, Steuerberater, Wirtschaftsprüfer, Vereine, Sport, Stiftungen	Heike Wolters
Gesundheit und Soziales	Behrang Raji
Stationärer Handel, Videoüberwachung nicht-öffentlicher Stellen	Bianka Albers-Rosemann
Versandhandel, Inkasso, Auskunfteien	Eggert Thode
Versorger (Strom, Gas, Abfall), Verkehr, Smart City, Gastronomie, Markt- und Meinungsforschung, Kirchen	Sabine Siekmann
Themenübergreifende Sachbearbeitung	Sebastian Reich

STICHWORTVERZEICHNIS

M

N

O

P

R

S

T

U

V

W

Y

Z

Auflage: 750 Exemplare
Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH
Foto Titelseite: Martin Schemm, bearbeitet von Thomas Krenz
Druck: oeding print GmbH

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

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Hamburg