TÄTIGKEITSBERICHT DATENSCHUTZ 2022

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Hamburg

31. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

2022

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: 500 Exemplare
Foto: Titelseite: www.mediaserver.hamburg.de
(U-Bahn-Station HafenCity Universität)
Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH
Druck: Bonifatius GmbH

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

---

vorgelegt im März 2023
Thomas Fuchs
(Redaktionsschluss: 31. Dezember 2022)

INHALTSVERZEICHNIS

Vorwort

Der vorliegende Tätigkeitsbericht Datenschutz 2022 ist dick geworden. Und das nicht, weil wir uns nicht mehr kurzfassen können, sondern weil die große Vielzahl an Themen und Tätigkeiten dies erfordert. Die Bandbreite des Datenschutzes als gesellschaftliches Querschnittsthema wächst weiter.

Im Bereich der durchgeführten Prüfungen hat die Hamburgische Datenschutzbehörde in diesem Jahr eine Höchstmarke erreicht. In diesem Bericht werden 17 davon vorgestellt – darunter zunehmend auch proaktiv eingeleitete Prüfungen, die vermutete Missstände aufhellen können. Zugenommen haben auch die Beratungen öffentlicher Stellen und die grenzüberschreitenden Fälle.

Gerade die europaweiten Verfahren haben in 2022 neue Maßstäbe erreicht. Mit sehr hohen Bußgeldern als Ergebnis europaweiter Abstimmungsverfahren beweist sich zunehmend die Wirksamkeit des europäischen Aufsichtssystems. Der Datenschutzraum Europa wächst weiter zusammen.

Hingegen sind die Eingaben zurückgegangen und liegen erstmals seit 2019 wieder unter 3.000. Ein bundesweiter Trend, für den es nach erster Analyse keine einfachen Erklärungen gibt. Sicher waren im letzten Jahr andere Themen und Krisen von ungleich größerer Bedeutung. Zugleich sind einige Datenschutzthemen – etwa im Zusammenhang mit der Corona-Pandemie – in den Hintergrund getreten. Und es gibt auch Erfolge, wie bei der Gestaltung der Cookie-Banner durch US-amerikanische Unternehmen, die darauf bezogene Beschwerden reduziert haben.

Gestiegen wiederum sind die gemeldeten Cyberangriffe. Mit 212 bei uns eingegangenen Meldungen wurde ein Höchststand erreicht. Dabei ist auffällig, dass zunehmend auch öffentliche Stellen, wie bspw. Hochschulen, Ziel von offenbar gut vorbereiteten und tief in die Systeme eindringenden Angriffen werden.

Insgesamt zeigt der Bericht eindrucksvoll, dass sich die im letzten Jahr angedeutete Änderung der Aufgaben einer Datenschutzbehörde bereits realisiert und das aktive Handeln gegenüber dem reagierenden Ansatz an Bedeutung gewinnt. Dies wird sich mit der anhaltenden digitalen Transformation der Gesellschaft, der weiter unbedingt notwendigen Digitalisierung der staatlichen Dienstleistungen und dem unverändert hohen technischen Fortschritt auch nicht ändern. Im Gegenteil, der HmbBfDI will diese Entwicklungen weiter konstruktiv begleiten, um zu einer positiv gestalteten Digitalisierung beizutragen, die den technischen Fortschritt für die Hamburger Bürger:innen zugleich leicht zugänglich und sicher nutzbar macht. Damit gehen wir auch den Weg weiter von einer reinen Aufsichtsbehörde zum Kompetenzzentrum für Datenschutz in Hamburg.

EINLEITUNG I.

I. Einleitung

Das Ende der Datensparsamkeit? Wie die Digitalstrategie der EU den Datenschutz verändern wird.

2020 stellte die EU-Kommission ihre Datenstrategie vor, mit der ein europäischer Datenbinnenmarkt geschaffen werden soll, der die EU global wettbewerbsfähiger machen und innovative Produkte und Dienstleistungen ermöglichen will. Zugleich soll der Zugang zu Daten für die Gesellschaft vereinfacht werden. In 2022 sind zahlreiche der damit verbundenen Rechtsakte verabschiedet worden, die teilweise bereits im Laufe dieses Jahres wirksam werden. Dieser neu entstehende Rechtsrahmen der digitalen Wirtschaft spiegelt einen digitalpolitischen Paradigmenwechsel wider, der die Realität großer Datenoligopole sowohl (an)erkennt als auch regulieren will. Außerdem soll für „Big Data"-Anwendungen ein Rechtsraum geschaffen werden, um Anreize zu setzen, Datenverarbeitungen im Gemeinwohlinteresse auszubauen.

Bereits in Kürze wird der Digital Markets Act (DMA) anwendbar, das Gesetz für digitale Märkte, das marktdominierenden großen Plattformen, sogenannten Gatekeepern, wettbewerbsrechtliche Verhaltenspflichten auferlegt.

Der Digital Services Act (DSA), das Gesetz für digitale Dienste, etwas euphorisch als neues digitales Grundgesetz gefeiert, regelt insbesondere den Umgang mit illegalen Inhalten, und gibt vor allem großen Plattformanbietern strenge Transparenz- und Vorsorgepflichten auf. Der DSA ist verabschiedet und gilt ab Anfang 2024.

Beiden Regelwerken ist gemeinsam, dass sie die Existenz sehr großer und sehr marktstarker Unternehmen mit datengetriebenen Geschäftsmodellen, zuvorderst also Firmen wie Alphabet, Meta oder Amazon, im Grunde als gegeben annehmen. Frühere politische

Diskussionen über „Zerschlagungen“ von Quasimonopolen sind damit wohl erst einmal beendet, die übergroße Marktmacht dieser Unternehmen soll nun durch Regulierung eingehegt werden. Zum einen indem die Verantwortung der Unternehmen für die von ihnen vorgehaltenen Inhalte Dritter erhöht wird, zum anderen durch wettbewerbliche Regeln, die die relativen Marktchancen anderer Anbieter verbessern sollen.

Hinzu kommen zwei Gesetze, die sich allgemeiner auf die Nutzung von und den Zugang zu Daten beziehen:

Mit dem Digital Governance Act (DGA) wird den Mitgliedsstaaten eine gesetzliche Grundlage gegeben, Daten, die bereits im öffentlichen Besitz sind, für andere verfügbar zu machen. Er definiert dafür geeignete Modelle wie Datenaltruismus und -spenden und setzt einen Rahmen für Datentreuhänder bzw. Datenvermittler, die diese öffentlichen Daten aggregieren und zur Verfügung stellen sollen. Auf Behörden wird daher die Frage zukommen, welche Daten sie eigentlich besitzen, welchen Wert diese für Dritte haben könnten und wie sie für diese nutzbar gemacht werden können. Das ist für viele Bereiche, wie bspw. Mobilität und Verkehr, ein fraglos sinnvoller Ansatz.

Auf Dauer wahrscheinlich die weitreichendste Änderung dürfte der noch im Entwurfsstadium befindliche Data Act (DA) mit sich bringen, der Unternehmen dazu verpflichtet, bestimmte Daten zu teilen bzw. anderen Zugang zu ihnen zu gewähren. Er bildet die Grundlage für eine EU-weite „data-sharing economy“, vor allem zwischen Unternehmen, etwa Zulieferern und Herstellern, aber auch in Beziehung zum Kunden und teilweise zu den Regierungen. Hier wird dem Umstand, dass die Bedeutung von Daten für alle Wirtschaftsbereiche wächst, auch für die produzierenden, man denke nur beispielhaft an die Automobilbranche, vorausschauend Rechnung getragen. Es entstehen neue Datenmengen, die von vornherein geteilt und zum Nutzen aller zur Verfügung stehen sollen, um neue Datenmonopole möglichst zu verhindern.

Hinzu kommen neue digitale Räume auf EU-Ebene, in denen Daten zu besonderen Sektoren wie bspw. Mobilität und Gesundheit EU-weit verfügbar gemacht werden sollen. Der European Health Data Space (EHDS), ein europäischer Gesundheitsdatenraum, ist hierbei schon am weitesten konturiert. Seine Logik ist einfach: Alle Inhaber von Gesundheitsdaten, also bspw. Krankenhäuser, sind verpflichtet, ihre Daten im europäischen Gesundheitsraum bereit zu stellen. Hier werden sie dann von einer Behörde aggregiert, anonymisiert und zu Forschungszwecken Dritten zur Verfügung gestellt.

Dieses Beispiel zeigt deutlich, was das Ziel ist: Die (sensiblen) personenbezogenen Gesundheitsdaten aller Bürger:innen werden zu (möglichst anonymen) Daten für Forschung und Politik weiterverarbeitet und dienen so dem gesellschaftlichen Fortschritt. Zugleich entsteht ein gemeinnütziger, nicht oder zumindest weniger ökonomisierter Datenraum, der die potentiellen Mehrwerte der Daten nicht großen amerikanischen Plattformen überlässt.

Was bedeutet diese Entwicklung nun für unser Verständnis von Datenschutz?

Fraglos entsteht hier ein unvermeidbares Spannungsverhältnis. Die Grundsätze des Datenschutzes sind u.a., dass die Erhebung und Verarbeitung von Daten einen rechtlichen Grund brauchen und erforderlich zum Erreichen eines benannten Zwecks sein müssen. Die Daten müssen auf für das Erreichen dieser Zwecke notwendige Maß beschränkt sein, die sogenannte Datenminimierung.

Datenminimierung wird oft als Datensparsamkeit ausgelegt oder synonym verwendet. Dies wird nicht mehr zu halten sein. Eine auf Datengewinnung, Datenteilung und Datennutzung orientierte Gesellschaft kann nicht datensparsam sein. Im Gegenteil, sie sucht den Datenreichtum (nicht die Datenverschwendung). Dies wird den Datenschutz vor Herausforderungen stellen.

Denn die grundrechtlichen Verankerungen des individuellen Rechts auf informationelle Selbstbestimmung bleiben unverändert gültig und die Souveränität der Bürger:innen über ihre Daten dürfen nicht in Frage gestellt werden. Was folgt daraus?

1.) Der Gesetzgeber ist gefordert, Datenpolitik wird immer konkreter und wichtiger werden. Die massenhafte Erhebung und Verwendung von Daten, die politisch gewollt ist, wird nicht auf der Basis von Einzel-Einwilligungen funktionieren. Big Data und einwilligungsbasierte Konzepte schließen sich in der Praxis aus bzw. führen zu Scheineinwilligungsmodellen, wie wir sie täglich bei den Cookie-Bannern vor uns sehen.

    Die Rechtsgrundlage dieser (auch) gemeinnützigen Datenerhebungen wird also viel häufiger die gesetzliche Regelung sein. Die Einwilligung als Rechtsgrundlage wird zunehmend an Bedeutung verlieren. In diesen Gesetzen werden die Betroffenenrechte (Widerruf, Transparenz) gesichert werden müssen. Und dies wird die Entwicklung hin zu rechtlich ausgestalteten opt-out-Modellen anstelle von opt-in-Ansätzen erheblich verstärken. Ohne bspw. ein Forschungsdatennutzungsgesetz wird die notwendige Rechtssicherheit für die Beteiligten nicht erreichbar sein.

2.) Transparenz wird noch stärker in den Mittelpunkt des Datenschutzes rücken. Das Wissen der Bürger:innen, welche ihrer Daten gerade wo und von wem genutzt werden, wird zur zentralen Bedingung. Nur wenn ich über die Weiterverarbeitung meiner Daten informiert bin, kann ich Betroffenenrechte wahrnehmen. Nur dann kann es legitim sein, meine Daten zu verarbeiten, ohne mich vorher zu fragen.

3.) Die Datenschutzaufsichtsbehörden werden sich viel intensiver mit Datennutzungs- und Datenzugangskonzepten beschäftigen (müssen). Dies wird den Arbeitsschwerpunkt verlagern von einzelnen Beschwerdeverfahren bei individuellen Rechtsgutverletzungen hin zur Kontrolle von Nutzungsszenarien hinsichtlich

ihrer Gewährleistung der Betroffenenrechte. Es wird die Erwartung erhöhen, Modelle positiv zu bewerten und konstruktiv zu begleiten. Und nicht zuletzt wird in die Abwägung von Interessen im Einzelfall nun auch das öffentliche Interesse in die Verarbeitung dieser Daten stärker einzubeziehen sein.

Somit werden die Datenschutzbehörden zwangsläufig „konstruktiver" im Sinne des Wortes werden. Und eine alte Forderung wird noch dringlicher: Die Datenschützer müssen so früh wie möglich, am besten im Planungsstadium, einbezogen werden, um die datenschutzrechtlichen Garantien von Anfang an mitdenken zu können.

Nur dann wird es gelingen, Daten im Gemeinwohlinteresse zu nutzen und zugleich Betroffenenrechte zu schützen.

PRÜFUNGEN II.

II. Prüfungen bei Sicherheitsbehörden

1. Prüfungen bei Sicherheitsbehörden

Auch in diesem Berichtszeitraum hat der HmbBfDI Prüfungen bei den Sicherheitsbehörden durchgeführt. Dabei handelte es sich jeweils um gesetzlich vorgeschriebene, turnusmäßige Pflichtpflichtprüfungen, aus dem Gesetz über die Datenverarbeitung der Polizei (PolDVG; 1.1) sowie hinsichtlich des Schengener-Informationssystem II (SIS II; 1.2) und der Antiterrordatei/Rechtsextremismus-Datei beim Landesamt für Verfassungsschutz (LfV Hamburg; 1.3).

1.1 Pflichtprüfungen der verdeckten und eingriffsintensiven Maßnahmen nach dem PolDVG

Die seit dem 1. Januar 2022 durch den HmbBfDI im Abstand von zwei Jahren durchzuführenden Pflichtprüfungen von verdeckten und/oder eingriffsintensiven Maßnahmen im Bereich der polizeilichen Gefahrenabwehr verliefen schleppend. Die Prüfungen wurden durch gravierende Mängel bei der Protokollierung der verdeckten Maßnahmen erheblich erschwert. Durch greifende materielle Probleme ergaben sich insgesamt nicht.

Säumnisse der Polizei erschwerten die Prüfungen nicht nur für beide Seiten, sondern ermöglichen im Ergebnis auch keine zweifelsfreie Feststellung der Anzahl der vorgenommenen Maßnahmen durch die Polizei Hamburg. Der fehlende Überblick über die Gesamtzahlen erschwerte daneben teilweise eine sinnvolle Stichprobenziehung für die Prüfung durch den HmbBfDI. Die Nachvollziehbarkeit der Datenverarbeitung durch die Polizei Hamburg in diesem Bereich war für den HmbBfDI schlicht nicht vollumfänglich gewährleistet. Defizite mussten zudem im Bereich der Benachrichtigung der Betroffenen festgestellt werden.

1. Die Prüfpflichten des HmbBfDI

Im Rahmen der Novellierung des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) im Jahr 2019 wurden neue gesetzliche Pflichtprüfungen durch den HmbBfDI in § 73 PolDVG aufgenommen. Danach hat der HmbBfDI die Einhaltung der gesetzlichen Vorschriften über die Verarbeitung von personenbezogenen Daten nach den §§ 20 bis 31 und 50 PolDVG im Abstand von höchstens zwei Jahren bei der Polizei Hamburg zu kontrollieren. Bei §§ 20 bis 31 PolDVG handelt es sich um verdeckte und eingriffsintensive Maßnahmen zur Gefahrenabwehr wie z.B. die Observation und die Telekommunikationsüberwachung.

Gefahrenabwehr umschreibt zunächst die Abwehr sämtlicher Gefahren für die öffentliche Sicherheit und Ordnung. Das Spektrum ist weit und reicht vom Auffinden vermisster Personen bis hin zur Lebensgefahr durch terroristische Aktivitäten. Verdeckt meint, dass der Betroffene im Regelfall von der Durchführung der Maßnahmen – anders als zum Beispiel bei einer Identitätskontrolle – zunächst nichts mitbekommt. Eingriffsintensiv sind die Maßnahmen, da sie geeignet sind, weit in geschützte Lebensbereiche der Personen einzudringen.

Diese nun vom Gesetzgeber vorgeschriebenen turnusmäßigen Pflichtprüfungen dienen der Umsetzung der Anforderungen aus der Rechtsprechung des Bundesverfassungsgerichts. Das höchste deutsche Gericht hat neben der grundsätzlichen Bedeutung der Gewährleistung einer wirksamen aufsichtlichen Kontrolle auch die Signifikanz einer hinreichenden gesetzlichen Vorgabe zu turnusmäßigen Pflichtkontrollen der Aufsichtsbehörden im Rahmen von heimlichen Überwachungsmaßnahmen betont (BVerfG, Urt. v. 20. April 2016 – 1 BvR 966/09 u.a., Rn. 141, 266).

Aufgrund der seit dem 24. Dezember 2019 geltenden Übergangsbestimmung in § 78 Abs. 3 PolDVG hat der HmbBfDI zum 1. Januar 2022 erstmals mit der Prüfung der Maßnahmen begonnen.

2. Fehlende Protokollierung der Maßnahmen durch die Polizei Hamburg

Als Hilfsmittel für die Prüfung durch den HmbBfDI sieht § 64 PolDVG vor, dass durch die Polizei Hamburg eine Protokollierung der zu prüfenden Maßnahmen nach §§ 20 bis 31 und 50 PolDVG vorzunehmen ist. Hiernach wären für jede Maßnahme zumindest die eingesetzten Mittel, der Zeitpunkt, Angaben zu erhobenen Daten und die Daten erhebende Organisationseinheit innerhalb der Polizei zu verzeichnen gewesen.

Bedauerlicherweise teilte die Polizei Hamburg dem HmbBfDI mit, dass bisher keine separate Protokollierung der Maßnahmen nach den Vorgaben von § 64 PolDVG erfolge. Allerdings seien die oben genannten Pflichtangaben zu den Maßnahmen dem Vorgangsbearbeitungssystem ComVor und ggf. auch dem jeweiligen Fallbearbeitungssystem oder dem Aktenrückhalt selbst „weitestgehend" zu entnehmen. Aufgrund der ab dem 1. Januar 2022 ebenfalls bestehenden Mitteilungspflicht hinsichtlich der hier durch den HmbBfDI zu prüfenden Maßnahmen an die Hamburgische Bürgerschaft nach § 75 PolDVG könnte jedenfalls ab diesem Zeitpunkt mitgeteilt werden, wie viele Maßnahmen zur Meldung an die Bürgerschaft registriert worden seien.

Der von der Polizei Hamburg geschilderte Ist-Zustand entspricht nicht den gesetzlichen Vorgaben nach § 64 PolDVG. Dies hat der HmbBfDI der Polizei Hamburg in einem Schreiben auch ausführlich dargelegt: Zur Erfüllung der gesetzlichen Pflicht genügt es nicht, dass die Informationen an beliebiger Stelle vorhanden sind. Vielmehr ist eine zentrale und vollständige Aufstellung der Einzelmaßnahmen mit den in § 64 PolDVG aufgeführten Angaben notwendig.

Diese Rechtsansicht des HmbBfDI beruht auf folgenden Überlegungen: Mit dieser Protokollierungsverpflichtung im PolDVG beabsichtigte der Hamburgische Gesetzgeber nach eigenen Angaben die Erfüllung der Anforderung aus dem vorbezeichneten Urteil des Bundesverfassungsgerichts (Bü-Drs. 21/17906, S. 76). Das Gericht

hatte in der Entscheidung betont, dass sichergestellt werden müsse, dass die Daten den Aufsichtsbehörden in praktikabel auswertbarer Weise zur Verfügung stehen. Die Aufstellung eines Verzeichnisses in der von § 64 PolDVG vorgegebenen Form hat dabei also gerade zusätzlich zur Speicherung der Daten z.B. im Vorgangsverwaltungssystem (ComVor) oder im Fallbearbeitungssystem zu erfolgen. Einer Pflicht zur Protokollierung wird nicht schon durch Erfüllung der allgemeinen Pflicht zur Aktenführung genüge getan. Dies folgt letztlich auch aus der gesetzlich normierten Zweckbindung: Die in § 64 PolDVG normierte Protokollierung darf nämlich nur für die Benachrichtigung der Betroffenen oder zur Prüfung der Rechtmäßigkeit der Maßnahmen verwendet werden. Die Protokolle sind nach § 64 Abs. 4 PolDVG bis zur Prüfung des HmbBfDI nach § 73 PolDVG zu speichern und nach Abschluss der Prüfung automatisch zu löschen. Eine Löschung der zur ordnungsgemäßen Aktenführung gespeicherten Inhalte an anderer Stelle kommt jedoch selbstverständlich nicht schon aufgrund des Abschlusses der Kontrolle durch den HmbBfDI in Betracht.

Soweit seitens der Polizei Hamburg abgestellt wird, dass jedenfalls seit dem 1. Januar 2022 die Informationen weitestgehend vorhanden seien, genügt dies nach Ansicht des HmbBfDI auch in zeitlicher Hinsicht nicht. Es besteht die Verpflichtung zur Protokollierung seit Inkrafttreten des PolDVG im Dezember 2019 und nicht erst ab dem 1. Januar 2022. Für Maßnahmen der Telekommunikationsüberwachung (§ 23 PolDVG n.F.) bestand zudem bereits in § 10c Abs. 3 PolDVG a.F. weit vor dem Jahr 2019 eine Protokollierungspflicht, die in § 64 PolDVG lediglich aufging (so auch der Hamburgische Gesetzgeber, vgl. Bü-Drs. 21/17906, S. 76).

Im Hinblick auf die Frage, wie bei den verdeckten und eingriffsintensiven Maßnahmen die Protokollierung der Informationen nach § 64 PolDVG in Zukunft konkret durchzuführen ist, wurde der HmbBfDI gegenüber der Polizei im Weiteren auch beratend tätig. Dabei sind sowohl Zweck der Norm als auch die Rechtsprechung des BVerfG zu beachten. Dadurch kommt man zwangsläufig zu dem Ergebnis, dass

derartige Aufstellungen – um eine „effektive aufsichtliche Kontrolle“ bei verdeckten Maßnahmen (BVerfG, Urteil v. 20. April 2016 – 1 BvR 966/09, Rn. 141) zu gewährleisten – soweit wie möglich keine Zweifel an der Vollständigkeit und Richtigkeit der den Aufsichtsbehörden zur Verfügung gestellten Daten zulassen dürfen. Um die erforderliche Vollständigkeit und Integrität der Daten sicherzustellen, wäre es daher erforderlich, dass z.B. bei Erstellung eines solchen Vorgangs in ComVor oder in einem Fallbearbeitungssystem diese Systeme automatisch erkennen, dass es sich dabei um eine Maßnahme nach §§ 20 bis 31 und 50 PolDVG handelt. Das System müsste dann selbstständig die nach § 64 PolDVG erforderlichen Daten zentral zusammentragen und eine manuelle Steuerung, Sperrung, Löschung oder Verhinderung müsste ausgeschlossen sein.

Soweit die existierenden Systeme der Polizei derartige technische Erweiterungen zum gegenwärtigen Zeitpunkt nicht zulassen, befindet sich der HmbBfDI im Austausch mit der Polizei Hamburg, wie eine Situation herzustellen sein könnte, die – trotz anhaltender Rechtswidrigkeit – den gesetzgeberischen Zielen so weit wie möglich Rechnung trägt. Dies ändert nichts daran, dass die Polizei Hamburg parallel darauf hinzuwirken hat, dass z.B. im Rahmen der Implementierung des Polizeireformprojektes „P20“ für derartige technische Vorkehrungen in Zukunft gesorgt wird, um wenigstens mittelfristig einen rechtmäßigen Zustand herzustellen.

Zwischenzeitlich hat die Polizei Hamburg dem HmbBfDI Informationen über eine geplante Übergangslösung zur Gewährleistung der Erfassung der Protokollinformationen zukommen lassen. Wird die Anordnung einer Maßnahme beantragt, ist ein weiteres Formular mit den Protokollierungsinformationen auszufüllen und auszudrucken. Diese werden gesammelt und bei Bedarf an den Leitungsstab zur Kontrolle durch den HmbBfDI übermittelt. Dem Formular liegt ein Glossar mit Definitionen und Erläuterungen bei, um ein richtiges Ausfüllen durch die jeweiligen Sachbearbeitenden zu gewährleisten. Eine Beurteilung durch den HmbBfDI steht noch aus.

3. Überprüfung der einzelnen Maßnahmen

Parallel zur Klärung der Fragen zur Protokollierung begann der HmbBfDI mit der Prüfung der einzelnen Maßnahmen. Geplant war eine Stichprobenkontrolle von Maßnahmen im Zeitraum seit Inkrafttreten des novellierten PolDVG (24. Dezember 2019) bis zum 30. Juni 2022.

Für den Zeitraum 1. Januar 2022 bis 30. Juni 2022 wurde zunächst der Schwerpunkt auf die Kontrolle von vielfach durchgeführten Maßnahmen mit für sich genommen eher geringer Eingriffsintensität und Anordnungsbefugnis durch den Polizeipräsidenten gelegt, was zu einer Prüfung von insgesamt über 300 Maßnahmen führte.

Für die seit dem 1. Januar 2022 vorgenommenen Maßnahmen hat der HmbBfDI eine Aufstellung mit den Informationen nach § 64 PolDVG angefordert sowie die für die Maßnahmen nach §§ 20 bis 28 PolDVG vorliegenden Anordnungen. Zudem wurde Auskunft verlangt, inwieweit Betroffene nach Abschluss der Maßnahme benachrichtigt wurden. Hinsichtlich der Maßnahmen aus dem Jahr 2022 ergaben sich Unstimmigkeiten, die erneuter Nachfragen und Erläuterungen bedurften. Die fehlenden Protokolle prägten auch hier den weiteren Prüfungsablauf:

Beispielhaft sei dies an den zu prüfenden Maßnahmen nach § 27 PolDVG dargestellt. Diese betreffen die sog. Bestandsdatenauskunft. Im Normalfall wird bei der Bestandsdatenauskunft anhand einer bekannten Telefonnummer der Inhaber des Anschlusses beim Telefonanbieter abgefragt und zu diesem weitere Daten (insb. die Wohnanschrift) an die Polizei übermittelt. Dem HmbBfDI konnten durch die Polizei Hamburg kaum belastbare Zahlen zur Menge der durchgeführten Maßnahmen der Bestandsdatenauskunft im ersten Halbjahr 2022 vorgelegt werden. Dies hätte nach Angaben der Polizei vielmehr die „händische Auswertung aller Handakten“ mit einem „enormen Zeitaufwand“ erfordert. Ohne einen Überblick über die Zahl und die Auffindbarkeit aller durchgeführten Maßnahmen war eine Stichprobenziehung zur Kontrolle durch den HmbBfDI nur eingeschränkt möglich. Zumindest sämtliche Bestandsdatenauskünfte,

die im Zusammenhang mit eingehenden Notrufen durch die Polizei Hamburg durchgeführt worden sind, lagen dem HmbBfDI in überprüfbarer Form vor. Diese waren wohl gesammelt bei der Polizei Hamburg auffindbar. Zu Bestandsdatenabfragen aus anderen Anlässen waren Fallzahlen nicht zu ermitteln.

Für das Jahr 2021 wurden zur Prüfung vorrangig Maßnahmen mit hoher Eingriffsintensität ausgewählt. Dem HmbBfDI wurden 43 Anordnungen vorgelegt, die überwiegend von Gerichten erlassen worden waren. Diese waren wohl aufgrund der außerpolizeilichen Anordnung leichter auffindbar als andere Vorgänge.

Für das Jahr 2020 stellte sich die Ermittlung der Fallzahlen ebenfalls problematisch dar. Letztendlich gelang es der Polizei Hamburg aber über Umwege, eine Liste aller Fälle zu generieren, in denen ein bestimmtes Antragsformular verwendet wurde, dessen Verwendung auf die Durchführung heimlicher oder eingriffsintensiver Maßnahmen hindeutete. Ohne vorherige, genauere Filtermöglichkeiten wurde hieraus durch den HmbBfDI eine Stichprobe von ca. 10% der verzeichneten Maßnahmen ausgewählt, die einen Querschnitt aller zu prüfenden Maßnahmen abbilden sollten.

Stichprobenartig und aufgrund von Unklarheiten in einzelnen Anordnungen ließ sich der HmbBfDI auch den Aktenrückhalt zu den zu prüfenden Maßnahmen vollständig oder teilweise zeigen. Vereinzelt war eine Übersendung auch aus Geheimhaltungsgründen nicht möglich, sodass dies zum Anlass genommen wurde, den Aktenrückhalt nebst Anordnung vor Ort bei der Polizei Hamburg einzusehen. Durchgreifende Zweifel an der grundsätzlichen Rechtmäßigkeit der kontrollierten Verfahren drängen sich in der Prüfung nicht auf.

Letztendlich kaum überprüfbar war für den HmbBfDI die Frage der mehrfachen Anwendung verschiedener Maßnahmen gegenüber einem Betroffenen. Dafür wäre ein listenmäßiges Verzeichnis notwendig gewesen. Teils konnte bei Sichtung des Aktenrückhalts durchaus eine erhebliche Mehrfachbelastung einzelner Betroffener durch

parallele oder sich wiederholende Anwendung der geprüften Maßnahmen festgestellt werden. In Einzelfällen traten daneben auch noch Überwachungsmaßnahmen aus dem Strafverfolgungsbereich. In den bei der Einsicht in die Akten festgestellten Fällen bestanden hinsichtlich der Rechtmäßigkeit auch umfassender Überwachungen jedoch im Verhältnis zur Gefährlichkeit der Personen keine Bedenken.

4. Fehlende Kennzeichnung der Daten aus heimlichen Maßnahmen

Die Anlieferung der erbetenen Informationen erfolgte insgesamt schleppend. Dies kann daher resultieren, dass die Polizei nicht nur keine Protokollierung nach § 64 PolDVG vornimmt, sondern der HmbBfDI auch nach dem derzeitigen Kenntnisstand davon ausgehen muss, dass die Polizei Hamburg ihrer gesetzlich normierten Verpflichtung zur Kennzeichnung der bei verdeckten und eingriffsintensiven Maßnahmen erhobenen Daten gem. § 65 Abs. 1 Satz 1 PolDVG wohl ebenfalls nicht nachkommt.

Vorrangig dient die gesetzlich normierte Verpflichtung zur Kennzeichnung dem gesetzgeberischen Willen nach der Einhaltung der Zweckbindung. Daten sollen auch später nur zu dem Zweck verarbeitet werden dürfen, zu dem diese ursprünglich erhoben worden sind. Ein Wechsel des Zwecks unterliegt engen Einschränkungen und ist rechtfertigungsbedürftig. Die Einhaltung dieser Kennzeichnungspflicht hätte vorliegend praktisch aber über diesen eigentlichen Zweck hinaus auch die aufsichtsbehördliche Prüfung erleichtern können. Wären Daten, die aus heimlichen und eingriffsintensiven Maßnahmen stammen, ordnungsgemäß gekennzeichnet, wären diese aus technischer Perspektive für die Kontrolle vermutlich auch leichter aufzufinden gewesen. Zudem könnte technisch an eine solche Kennzeichnung angeknüpft werden, um eine Protokollierung der Vorgänge zu ermöglichen.

Nach Auskunft der Polizei ist frühestens im Jahr 2025 mit der Erfüllung der Kennzeichnungspflicht zu rechnen. Anders als für die Protokollierung existiert mit § 78 Abs. 1 PolDVG allerdings eine Übergangsregelung für die Kennzeichnung. Diese erlaubt der

Polizei Hamburg auf unbestimmte Zeit, Übermittlungen auch dann vorzunehmen, wenn die Daten nicht ordnungsgemäß gekennzeichnet worden sind. Der Verzicht auf die Kennzeichnung bleibt insoweit zunächst folgenlos.

5. Mängel bei der Benachrichtigung der Betroffenen

Im Rahmen der Kontrolle der Benachrichtigungen der von den Maßnahmen Betroffenen nach § 26 Abs. 4 bzw. § 28 Abs. 2 bzw. § 29 Abs. 4 PolDVG i.V.m. § 68 PolDVG wurden erhebliche Mängel festgestellt. Da es in der Natur von heimlichen Maßnahmen liegt, dass die Betroffenen hiervon zunächst nichts mitbekommen sollen, sind diese im Anschluss in den vorgenannten Fällen zu benachrichtigen. In einigen Fällen kann hierauf (vorerst) verzichtet werden, insbesondere wenn weitere Ermittlungen gefährdet werden. Sofern aber eine solche Pflicht zur Benachrichtigung besteht, sieht § 68 Abs. 1 PolDVG für diese Benachrichtigung auch bestimmte Mindestinhalte vor.

Insbesondere ist darauf Wert zu legen, dass die Benachrichtigung schriftlich und unter Angabe eines Rechtsbehelfs erfolgt. In mehreren Fällen erfolgte die Benachrichtigung durch die Polizei Hamburg jedoch nur telefonisch. So ist kaum sicherzustellen und vor allem für eine spätere Prüfung durch den HmbBfDI nicht dokumentiert, dass die Benachrichtigung den Mindestanforderungen genügte.

In den Fällen, in denen die Benachrichtigung schriftlich erfolgte, wurde durch die Polizei Hamburg bisher ein standardisiertes Formular verwendet. Dies hat sich der HmbBfDI zur Prüfung übersenden lassen. Aus diesem Anlass stellte die Polizei Hamburg selbst noch vor Übersendung fest, dass das Formular den gesetzlichen Anforderungen an die Benachrichtigung aus § 68 PolDVG nicht genügte. Der HmbBfDI teilt diese Auffassung nach Ansicht des Formulars. Das Formular enthält über die Information über die Durchführung der Maßnahme hinaus kaum relevante Informationen. Vor allem fehlen die nach § 68 PolDVG vorgeschriebenen Mindestinformationen nahezu vollständig. Insbesondere fehlt es an einem Hinweis auf das Beschwerderecht zum HmbBfDI, vgl. § 68 Abs. 1 Nr. 1 Buch-

stabe d) PolDVG und auf dessen Erreichbarkeit gemäß Buchstabe e). Der hohen Bedeutung unabhängiger Aufsicht und nachträglicher Kontrolle von Maßnahmen im heimlichen Eingriffsbereich wird dies nicht gerecht. Zudem fehlt es an einem Hinweis auf die Betroffenenrechte (§ 68 Abs. 1 Nr. 1 Buchstabe b) PolDVG). Der Zweck der Maßnahme wurde ebenfalls nur grob umschrieben (§ 68 Abs. 1 Nr. 1 Buchstabe a) PolDVG): „zum Zweck der Gefahrenabwehr".

Dem HmbBfDI wurde durch die Polizei Hamburg die Überarbeitung und Anpassung an § 68 PolDVG in Aussicht gestellt, zum Redaktionsschluss lag das überarbeitete Formular allerdings noch nicht vor.

6. Fazit

Die auch vom Bundesverfassungsgericht hervorgehobene Bedeutung von turnusmäßigen Pflichtkontrollen der datenschutzrechtlichen Aufsicht findet sich nicht nur in nationalen Gesetzen, sondern zunehmend auch in europäischen Verordnungen und Beschlüssen wieder. Mit einem weiteren Anstieg dieser gesetzlich verankerten Pflichtprüfungen ist zu rechnen. Die gesetzgeberischen Entscheidungen sind im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts zu begrüßen. Ob der HmbBfDI diesen stets zunehmenden Verpflichtungen aber in Zukunft zeitlich und umfänglich gerecht werden kann, hängt neben der den wachsenden Verpflichtungen anzupassenden personellen Ausstattung der Aufsichtsbehörde auch davon ab, ob die Sicherheitsbehörden als verantwortliche Stellen ihrerseits ihren gesetzlichen Anforderungen wie z.B. Protokollierung und Kennzeichnung nachkommen. Nur dann wird die datenschutzrechtliche Kontrolle in dem Umfang ermöglicht, wie gesetzlich vorgesehen und ist auch praktisch für die Aufsichtsbehörden handhabbar. Versäumnisse in der Etablierung derartiger Prozesse dürften auf beiden Seiten – wie in dieser Prüfung leider geschehen – zu nicht unerheblichen Verzögerungen und (unnötigem) Arbeitsaufwand führen.

1.2 Prüfungen von SIS-II (Art. 36 Beschluss Prüfungen)

Mit der im Berichtszeitraum durchgeführten Kontrolle der Ausschreibun gen nach Art. 36 SIS II-Beschluss beim Landeskriminalamt Hamburg ist der HmbBfDI seinen gesetzlich vorgeschriebenen Kontrollpflichten nach Art. 60 Abs. 2 SIS II-Beschluss nachgekommen. Der HmbBfDI hat sich hierzu einer europaweiten, koordinierten Prüfung der datenschutzrechtlichen Auf sichtsbehörden in diesem Bereich angeschlossen. Bei der Polizei Hamburg konnten im Ergebnis keine gravierenden Mängel festgestellt werden. Der Polizei Hamburg sind jedoch einige formelle Verbesserungen an die Hand zu geben.

Art. 36 SIS II-Beschluss sieht die schengenweite Ausschreibung von Personen oder Sachen zur verdeckten oder gezielten Kontrolle vor. Die Ausschreibung kann zu Zwecken der Gefahrenabwehr oder der Strafverfolgung erfolgen. Für den Bereich der Gefahrenabwehr findet sich die mitgliedsstaatliche, landesrechtliche Umsetzung in § 31 PolDVG. Diese Maßnahmen fallen zugleich auch in den Bereich der Kontrollen nach § 73 PolDVG, über die im vorherigen Abschnitt berichtet wurde (II 1.1). Für den Bereich der Strafverfolgung ist § 163e StPO die Rechtsgrundlage der Ausschreibungen.

Es erfolgt auf Grundlage der o.g. Normen zunächst ein Eintrag der Person in das Schengener Informationssystem (SIS). Dieses wird von den Grenzschutz- und Zollbehörden sowie den Visums- und Polizeibehörden im gesamten Schengen-Raum genutzt. Eine gezielte Fahndung nach der ausgeschriebenen Person ist mit dem Eintrag in das SIS allerdings nicht verbunden: Sofern die ausgeschriebene Person durch eine oben genannte Behörde (zufällig) kontrolliert und in dem Fall, dass bestimmte Voraussetzungen dafür erfüllt sind, im Schengener Informationssystem abgefragt wird, erlangt die kontrollierende Behörde Kenntnis von der Ausschreibung. Die kontrollierende Behörde informiert die ausschreibende Behörde. In der Regel ist der

Person die Ausschreibung bei einer solchen Kontrolle nicht bekannt zu geben (sog. verdeckte Kontrolle). So werden vom Zeitpunkt der Ausschreibung an alle über die eingetragene Person gewonnenen Erkenntnisse bei der ausschreibenden Stelle gebündelt ausgewertet. Hieraus lassen sich bspw. Rückschlüsse auf Aufenthaltsorte und Reiserouten einer Person ziehen.

Das Bundeskriminalamt (BKA) ist Zentralstelle für den Betrieb des nationalen Teils des SIS (§ 3 Abs. 2 BKAG). Die Verantwortung für die Übermittlung der Daten und die Aktualität der Daten an das BKA trägt aber die ausschreibende Stelle. Nach Art. 60 Abs. 2 SIS II-Beschluss bzw. Art. 44 Abs. 2 VO 1987/2006/EG (Migration) sind die Datenverarbeitungsvorgänge der Mitgliedsstaaten grundsätzlich alle vier Jahre zu überprüfen. Praktisch soll die Prüfung – wie hier geschehen – koordiniert in europäischer Zusammenarbeit erfolgen (Art. 62 Abs. 2 SIS II Beschluss). In Hamburg ist der HmbBfDI die zuständige Kontrollinstanz.

Für die Prüfung wurden zunächst die aktiven Ausschreibungen im Bereich der Gefahrenabwehr ermittelt. Zwischen den Aufsichtsbehörden der Mitgliedsstaaten wurde hierfür ein Stichtag abgestimmt (29. Oktober 2021). Für den Bereich der Strafverfolgung war die Zahl der Ausschreibungen an diesem Tag rückwirkend nicht zu ermitteln. Für den Bereich der Gefahrenabwehr ließ sich der HmbBfDI sämtliche Anordnungen zur Ausschreibung des genannten Stichtages übersenden. Im Bereich der Strafverfolgung wurden stattdessen die tagesaktuellen Ausschreibungen des 23. September 2022 gewählt. Die Anordnungen wurden anhand einer Checkliste auf ihre formelle Vollständigkeit und sodann auf ihre inhaltliche Nachvollziehbarkeit hin überprüft. Bei Auffälligkeiten wurde zudem in einigen Fällen der Aktenrückhalt vor Ort gesichtet.

Voraussetzung für die Ausschreibung ist entweder das Vorliegen tatsächlicher Anhaltspunkte dafür, dass eine Person eine schwere Straftat plant oder begeht (Art. 36 Abs. 2 Buchstabe a) SIS II Beschluss, § 31 Abs. 1 Nr. 2 PolDVG) oder eine Gesamtbeurteilung

der Person insbesondere auf Basis bisheriger Straftaten, aufgrund derer zu erwarten ist, dass künftig schwere Straftaten begangen werden (Art. 36 Abs. 2 Buchstabe b) SIS II Beschluss; § 31 Abs. 1 Nr. 1 PolDVG). Die Anordnung hat in den Fällen des § 31 PolDVG durch den Polizeipräsidenten oder Vertreter im Amt zu erfolgen. Im Falle des § 163e StPO ist grundsätzlich eine richterliche Anordnung notwendig. Bei Gefahr im Verzug kann nach § 163e Abs. 4 Satz 2 StPO die Anordnung im Einzelfall durch die Staatsanwaltschaft erfolgen. Die Anordnung ist zu befristen und es müssen sich aus der Anordnung Art, Beginn und Ende der Maßnahme, die Tatsachen, die den Einsatz begründen sowie Zeitpunkt und Name und Dienststellung des Anordnenden ergeben (§ 31 Abs. 3 Satz 1 und 2 i.V.m. § 21 Abs. 2 Satz 4 Nrn. 1-3 Abs. 4 PolDVG).

In vielen Teilbereichen der Prüfung traten keine Auffälligkeiten auf: Für jede Ausschreibung lag eine (Verlängerungs-)Anordnung vor, die von einer autorisierten Person stammt. Auch wurde die zeitliche Begrenzung der Anordnung auf ein Jahr in allen Fällen eingehalten. Vielfach waren die Anordnungen sogar auf sechs Monate beschränkt. In keinem Fall wurden – anders als in anderen Bundesländern – reine Kontaktpersonen eines Störers ausgeschrieben.

In anderen Bereichen ließen sich die auch in anderen Bundesländern festgestellten Mängel aber ebenso bei der Polizei Hamburg feststellen. So ließen einige Anordnungen den Namen des Anordnenden nicht erkennen. Dies betraf insbesondere die Fälle, in denen Vertreter des Polizeipräsidenten die Anordnung unterschrieben. Deren Identität ist ohne Namensangabe nicht ohne weitere Nachforschungen aufklärbar.

Weiterhin wurde in einer Vielzahl von Fällen keine an den individuellen Einzelfall angepasste Verhältnismäßigkeitsprüfung in der Anordnung dokumentiert. Der Eingriff in die Rechte des Einzelnen durch die Ausschreibung ist zu den erhofften Ergebnissen in eine Relation zu setzen. Vereinzelt fehlt es zudem an einer ausdrücklichen Begründung der Schengen-Relevanz der Ausschreibung (Art.

21 SIS II-Beschluss) in der Anordnung. Hier ist darzulegen, warum eine Ausschreibung gerade für den gesamten Schengen-Raum für erforderlich gehalten wird. Ansonsten käme auch eine lediglich nationale Ausschreibung als milderes Mittel in Frage. Nach der Sichtung des Aktenrückhalts konnten anfängliche Zweifel an der Schengen-Relevanz und der Verhältnismäßigkeit jedoch in sämtlichen Fällen ausgeräumt werden.

Der HmbBfDI wird der Polizei Hamburg Empfehlungen im Hinblick auf die Erfüllung der formalen Anforderungen der Anordnungen vorlegen. Die bisher hauptsächlich polizeiintern relevanten Ausschreibungen erhalten durch die Kontrollpflichten des HmbBfDI einen neuen Charakter: Dem polizeilichen Bearbeiter eines Vorgangs ist die gesamte Akte regelmäßig bekannt. Die Anordnungen sind oft dementsprechend knapp gehalten. Der Aufsichtsbehörde fehlt hingegen bei der Prüfung naturgemäß dieses Hintergrundwissen über den konkreten Vorgang. Dieses kann sich aufgrund der Vielzahl der Fälle auch nicht ohne Weiteres angeeignet werden.

Die formell ordnungsgemäße Anordnung dient heute nicht nur internen Dokumentationszwecken, sondern vereinfacht auch die aufsichtsrechtliche Prüfung und Stichprobenauswahl. Formell gut nachvollziehbare Anordnungen erleichtern die zukünftige Kontrolle für beide Seiten: Beantwortet bereits die Anordnung alle Tatsachen- und Rechtsfragen der Aufsichtsbehörde, ist die Einsichtnahme in den kompletten Vorgang seltener nötig. Die Aufsichtsbehörde kann sich so auf die grundrechtlich kritischen Fälle statt auf Formalia fokussieren, die Polizei Hamburg Ressourcen bei der erneuten Aufarbeitung des Vorgangs für die Aufsichtsbehörde sparen.

1.3 Prüfung der ATD/RED beim Landesamt für Verfassungsschutz Hamburg

Der HmbBfDI hat im Berichtszeitraum auch seine turnusmäßigen Pflichtprüfungen der Antiterrordatei (ATD) sowie der Rechtsextremismus-Datei (RED) beim Landesamt für Verfassungsschutz Hamburg (LfV HH) wiederholt. Nachfragen zu formellen Auffälligkeiten in den Protokollen konnten schnell und umfassend aufgeklärt werden.

Sowohl bei der ATD als auch der RED handelt es sich um gemeinsame, standardisierte und zentrale Dateien, die jeweils von verschiedenen Sicherheitsbehörden des Bundes sowie der Landeskriminalämter und der Verfassungsschutzbehörden der Länder beim BKA geführt werden.

Die ATD dient dem Zweck der Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland (§ 1 Abs. 1 Antiterrordateigesetz (ATDG)). Die RED wurde zum Zweck der Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus geschaffen (§ 1 Abs. 1 Rechtsextremismus-Datei-Gesetz (RED-G)). Mit diesen Dateien sollten Erkenntnisse von Polizeibehörden und Nachrichtendiensten aus den genannten Bereichen vernetzt und die Informationen für die beteiligten Behörden gegenseitig auffindbar gemacht werden. Sowohl die Polizei Hamburg als auch das LfV Hamburg sind verpflichtet, von ihnen erhobene personenbezogene Daten nach den Vorgaben des jeweiligen Gesetzes in den Dateien zu speichern (vgl. § 2 ATDG bzw. RED-G). Die datenschutzrechtliche Verantwortung für die in der Datei gespeicherten Daten, trägt die Behörde, die die Daten eingegeben hat (vgl. § 9 Abs. 1 Satz 1 RED-G bzw. § 8 Abs. 1 Satz 1 ATDG): Die eintragende Behörde verantwortet die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten.

Der HmbBfDI hat sich in diesem Turnus insbesondere auf die Kontrolle der Protokolldaten, konzentriert. Protokolldaten sind nach § 9 Abs. 1 ATDG und § 10 Abs. 1 RED-G für jeden Zugriff auf die Dateien für die Datenschutzkontrolle zu erstellen. Auf dem Protokollserver des BKA werden dazu sog. Reports zur Ausweisung bestimmter Auswertungskriterien programmiert, wie beispielsweise neu angelegte Objekte oder geänderte Objekte. Daher hat der HmbBfDI bezogen auf das LfV Hamburg als beteiligte Behörde nach § 1 Abs. 1 ATD bzw. § 1 Abs. 1 ATD/RED Protokolldaten für neu angelegte Objekte, gelöschte Objekte und angesehene Objekte für den Zeitraum 15. August 2020 bis 28. Juli 2022 angefordert.

Zunächst bei der Auswertung der Protokolldaten erkannte Auffälligkeiten konnten im Nachgang mit dem LfV Hamburg geklärt bzw. vom LfV Hamburg schlüssig und nachvollziehbar beantwortet werden. Aufgrund des hohen Geheimhaltungsgrades der Protokolldaten (VS-Geheim) sind detaillierte Ausführungen über den Inhalt der Protokolldaten und den Verlauf der Prüfung in diesem Tätigkeitsbericht nicht möglich.

Der HmbBfDI verweist zudem erneut auf die bereits im Rahmen der letzten Prüfung getroffene Feststellung, dass andere Kommunikationswege und -formen in der Praxis deutlich mehr Relevanz bei der Arbeit der Sicherheitsbehörden aufweisen dürften als die ATD- und RED-Dateien (vgl. 29. TB, III 1.1, sowie BfDI 28. TB, S. 52 ff.).

Aufgrund der gesetzlichen Vorgaben müssen aber genau diese Dateien mindestens alle zwei Jahre durch die Datenschutzaufsicht überprüft werden. Bei der nunmehr durchgeführten Prüfung handelt es sich um die jeweils dritte Prüfung der ATD und RED beim LfV Hamburg durch den HmbBfDI.

2. Prüfung der Datenübermittlung zwischen Staatsanwaltschaft und den Ausländerbehörden

Der HmbBfDI wurde von der Staatsanwaltschaft Hamburg im Berichtszeitraum in Kenntnis gesetzt, dass sowohl bei der gesetzlich vorgeschriebenen Übermittlung der Einleitung von strafrechtlichen Ermittlungsverfahren als auch bei der Mitteilung von Einstellungen an die Ausländerbehörden zu circa 80.000 Fehlübermittlungen und Unterlassungen aufgrund von Fehlern in der Programmierung gekommen sei. Erste Maßnahmen zur Mängelbeseitigung hat die Staatsanwaltschaft unmittelbar nach Bekanntwerden getroffen, der HmbBfDI steht jedoch weiterhin im Austausch mit der Staatsanwaltschaft mit dem Ziel der Behebung technisch- organisatorischer Mängel und Optimierung der Prozesse.

Nach § 87 Abs. 4 Aufenthaltsgesetz (AufenthG) haben die für die Einleitung und Durchführung eines Strafverfahrens zuständigen Stellen die zuständigen Ausländerbehörden unverzüglich über die Einleitung eines Strafverfahrens bei der Staatsanwaltschaft zu unterrichten. Nach § 87 Abs. 4 Var. 2. AufenthG ist zudem durch die Staatsanwaltschaft über die Erledigung des Verfahrens zu unterrichten (vgl. 42 der Anordnung über Mitteilungen im Strafverfahren (MiStra)).

Dem HmbBfDI wurden im August 2022 im Rahmen einer sog. Data-Breach-Meldung nach § 65 Bundesdatenschutzgesetz bekannt, dass es im Rahmen dieser Verpflichtungen über einen längeren Zeitraum zu einem Fehlverhalten gekommen ist. So wurde festgestellt, dass auch bei deutschen Staatsangehörigen teilweise eine Mitteilung der Einleitung eines Ermittlungsverfahrens an die Ausländerbehörde erfolgt sei. Dies betrifft insbesondere Personen, die neben der deutschen noch mindestens eine weitere ausländische Staatsangehörigkeit haben. Das System habe nur die ausländische Staatsangehörigkeit erkannt und den Mitteilungsvorgang sodann

automatisch in Gang gesetzt. In diesem Zusammenhang wurde mitgeteilt, dass seit dem 01. Januar 2018 in einer Vielzahl von Fällen Mitteilungen der Staatsanwaltschaft im Hinblick auf Erledigungen an die Ausländerbehörde nicht erfolgt sind.

Die Staatsanwaltschaft Hamburg nutzt zur Vorgangsbearbeitung einen in 7 Bundesländern genutzten Standard, das sog. technische Unterstützungssystem für Mehrländer-Staatsanwaltschafts-Automation (MESTA). Hieraus werden in Hamburg in festen Intervallen Exporte der aktuellen mitteilungspflichtigen Vorgänge angefertigt, die erforderlich sind, um die genannten gesetzlichen Voraussetzungen zu erfüllen. Dabei gibt es in MESTA selbst keine Schnittstelle für die Anbindung des Programms an die Ausländerbehörden. Die IT-Abteilung der Staatsanwaltschaft Hamburg hat vielmehr ein entsprechendes Tool entwickelt, mit dem eine erste und mit der späteren Erledigung des Verfahrens durch Einstellung bei der Staatsanwaltschaft eine abschließende Mitteilung an die Ausländerbehörde generiert wird. Das Tool wird auf FHH Basis-Rechnern betrieben. Die zur Verfügung stehende Softwareauswahl auf diesen Basis-Rechnern erscheint für derartige Automatisierungsaufgaben weniger geeignet als dafür dedizierte Umgebungen und Anwendungen und ist laut Aussage der Staatsanwaltschaft dem Umstand geschuldet, dass bisher sowohl personelle als auch finanzielle Mittel fehlten.

Die Staatsanwaltschaft teilte dem HmbBfDI mit, dass mit Wirkung zum 01. Januar 2018 die MESTA-Erledigungskennziffern für Einstellungen nach § 170 Abs. 2 Strafprozessordnung (StPO) geändert wurden, um den Datenschutzanforderungen der Polizei gerecht zu werden. Erledigungskennziffern der neu geschaffenen Unterkategorien wurden in den Parametern des Übermittlungsprogramms für automatisierte Mitteilungen an die Ausländerbehörde jedoch versehentlich nicht nachgepflegt. Dies führte dazu, dass ein Großteil der Verfahrenseinstellungen nach § 170 Abs. 2 StPO nicht automatisiert an die Ausländerbehörde übermittelt wurde. Nach derzeitiger Schätzung auf Grundlage der Anzahl der Ermittlungsverfahren gegen ausländische Staatsangehörige, deren Einstellung in MESTA

unter den betroffenen Kennziffern erfasst worden ist, waren hiervon circa 80.000 Verfahren betroffen (vgl. Bürgerschaft der Freien und Hansestadt Hamburg, Drucksache 22/8990).

Infolgedessen begann der HmbBfDI damit, die genauen Umstände und technischen Voraussetzungen der Systeme zu ermitteln. Hierzu gab es im Oktober 2022 auch ein Treffen mit dem zuständigen Dezernenten bei der Staatsanwaltschaft, dem behördlichen Datenschutzbeauftragten sowie der für die technische Realisierung verantwortlichen IT-Abteilung, in dem die einzelnen Systeme näher erläutert worden sind. Die unmittelbaren, für das Fehlverhalten ursächlichen Systeme wurden zu diesem Zeitpunkt bereits angepasst, sodass ein stabiler Betrieb inkl. der tagesaktuellen Meldungen an die Ausländerbehörden wieder möglich war. Allerdings stellte sich heraus, dass die Systeme grundsätzlich an die technische Entwicklung angepasst werden müssen und die Staatsanwaltschaft diese auch im Zuge ihrer Digitalisierungsstrategie einplant; allerdings bislang ohne konkreten Zeitplan. Dies führt zur gegenwärtigen Situation, dass ein fehleranfälliges Altsystem weitergenutzt wird, welches sich nicht gut pflegen und aktualisieren lässt und somit bspw. bei Anpassungen von MESTA händisch angepasst werden muss, da ansonsten fehlerhafte Exporte aus den Datenbeständen drohen würden.

Zudem wurden diese Anpassungen bislang nicht gemäß der geltenden Verwaltungsvorschriften der FHH in Form von Freigabetests abgebildet oder dokumentiert, wodurch intransparent wird, welche Personen(-kreise) Änderungen an den beteiligten IT-Systemen durchgeführt haben. Ein belastbarer Betrieb erscheint aber so nicht dauerhaft möglich.

Die Staatsanwaltschaft sieht nun organisatorisch einen Prozess vor, in dem durch entsprechende Genehmigungsprozesse sowie Abnahmetests die Funktionsfähigkeit – auch bei zentralen Anpassungen in MESTA – gewährleistet werden soll. Inwieweit dieser Prozess schon etabliert ist, konnte zum Ende des Berichtszeitraums nicht geklärt werden. Auch ein detaillierter Fragenkatalog zur weiteren Sachver-

haltsaufklärung wurde noch nicht beantwortet, sodass zum Ende des Berichtszeitraumes unklar bleibt, unter welchen Rahmenbedingungen die Meldungen von Staatsanwaltschaft an die Ausländerbehörden mittel- und langfristig stattfinden werden.

Kurz vor Redaktionsschluss wurde dem HmbBfDI mitgeteilt, dass aufgrund der Unterbesetzung der IT-Abteilung die aufgeworfenen Fragen nicht im Berichtszeitraum beantwortet werden können. Es konnte jedoch mitgeteilt werden, dass die Staatsanwaltschaft Hamburg weiterhin im regelmäßigen Austausch mit der Ausländerbehörde Hamburg steht und zur Nachmeldung unterbliebener Mitteilungen nunmehr eine Tabelle erstellt wurde, die einen Umfang von 10.000 Verfahren in der Zeit seit 01. September 2021 habe. Unklar bleibt daher weiter, in welchem Umfang Meldungen an Ausländerbehörden außerhalb Hamburgs unterblieben und somit nachzuholen sind und weshalb der Zeitraum zwischen 01. Januar 2018 bis 31. August 2021 nicht inkludiert ist. Dies wird der HmbBfDI im kommenden Jahr weiterverfolgen und auf eine zeitnahe Behebung der Missstände dringen.

3. Prüfung von Videokonferenzsystemen beim IT-Dienstleister Dataport

Prüfgegenstand waren durch Dataport selbstentwickelte Videokonferenzsysteme auf Basis quelloffen entwickelter Software sowie ein Produkt auf Basis einer proprietären Cisco-Anwendung. Im Ergebnis wurden einige Mängel festgestellt, von denen bereits mehrere durch Dataport behoben worden sind bzw. in naher Zukunft behoben werden sollen. Die noch offenen Punkte werden weiterverfolgt, um sie gemeinsam mit Dataport zu klären.

Der HmbBfDI hat sich im Berichtszeitraum weiter zusammen mit den Datenschutzaufsichtsbehörden der Dataport-Trägerländer Schleswig-Holstein, Sachsen-Anhalt und Bremen an der gemeinsa-

men Prüfung der Videokonferenzsysteme bei Dataport beteiligt, die den Behörden als Angebot zur Auftragsverarbeitung zur Verfügung stehen (vgl. 30. TB, 2.5). Bei den untersuchten Videokonferenzsystemen handelt es sich einerseits um eine seit mehreren Jahren im Dataport-Portfolio befindliche Lösung auf Basis von Cisco mit dem Produktnamen dVideokommunikation und andererseits um zwei Lösungen, die Dataport im Kontext des sog. Projekt Phoenix auf Basis von Jitsi Meet entwickelt und unter dem Produktnamen dOnlineZusammenarbeit in Version 1.0 und 2.0 auch als Einzelkomponenten vermarktet. Darüber hinaus bieten die Systeme zusätzliche Chat- und andere Mehrwertfunktionalitäten, die allerdings nicht Gegenstand der nun abgeschlossenen Prüfung waren. Der Fokus lag stets auf den Videokonferenz-Komponenten der geprüften Systeme.

Die Datenschutzaufsichtsbehörden versandten Mitte 2022 ein vorläufiges Prüfergebnis an Dataport und regten einen Austausch zu den festgestellten Punkten an. Nachdem dieser Austausch stattgefunden hatte und Dataport zudem Gelegenheit zur Stellungnahme erhielt, wurde schließlich im September ein finales Prüfergebnis mitgeteilt, welches auch nachrichtlich den für ressortübergreifende IT-Angelegenheiten zuständigen Behörden in den vier Trägerländern zuging; für Hamburg ist dies die Senatskanzlei.

Im Ergebnis kann festgehalten werden, dass bei allen geprüften Systemen Mängel festgestellt wurden. Diese sollen im Folgenden exemplarisch skizziert werden.

Aufgezeigte Mängel bei dVideokommunikation
Die Mängel im Falle des Dienstes dVideokommunikation betrafen u.a. unzureichende Umsetzungen der Anforderungen des Art. 5 DSGVO zu den Grundsätzen der Verarbeitung personenbezogener Daten. Insbesondere die Tatsache, dass dVideokommunikation ausschließlich für Szenarien ausgelegt ist, in denen ein normaler Schutzbedarf vorliegt und somit keine besonderen Kategorien personenbezogener Daten (gem. Art. 9 DSGVO), Verschlusssachen oder andere Inhalte, die einem Amtsgeheimnis unterliegen, verarbeitet werden, muss ein-

deutig aus den Musterdokumentationen hervorgehen und den Verantwortlichen vor Vertragsabschluss mitgeteilt werden, damit dieser beurteilen kann, ob das Produkt für seinen Bedarf geeignet ist. Hier hat Dataport bereits in Aussicht gestellt, dass die Leistungsbeschreibungen überarbeitet werden und ergänzende Hinweise aufgenommen werden, dass das Produkt nur für Daten mit Schutzbedarf „normal" ausgerichtet ist. Die ggf. erforderlichen Vertragsanpassungen werden bis Ende des ersten Quartals 2023 umgesetzt. Dies ist ein guter Schritt in Richtung einer transparenten Dokumentation.

An dieser Stelle sei deutlich betont, dass die Auswahl eines geeigneten Videokonferenzsystems stets dem Verantwortlichen obliegt und dieser entscheiden muss, ob die von ihm vorgesehenen Daten verarbeitet werden dürfen.

Ein weiterer Punkt, den die beteiligten Aufsichtsbehörden bemängelten, betrifft das Fehlen des differenzierten Rollenkonzeptes auf Seite der Nutzenden und tangiert somit die Anforderungen des Art. 25 DSGVO. So waren keine Maßnahmen zur Teilnehmersteuerung nutzbar, mit der Konsequenz, dass Gäste der Konferenz weitere Teilnehmer zulassen oder gar den Gastgeber aus der Konferenz werfen können. Prinzipiell können Cisco-basierte Videokonferenzplattformen eine Moderatoren- bzw. Gastgeberrolle vorsehen. Die fehlende Nutzung verschiedener Rollen mit unterschiedlichen Berechtigungen wird zwar nicht als direkter Datenschutzverstoß gewertet, aber sie ist zumindest problematisch, da dadurch keine bzw. keine effektive Steuerung des Systems, auf dem anwendungsbedingt große Mengen personenbezogener Daten verarbeitet werden, möglich ist.

Auch hier hat Dataport bereits in Aussicht gestellt, dass geprüft wird, ob und in welcher Form eine Erweiterung der bestehenden Dienste um Steuerungsfunktionen möglich ist, mittels derer eine Gastgeberrolle installiert werden kann. Diese Prüfung soll in den ersten Januarwochen 2023 abgeschlossen sein und die Umsetzung wäre dann – sofern die Umsetzung technisch möglich ist – für April 2023 vorgesehen.

Darüber hinaus erfolgten diverse weitere Hinweise auf Aspekte, die die Anforderungen der Art. 13, 28 und 32 DSGVO betreffen.

Zuletzt sei bei dieser Teilprüfung erwähnt, dass auch hier die Frage der rechtmäßigen Verarbeitung in Drittstaaten, insbesondere im Supportfall, eine Rolle spielt. Hier sind die beteiligten Aufsichtsbehörden weiter mit Dataport im Gespräch und werden berichten, sobald hierzu Ergebnisse verzeichnet werden können.

Aufgezeigte Mängel bei dOnlineZusammenarbeit 1.0 und 2.0

Die Mängel im Falle der Dienste dOnlineZusammenarbeit 1.0 und 2.0 umfassten u.a. ebenfalls Anforderungen der Art. 5 und 28 DSGVO. Gegenstand waren hier insbesondere unvollständige Dokumente, wie u.a. ein sich seit über einem Jahr in Erstellung befindliches Sicherheitskonzept. Hierzu hat Dataport mitgeteilt, dass der Zieltermin für die Fertigstellung des Sicherheitskonzeptes für dOnlineZusammenarbeit 1.0 der 31.12.2022 sei. Der Zieltermin für die Fertigstellung des Sicherheitskonzeptes für dOnlineZusammenarbeit 2.0 könne ab dem 31.12.2022 mitgeteilt werden. Dieser Umstand ist nicht nur ein formal misslicher Umstand, sondern stellt alle Verantwortlichen, die einen der beiden Dienste nutzen, vor die Herausforderung, vollständig in Eigenregie potentielle (Sicherheits-)Risiken, die ggf. aus dem Betrieb der Dienste bzw. der einzelnen IT-Komponenten resultieren, in Erfahrung bringen zu müssen. Dies ist in der Praxis ohne die Mitwirkung des für den Betrieb beauftragten Dienstleisters nahezu unmöglich und dürfte daher von vielen Verantwortlichen nicht umgesetzt worden sein. Dataport dokumentierte daraufhin in den Muster-Dokumenten zunächst, einige Risiken der Verarbeitung selbst zu übernehmen. An dieser Stelle sei daher darauf hingewiesen, dass die durch die verzögerte Bearbeitung ggf. auftretenden datenschutzrechtlichen Risiken nicht durch Dataport als Auftragsverarbeiter getragen werden können, sondern diese den jeweiligen Kunden als eigentliche datenschutzrechtliche Verantwortliche mitzuteilen sind, damit diese eine Entscheidung treffen können.

Ein weiterer Mangel lag in der Bereitstellung ausschließlich generischer Vertragsmuster, die im Falle von dOnlineZusammenarbeit 1.0 nicht spezifisch auf die konkreten Rahmenbedingungen eingehen und somit keine für die Verantwortlichen wirklich nutzbare Form darstellten. Hier hat Dataport bereits bestätigt, dass produktspezifische Vertragsmuster in Arbeit sind.

Darüber hinaus erfolgten diverse weitere Hinweise auf Aspekte, die die Anforderungen der Art. 25 und 32 DSGVO betreffen.

Die Prüfung der Videokonferenzsysteme ist zwar trotz Feststellung des finalen Prüfergebnisses noch nicht vollständig abgeschlossen, da weitere Merkposten verbleiben und teilweise Zusicherungen Dataports auf Ergänzungen und Anpassungen ins Jahr 2023 datieren, die von den an der Prüfung beteiligten Aufsichtsbehörden dann zu gegebener Zeit begutachtet werden. Dennoch kann bereits jetzt konstatiert werden, dass die Zusammenarbeit und Kooperationsbereitschaft mit Dataport als sehr positiv zusammengefasst werden kann. Es herrschte stets eine kooperative, zielgerichtete Arbeitsweise und zugesicherte Zulieferungen sowie Fristen wurden verlässlich eingehalten. Zuletzt kann festgehalten werden, dass im Rahmen der Teilprüfung von dOnlineZusammenarbeit 1.0 und 2.0 häufig belastbarere Unterlagen bereitgestellt werden konnten. Zudem wurde im Laufe der Prüfung klar, dass Dataport deutlich tiefergehende Anpassungen an den beiden auf quelloffenen Diensten basierenden Systemen umsetzen kann bzw. dies nach Aufträgen der Kunden tun könnte. Dem gegenüber steht dVideokommunikation als für sich im Funktionsumfang fest umrissener Dienst, der ohne Weiterentwicklungen des Herstellers wenige Anpassungen oder Erweiterungen für Dienstleister wie Dataport ermöglicht. Hier zeigt sich, dass die Flexibilität durch transparente und quelloffene Systeme dazu führt, dass Verantwortliche und Dienstleister souverän über ihre IT-Systeme entscheiden können und dies auch aus datenschutztechnischer Sicht Überprüfungen der Dienste erleichtert.

4. E-Mail-Kommunikation der FHH an Externe

4.1 Transportverschlüsselung

Die Senatskanzlei und Dataport haben die Empfehlungen des HmbBf DI bezüglich eines umfassenden Basis Schutzes für die Transportver schlüsselung aufgegriffen. Die entsprechende Konfiguration der Mail-Infrastruktur wurde zwar von der Senatskanzlei noch nicht beauftragt, aber in Aussicht gestellt.

Bereits kurz nach der Veröffentlichung der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" der Datenschutzkonferenz Mitte 2021 nahm der HmbBfDI Gespräche mit der Senatskanzlei auf, um den Einsatz von zusätzlichen Absicherungsmaßnahmen bei der Übermittlung von E-Mails zu forcieren. Insbesondere wurden dabei Maßnahmen besprochen, die auf dem Transportwege ergriffen werden sollten und einen Basis-Schutz zur Erfüllung gesetzlicher Anforderungen darstellen. In der FHH wurden zu diesem Zeitpunkt bereits schon flächendeckend Maßnahmen zur Transportverschlüsselung der Mailinhalte genutzt. Dieser Schutz sorgt dafür, dass potentielle Angreifer die Inhalte der Mail auf dem Übertragungsweg nicht einsehen können. Dennoch bleiben die Endpunkte der Übertragung, nämlich die Sender und Empfänger sowie etwaige Metadaten dabei weitestgehend ungeschützt. Die Orientierungshilfe hält daher fest, dass der aktuelle Stand der Technik weitergehende technische Maßnahmen – selbst bei normalen datenschutzrechtlichen Risiken – umfasst. So sind zur Sicherstellung der Authentizität und Integrität der empfangenen E-Mail-Nachrichten Prüfungen der sog. DKIM-Signatur erforderlich. DKIM begrenzt die Möglichkeit, E-Mail-Absenderadressen zu verschleiern, da man feststellen kann, ob eine E-Mail tatsächlich über die angegebene Domäne versendet wurde. Sofern die Prüfung der Signaturen fehlschlägt, können diese Nachrichten dann als verdächtigt markiert oder direkt zurückgewiesen werden. Die

auszuführende Reaktion ergibt sich aus dem E-Mail-Authentifizierungsprotokoll DMARC, das auf DKIM aufsetzt.

Um diese Anforderungen für die FHH umzusetzen, nahm der HmbBfDI an Sitzungen der Arbeitsgruppe teil, die die Mail-Server-Infrastruktur der Verwaltungen der Dataport-Trägerländer Bremen, Hamburg, Schleswig-Holstein und Sachsen-Anhalt koordiniert und entsprechende technische Ergänzungen beauftragt. Dabei stellte sich schnell heraus, dass das Gremium zwar die Erforderlichkeit zur Nutzung von DKIM/DMARC sah, die damalige Mail-Infrastruktur allerdings bereits geplant durch ein neueres Produkt abgelöst werden sollte. Die vom HmbBfDI – in Vertretung für die anderen Aufsichtsbehörden der Dataport-Trägerländer – vorgetragenen Anforderungen bzgl. DKIM und DMARC wurden als fester Bestandteil des Anforderungskataloges der Ausschreibung der neuen Mail-Infrastruktur aufgenommen.

Kurz vor Redaktionsschluss haben die Senatskanzlei und Dataport in Aussicht gestellt, dass nunmehr eine Beauftragung einer anforderungsgerechten Konfiguration erfolgen solle. Mit dieser Konfiguration wäre ein wichtiger Schritt zu einer anforderungsgerechten Transportverschlüsselung mit einem Basis-Schutz nach dem Stand der Technik erfolgt.

Der HmbBfDI hat in den Gesprächen mit der Senatskanzlei wiederholt deutlich gemacht, dass ein grundlegender Basis-Schutz der Transportverschlüsselung jedoch nicht ausreicht, wenn sensible personenbezogene Daten per Mail übertragen werden sollen. Nach der Orientierungshilfe der Datenschutz-Aufsichtsbehörden sind in diesen Fällen weitere Maßnahmen über diesen Basis-Schutz hinaus erforderlich, um zu einer qualifizierten Transportverschlüsselung zu kommen. Dazu gehören u.a., dass kryptografische Algorithmen und Protokolle dem Stand der Technik entsprechen und die weiteren Anforderungen der Technischen Richtlinie BSI TR-02102 erfüllen. Auch wenn diesbezüglich noch kein Konsens mit der Senatskanzlei hergestellt werden konnte, wird der HmbBfDI weiter den Weg verfolgen,

in konstruktiven Gesprächen mit der Senatskanzlei und Dataport konkret Schritte anzustoßen, um auch eine anforderungsgerechte Lösung für die Mail-Kommunikation bei hohem Schutzbedarf bereitzustellen, da in vielen Arbeitsfeldern der Behörden solche sensiblen Daten regelmäßig und in großem Umfang anfallen.

4.2 Ende-zu-Ende-Verschlüsselung mit den Jugendhilfe-Trägern

Der Start der Ende-zu-Ende-Verschlüsselung mit den Jugendhilfe-Trägern verschiebt sich um ein weiteres Jahr – aber die erfolgreich pilotierte Lösung wird von den beteiligten Behörden weiterverfolgt. Ein Plantermin für den produktiven Start ist jedoch noch offen.

Verantwortliche, die E-Mail-Nachrichten versenden, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, müssen gemäß der Orientierungshilfe der Datenschutz-Aufsichtsbehörden „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ über die qualifizierte Transportverschlüsselung hinaus regelmäßig eine Ende-zu-Ende-Verschlüsselung vornehmen. Der Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Nur die Empfänger:innen können die verschlüsselte E-Mail mit ihrem privaten Schlüssel entschlüsseln.

Bereits 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. Dies ist ein Beispiel, beim dem ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht. Auch wenn Ende 2021 schon fünf Jahre seit dem Beginn der Prüfung verstrichen waren, war der HmbBfDI verhalten optimistisch, dass nach der erfolgreichen Pilotierung im Jahr 2020 die Vorbereitung des Rollouts im März 2022 abgeschlossen sein würde und ab November 2022 endlich die Ende-zu Ende-verschlüsselte Kommunikation mit den externen Jugendhilfe-Trägern erfolgen würde (vgl. 30. TB, 2.2).

Es kam jedoch anders: Nach wie vor sind die Vorbereitungen des Rollouts nicht abgeschlossen. Insbesondere drei Schwierigkeiten hat die Lenkungsgruppe des Projekts im Dezember 2022 festgestellt:

- Alle Jugendhilfe-Träger müssen eingebunden werden und Verschlüsselungszertifikate bereitstellen. Doch bis zum Jahresende wurden die Jugendhilfe-Träger von der Sozialbehörde, die diesen Teil des Projekts übernommen hat, noch nicht einmal angeschrieben und ausführlich informiert. Als Gründe wurden u.a. Personalwechsel und interne Umorganisation angegeben. Nunmehr soll das Schreiben an die Träger Ende Februar 2023 vorliegen, also etwa ein Jahr später als geplant.
- Für die Beschäftigten des ASD müssen Verschlüsselungszertifikate bereitgestellt werden. Technisch übernimmt dies Dataport als Dienstleister. Nach wie vor ist jedoch der Prozess der Personenidentifizierung bzw. Authentisierung innerhalb der Bezirksämter noch nicht abschließend geklärt. Dies soll nach Planungen der Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke (BWFGB) im Januar 2023 erfolgen.
- Eine Ende-zu-Ende-Verschlüsselung setzt voraus, dass für alle Nutzenden Verschlüsselungszertifikate zur Verfügung gestellt werden. Diese werden im Governikus MultiMessenger (GMM) gespeichert. Für eine einfache Suche nach Identitäten bzw. Empfängeradressen im Identitätenspeicher des GMM wird der Verzeichnisdienst-Connector (VDC) genutzt. Ein mandantenfähiger VDC stand erst seit Dezember 2022 zur Nutzung zur Verfügung.

Nach dem weitgehend ungenutzt verstrichenen Jahr 2022 setzt der HmbBfDI darauf, dass die von den beteiligten Behörden zugesagten Ankündigungen eingehalten werden und nunmehr spätestens in der 2. Jahreshälfte 2023 die Ende-zu-Ende-Verschlüsselung zwischen ASD und Jugendhilfe-Trägern genutzt werden kann. Gleichzeitig zeigt dieser Einführungsprozess, wie wenig der öffentliche Dienst in der FHH aufgestellt ist für eine umfangreiche digitale Verwaltung ohne Medienbrüche.

5. Biometrische Gesichtserkennung am Flughafen Hamburg

Kontrollstellen mit biometrischer Gesichtserkennung müssen deutlich von den anderen getrennt sein, damit keine biometrischen Templates von Personen erfasst werden, die dafür keine Einwilligung erteilt haben. Der HmbBfDI hat darauf hingewirkt, dass am Flughafen Hamburg nur die Fluggäste die neuen, mit einem biometrischen System ausgestatte ten zentralen Sicherheitskontrollen passieren, die zuvor ihre Registrie rung auf einer Plattform vorgenommen und dort ihre Einwilligung erteilt haben.

Kontaktlos reisen mit Gesichtserkennung kann man seit dem Frühjahr 2022 auch am Flughafen Hamburg. Der Dienst verspricht einen verbesserten Reisekomfort und steht Fluggästen der Lufthansa Group zur Verfügung, die die Sicherheitskontrollen an Flughäfen sowie an den Gates kontaktlos passieren wollen.

Der Zutritt zu den verschiedenen Sicherheitsbereichen am Flughafen wird unterschiedlich kontrolliert. Wer eine gültige Bordkarte besitzt, erhält Zugang zum kontrollierten Bereich des Flughafens. Die Bordkartenkontrolle erfolgt durch automatische Anlagen, die einen Bordkartenleser integriert haben, der die Barcodes/QR-Codes der Bordkarte erfasst.

Bordkarten erhält man am Check-In Schalter des Flughafens, durch einen eigenen Ausdruck im Online-Check-In oder digital und papierlos auf dem Smartphone oder der Smartwatch. Fluggäste einiger Fluggesellschaften, die sich zuvor für ein bestimmtes Loyalitätsprogramm registriert haben, können außerdem mit einem einzigen Blick – so wird es angepriesen – jetzt auch die Sicherheitskontrolle am Flughafen Hamburg passieren. Diese Fluggäste haben Ihre Zustimmung zur Identifizierung durch Gesichtserkennung erteilt, indem sie in die Verarbeitung der besonderen Kategorien personenbezogener Daten gem. Art. 9 Abs.1 DSGVO (biometrische Daten) eingewilligt haben. Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen (vgl. Art. 4 Nr. 14 DSGVO).

Zu diesem Zweck wurden an den Fastlanes der zentralen Sicherheitskontrolle am Flughafen Hamburg Touchpoint-Kameras angebracht, die eine kurze Videosequenz des Gesichts des Fluggastes erheben, sobald er sich in den Erkennungsbereich begibt. Aus der Videosequenz wird anschließend automatisiert ein Foto extrahiert, welches zur Identifizierung genutzt wird, indem es mit einem oder mehreren zuvor im Registrierungsprozess zur biometrischen Gesichtserkennung hinterlegten Bildern des Fluggastes abgeglichen wird. Beim Abgleich wird mit einer Erkennungssoftware das Gesicht lokalisiert und seine charakteristischen Eigenschaften berechnet. Das Ergebnis dieser Berechnung, das sog. Template, wird mit jenen verglichen, die im Rahmen der Registrierung mit Einwilligung des Fluggastes erstellt wurden, damit erkannt werden kann, ob es sich bei der betroffenen Person um einen registrierten Fluggast handelt oder nicht. Das System zielt darauf ab, Fluggäste aus einer Datenbank wiederzuerkennen und von nicht-registrierten Fluggästen zu unterscheiden. Fällt der Abgleich positiv aus, werden Informationen der Bordkarte automatisch übermittelt und dann vom Flughafen Hamburg geprüft.

Biometrische Systeme, die nicht in kontrollierten Umgebungen installiert sind, können biometrische Templates von allen Personen erstellen, deren Gesichter in den Erfassungsbereich der Kamera geraten, und damit auch von Personen, die nicht in die Erfassung biometrischer Merkmale eingewilligt haben. Besteht der Zweck darin, natürliche Personen eindeutig zu identifizieren, ist eine Ausnahme nach Art. 9 Abs. 2 DSGVO, beispielsweise eine Einwilligung, für alle von der Kamera erfassten Personen erforderlich.

Bei Prüfungen vor Ort am Flughafen Hamburg hat der HmbBfDI festgestellt, dass auch Personen den Fastlane-Bereich mit Gesichtserkennung betreten, die nicht zuvor in eine Gesichtserkennung eingewilligt hatten. Die vorhandenen, auf Gesichtserkennung hinweisenden Markierungen und Beschilderungen hielten dennoch nicht alle anderen Reisenden, die nicht in die Gesichtserkennung eingewilligt hatten, davon ab, diese Zugänge für eine schnelle Kontrolle zu nutzen.

Der Flughafen Hamburg hat zeitnah technische und organisatorische Maßnahmen ergriffen, um zu verhindern, dass Personen ohne Einwilligung erfasst werden. Folgende zusätzliche Maßnahmen wurden zunächst ergriffen: Der Hinweis auf den biometrischen Zugang auf dem Monitor über der Fastlane wurde besonders farblich hervorgehoben, zusätzliche Aufsteller vor den eGates, um den Zugang zu regulieren, Markierung der eGates mit Pfeilen und Piktogrammen, Warnhinweise und Piktogramme auf den Schwenkflügeln der eGates, höhere Sichtbarkeit der Datenschutzhinweise, Hinweise auf dem Fußboden auf der Spur zu den eGates, Abtrennung der Fastlane-Zugänge mit und ohne Gesichtserkennung durch Gurtband zur Separierung der Schleusen. Weitere Maßnahmen sollen noch ergriffen werden.

Der HmbBfDI hat keine weiteren Prüfungen der datenschutzrechtlichen Zulässigkeit der biometrischen Gesichtserkennung vorgenommen, da insoweit keine weitere Zuständigkeit angenommen wird.

6. Feuerwehr – Beseitigung des Mangels erst nach 6 Jahren

Die Übertragung der personenbezogenen Notfalldaten der Feuerwehr erfolgt seit November 2022 nur noch verschlüsselt. Das Ergebnis zeigt, dass es sich gelohnt hat, trotz zahlreicher Rückschläge in der Umsetzung bei der Feuerwehr kontinuierlich den jeweiligen Stand zu hinterfragen und sich zu Datenschutzaspekten beratend und hinweisend einzubringen.

Bereits im Herbst 2016 hat der HmbBfDI erfahren, dass die Notfallalarmierungen der Feuerwehr Hamburg, die unverschlüsselt per Funk an die Einsatzkräfte übertragen werden, von Unbekannten illegal abgehört wurden. Die sensiblen personenbezogenen Daten wurden mehrfach ins Internet gestellt. Die Feuerwehr Hamburg hat nach der Unterrichtung durch den HmbBfDI als erste kurzfristige Maßnahme die übertragenen Daten zwar reduziert. Aber auch dieser reduzierte Datensatz enthielt bis zum Herbst 2022 immer noch sensible Daten, die nur verschlüsselt übertragen werden dürfen. Mit der Feuerwehr wurde bereits Mitte 2017 ein Konsens erzielt, dass schnellstmöglich eine Verschlüsselung der per Funk übertragenen Notfalldaten erfolgen soll. Gleichzeitig bestand zwischen der Feuerwehr Hamburg und dem HmbBfDI Einvernehmen, dass zu jeder Zeit eine stabile Notfallalarmierung gewährleistet werden muss.

Um den in 2016 bekannt gewordenen Mangel zu beheben, wurden von der Feuerwehr zwei Alarmierungswege mit verschlüsselter Funkdatenübertragung realisiert. Alle Notfalldaten werden parallel über beide Alarmierungswege übertragen.

- 1. Alarmierungsweg
  Die Funkübertragung auf dem 1. Alarmierungsweg basiert auf dem BOS-Digitalfunk, der in Hamburg bei Polizei und Feuerwehr seit Jahren produktiv genutzt wird. Das im TETRA-BOS-Digitalfunk verwendete Kryptosystem des BSI (Bundesamt für Sicher-

heit in der Informationstechnik) besteht aus einem Ende-zu-Ende-Verschlüsselungssystem mit hohem Sicherheitsstandard, bei dem auch ein regelmäßiger Schlüsselwechsel möglich ist. Um dieses Netz auch für die Notfallalarmierung nutzen zu können, war es insbesondere notwendig, das Netz in enger Abstimmung mit dem Bund für diese zusätzliche Nutzung zu ertüchtigen, für alle zu informierenden Organisationseinheiten die erforderlichen TETRA-BOS-Meldeempfänger (TME) zu beschaffen und auszuliefern und die Informationsprozesse in der Einsatzleitzentrale entsprechend anzupassen. Der Rollout der TME konnte in der ersten Jahreshälfte 2022 abgeschlossen werden. Um eine stabile Notfallalarmierung auch unter Pandemie- und Krisenbedingungen sicherstellen zu können, hatte sich die Feuerwehr Hamburg entschlossen, das bisherige unverschlüsselte Übertragungssystem erst mit der Inbetriebnahme der neuen Einsatzleitzentrale im November 2022 abzuschalten. Die unverschlüsselte Übertragung der Notfalldaten wurde mit dieser Umstellung beendet.

- 2. Alarmierungsweg
  Dieser Alarmierungsweg erfolgt unter Nutzung der SyBOS-App, die für Smartphones zur Verfügung steht. Die übertragenen Daten werden als Push-Nachrichten mit dem Verschlüsselungsverfahren AES-256 verschlüsselt. Die Feuerwehr Hamburg begann 2019 mit der Realisierung dieser Lösung und hat in der ersten Jahreshälfte 2022 die SyBOS-App als zweiten Alarmierungsweg in Betrieb genommen.

Im Zuge der Umsetzung der beiden Alarmierungswege, die der HmbBfDI beratend eng begleitet hat, kam es mehrfach zu deutlichen Verzögerungen gegenüber den vorgestellten Planungen. Dazu trugen u.a. technische Rückschläge, Fehler bei der Softwareentwicklung, Klärung der Nutzungsbedingungen der SyBOS-App durch die Freiwillige Feuerwehr, die Aufwände für die Beschaffung zusätzlicher TETRA-BOS-Meldeempfänger, die Abhängigkeit zur neuen Einsatzleitzentrale und auch durch die zusätzlichen Belastungen durch die Corona-Pandemie bei. Gleichwohl ist ein Zeitraum von 6 Jahren für

die Mangelbeseitigung, der damit doppelt so lange ausfiel, wie die Planungen der Feuerwehr zunächst vorsahen, kaum nachvollziehbar.

7. Prüfung der Vertrauensstelle BSB

Der HmbBfDI ist im Berichtszeitraum seiner Verpflichtung gemäß § 98a Absatz 7 HmbSG nachgekommen und prüft die Vertrauensstelle der Behörde für Schule und Berufsbildung (BSB) umfassend.

Mit dem zweiundzwanzigsten Gesetz zur Änderung des Hamburgischen Schulgesetzes (HmbSG) wurde im Jahr 2016 die Vorschrift des § 98b HmbSG geschaffen und mit ihr eine sogenannte Vertrauensstelle in der Behörde für Schule und Berufsbildung eingesetzt. Es sollte damit eine rechtliche Grundlage für die Verknüpfung von schulstatistischen Rohdaten mit Daten von Schüler:innen aus Testverfahren, Unterrichtsbeobachtungen und anderen Evaluationsverfahren im Sinne von § 100 HmbSG und der Speicherung dieser zusammengeführten Datensätze geschaffen werden. Diese Verknüpfungen werden seitens der BSB für erforderlich erachtet, damit Bildungsverläufe dargestellt und wissenschaftlich auswertbar gemacht werden können. Die Änderung des Schulgesetzes folgte zudem auch als Reaktion auf Beanstandungen des HmbBfDI bezüglich der rechtlichen Voraussetzungen solcher Datenerhebungen und ihrer statistischen Auswertung. Die Vertrauensstelle ist dem Institut für Bildungsmonitoring und Qualitätsentwicklung (IfBQ) zugeordnet und ihre Arbeit wird dort von zwei Stellen wahrgenommen.

Durch die Zwischenschaltung einer Vertrauensstelle für den Prozess der Verknüpfung von Datensätzen aus unterschiedlichen Bereichen der Schullandschaft sollte sichergestellt werden, „dass keiner der Beteiligten außerhalb dieser Vertrauensstelle auch mit dem größtmöglichen Zusatzwissen in der Lage wäre, die einzelnen Daten zu

solchen Informationen zu verdichten, die Rückschlüsse auf einzelne identifizierbare Schülerinnen und Schüler zuließe“ (Drucksache 21/4949, Gesetzesbegründung zu Nr.11, Seite 8). Dem Ausschluss der Re-Identifizierbarkeit von Schüler:innen kommt besondere Bedeutung zu, weil die Verknüpfung verschiedener Datensätze und ihre Herausgabe auf Antrag nach § 98a Abs. 6 HmbSG gleichbedeutend mit dem Datenaustausch zwischen datenschutzrechtlich jeweils eigenständig verantwortlichen Stellen ist, ggf. auch externe Stellen des nicht-öffentlichen Bereichs umfasst, ggf. eine gesamte Schulkarriere von Schüler:innen abbildet und sich daraus ein besonderes Risiko für die Rechte und Freiheiten der betroffenen Schüler:innen ergibt. Auch wenn die Vorschrift des § 98a HmbSG im Einzelnen in Bezug auf die Anforderungen an die Unmöglichkeit der Reidentifizierbarkeit der betroffenen natürlichen Personen und die Abschottung der Stelle von anderen Aufgaben des Verwaltungsvollzuges hinter den Regelungen in §§ 7 und 9 Hamburgisches Statistikgesetz (HmbStatG) zurückbleiben mag, kann zumindest ein relativ hoher Pseudonymisierungsgrad hinsichtlich der verknüpften Daten erreicht werden.

Die Verarbeitungsvoraussetzungen in § 98a Abs. 1-6 HmbSG wurden in § 98a Abs. 7 HmbSG zusätzlich durch eine Prüfverpflichtung des HmbBfDI ergänzt, die im Jahr 2022 angestoßen wurde. Im Rahmen der Prüfung der Vertrauensstelle und der ihr zugrundliegenden Datenbank wurde in mehreren Schritten zunächst die personelle und technische Organisation der Vertrauensstelle in Bezug auf die Übereinstimmung mit den schulgesetzlichen Vorgaben und die tatsächlich von der Stelle vorgenommenen Datenverknüpfungen und Herausgaben im Antragsverfahren nach § 98a Abs. 6 HmbSG geprüft. Dabei zeigte sich die Behörde für Schule und Berufsbildung vertreten durch ihren Datenschutzbeauftragten und die Mitarbeiter:innen der Vertrauensstelle überaus kooperativ, offen für Nachfragen und sie gewährte umfassend Einsicht in die datenschutzrechtliche Dokumentation. Es wurde deutlich, dass die Mitarbeiter:innen der Vertrauensstelle datenschutzrechtlichen Fragestellungen einen hohen Stellenwert beimessen und ihrer

Arbeit entsprechend verantwortungsvoll nachkommen wollen. Es wurden dem HmbBfDI insbesondere Verfahrensbeschreibungen, Beschreibungen der Verarbeitungstätigkeit, Antragsverzeichnis, Risikobetrachtungen, Schwellenwertanalyse und Datenschutzfolgeabschätzung und Stellenbeschreibungen zur Verfügung gestellt. Bei der weiteren Prüfung dieser Dokumente wird ein Hauptaugenmerk auf der ausreichenden Trennung der Aufgaben und der bei der Vertrauensstelle vorliegenden Daten von den übrigen Aufgaben des Verwaltungsvollzuges, Art und Anlass der auftretenden Datenströme, der technischen Ausgestaltung der Datenbank der Vertrauensstelle, Fragen der Datensicherheit und Identifizierbarkeit von Betroffenen und der Ausgestaltung des durch die Vertrauensstelle zu betreuenden Antragsverfahrens liegen.

Die Prüfung ist zum Ende des Berichtszeitraumes noch nicht abgeschlossen und dauert noch an. Unabhängig vom Ergebnis der Prüfung wird ggf. anhand der Feststellungen auch gesetzgeberischer Handlungsbedarf ermittelt werden und an den Gesetzgeber zurückgemeldet werden können.

8. Parken mit Kfz-Kennzeichenerkennung

Der HmbBfDI erhielt im Berichtsjahr Beschwerden sowie Beratungsan fragen zum Thema Parken mit Kfz-Kennzeichenerkennung. Bei Einsatz eines Kennzeichenerkennungssystems und der damit einhergehenden Datenverarbeitung ist aus datenschutzrechtlicher Sicht einiges zu be achten.

Parken mit Kfz-Kennzeichenerkennung basiert auf einer Kameratechnik, die Bilder von Kennzeichen innerhalb kürzester Zeit und unter komplexen Bedingungen (bewegtes Objekt, schlechtes Umgebungslicht etc.) erfassen und mittels Texterkennungssoftware auslesen kann. Vom Einsatzzweck her ist sie damit abzugrenzen

von einer Videoüberwachung, die der großflächigen Überwachung von Räumen dient. Bei der Kennzeichenerkennung werden zusätzlich zum erkannten Kennzeichen bei Einfahrt regelmäßig die Bilddatei des Kennzeichens, das Datum und die Uhrzeit eines Parkvorgangs in einer Datenbank erfasst. Auf diese Datenbank wird bei Bezahlung des Parkvorgangs zur Ermittlung der Höhe der Parkgebühr sowie bei Ausfahrt zugegriffen, wenn das Kennzeichen ein weiteres Mal ausgelesen und mit den dazu gespeicherten Daten abgeglichen wird.

Betreiber privater Parkplätze und -häuser setzen Kennzeichenerkennungssysteme immer häufiger ein oder wollen sie gerne zum Einsatz bringen, um Verträge über die Nutzung ihrer Parkflächen abzuschließen und abzuwickeln. Als Argumente für das Parken mit Kfz-Kennzeichenerkennung werden neben einem verbesserten Komfort für die Parkplatznutzenden durch schnelleres Ein- und Ausfahren (bei Systemen ganz ohne Ticket und/oder Schranke), der Wegfall von höheren bzw. zusätzlichen Kosten bei Ticketverlust oder vergessener Parkscheibe sowie die Möglichkeit des ressourcenschonenden Verzichts auf Papier-/Plastiktickets angeführt – das natürlich nur bei Systemen komplett ohne Ticket. Für die Betreiber spielt auch die Reduzierung des wirtschaftlichen Risikos eine Rolle, das sich bei reinen Ticketsystemen daraus ergeben kann, dass nach zeitlich ausgedehnten Parkvorgängen der Verlust des Tickets behauptet wird und so eine niedrigere als die tatsächlich geschuldete Parkgebühr anfällt.

Bei den Nutzenden kann Parken mit Kennzeichenerfassung aus den unterschiedlichsten Gründen zu Irritationen führen. Das liegt darin begründet, dass unabhängig von der Frage, wie die Bezahlung eines Parkvorgangs abgewickelt wird, ein anonymes Parken nicht mehr möglich ist. Denn über das verarbeitete Kfz-Kennzeichen lässt sich immer die Person ermitteln, die als Halter:in eingetragen ist. Daher ist auf jeden Fall Personenbezug gegeben und sind beim Einsatz von Kennzeichenerkennungssystemen die Vorgaben der Datenschutz-Grundverordnung (DSGVO) zu berücksichtigen. Das gilt ganz

unabhängig davon, wie diese Systeme konkret ausgestaltet sind: Ob sie grundsätzlich ohne Ticket auskommen (außer vielleicht in Fällen des Kameraausfalls) oder bei Einfahrt zusätzlich zur Kennzeichenerkennung immer auch ein Ticket gezogen und mit den Informationen zum dazugehörigen Kennzeichen verknüpft wird.

Wenn Betreiber privater Parkplätze und -häuser ein Kfz-Kennzeichenerkennungssystem nutzen, bedarf es daher immer einer Rechtsgrundlage. Das kann gegenüber solchen Personen, die einen Dauerparkplatz angemietet haben, eine Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO sein, die bei Gelegenheit des Vertragsabschlusses eingeholt wird. Zur Vertragsabwicklung ist die Kennzeichenerkennung nach Artikel 6 Abs. 1 lit. b) DSGVO nur dann erforderlich, wenn nicht zusätzlich zu Beginn eines jeden Parkvorgangs ein Ticket gezogen werden muss. Unter Umständen kann für eine gewisse Übergangszeit – zur Gewöhnung an ein neues Kennzeichenerfassungssystem – etwas anderes gelten und die parallele Nutzung von Ticket und Kennzeichenerkennung möglich sein. Schließlich kommt als Rechtsgrundlage auch Art. 6 Abs. 1 lit. f) DSGVO in Betracht, wenn Betreiber eines Parkplatzes oder -hauses darlegen können, dass die Kfz-Kennzeichenerkennung, vielleicht auch zusätzlich zum Ticket, zur Wahrung ihrer oder der berechtigten Interessen Dritter erforderlich ist und sofern nicht die Interessen der Betroffenen überwiegen. Wenn ein Betreiber sich z.B. auf sein berechtigtes Interesse an der Reduzierung des wirtschaftlichen Risikos durch Betrugsfälle (behaupteter Ticketverlust nach Langzeitparkvorgang) stützen will, müsste der finanzielle Schaden, der dadurch regelmäßig entsteht, nachgewiesen werden können. Gleiches gilt, wenn mit der Kennzeichenerkennung andere Interessen verfolgt werden.

Außerdem müssen die datenschutzrechtlichen Vorgaben zu den Transparenz- und Informationspflichten eingehalten werden. Das heißt, dass es eine gut sicht- und erkennbare sowie verständliche Hinweisbeschilderung geben muss, auch in Form eines aus der Entfernung erfassbaren Piktogramms. Ein solches sollte nicht den Eindruck vermitteln, dass eine großflächige Videoüberwachung statt-

findet, sondern deutlich machen, dass es allein um die Erstellung einer Bilddatei des Kennzeichens und dessen Erfassung geht. Darüber hinaus muss die Hinweisbeschilderung so ausgestaltet sein, dass es den Parkplatz-Nutzenden möglich ist, der Kennzeichenerkennung auszuweichen. Für den Fall, dass ein Ausweichen aufgrund der räumlichen Situation nicht möglich ist, sollten die verantwortlichen Betreiber es einrichten, dass die Parkflächen innerhalb eines bestimmten Zeitraums ohne Anfallen von Kosten verlassen werden können und das erfasste Kennzeichen umgehend nach Ausfahrt gelöscht wird. Ohnehin sind – mit Blick auf die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DSGVO – regelmäßig kurze Löschfristen für die Informationen zu den Kfz-Kennzeichen vorzusehen. Auch muss darauf geachtet werden, dass mittels der eingangs beschriebenen Kameratechnik nicht das gesamte Fahrzeug und vor allem keine Fahrzeuginsassen erfasst werden. Dass die Informationen zu den Kennzeichen nicht zu anderen als den im konkreten Fall vorgesehenen Zwecken verwendet werden dürfen, steht außer Frage.

Der HmbBfDI befindet sich in einzelnen Beschwerdefällen, die sich auch auf die Einrichtung einer sog. Kurzhaltezone mit Kennzeichenerkennung am Hamburger Flughafen beziehen, im Austausch mit den Verantwortlichen. Auch die Beratung zum Thema Parken mit Kfz-Kennzeichenerkennung wird über das Berichtsjahr hinaus fortgeführt werden.

9. Verkehrszählung von Hamburg Wasser

Verkehrszählungen, bei denen Kfz-Kennzeichen so verarbeitet werden, dass eine Personenbeziehbarkeit gegeben ist, müssen den datenschutzrechtlichen Vorgaben genügen, unter anderem im Hinblick auf Transparenz und Erfüllung der Informationspflichten. Der HmbBfDI hat im Fall einer solchen Erhebung im Vorfeld von Sielbaumaßnahmen den Verantwortlichen noch einmal sensibilisiert und angehalten, ihn rechtzeitig einzubeziehen.

Durch eine Presseberichterstattung im Hamburger Abendblatt Ende März 2022 ist der HmbBfDI auf eine 24-stündige Verkehrszählung im Alstertal (in der Wellingsbütteler Landstraße) aufmerksam geworden. Dazu hieß es dort: „... Verkehrszählung soll Klarheit über Wege der Fahrzeuge bringen. Dabei geht es nicht nur um eine reine Zählung der Fahrzeuge, sondern um die tatsächliche Auswertung der Wege, die Pkw, Lkw und Schwerlastverkehr nehmen. Dafür werden die Kennzeichen aller Autos erfasst, verschlüsselt und über alle Messpunkte hinweg abgeglichen. Die Stadt weist darauf hin, dass die Messung datenschutzkonform erfolge, die Kameras zeichneten Gesichter und Fußgänger nicht auf. ...“

Die gewählte Formulierung gab Anlass zu klären, ob die Tatsache, dass auch Kfz-Kennzeichen personenbezogene Daten sind, bei der konkreten Ausgestaltung der Verkehrszählung ausreichend Berücksichtigung gefunden hatte. Denn aus datenschutzrechtlicher Sicht geht es nicht allein um die Erfassung von Gesichtern oder Personen, sondern auch um die Art und Weise der Verarbeitung von personenbeziehbaren Kfz-Kennzeichen, gerade wenn auf dieser Basis nachvollzogen werden soll, welche Wege ein Kfz genommen hat.

Der HmbBfDI hat sich daher an den Verantwortlichen gewandt. Die Verkehrszählung sollte im Vorfeld von längerfristigen Sielbaumaßnahmen durchgeführt werden, um mit einem Verkehrskonzept

die daraus resultierenden Verkehrsbeeinträchtigungen reduzieren zu können. Verantwortlich zeichnete daher die für die Durchführung der Sielbauarbeiten zuständige Hamburger Stadtentwässerung Anstalt des öffentlichen Rechts (HSE). Die HSE hat dem HmbBfDI auf Anfrage die datenschutzrelevante Dokumentation zu der Verkehrserhebung im Alstertal zur Verfügung gestellt. Aus dieser ergab sich u.a., dass die im Rahmen der Verkehrszählung erhobenen Kfz-Kennzeichen vor der Weiterverarbeitung mit einer Hash-Funktion pseudonymisiert und auf einer verschlüsselten Datenbank des für die Verkehrserhebung eingesetzten Dienstleisters gespeichert wurden. Eine Speicherung der Kfz-Kennzeichen im Klartext hat nicht stattgefunden. Screenshots der Fahrzeuge in geringer Auflösung wurden allein zur Klassifizierung der Fahrzeugtypen erstellt. Eine Identifikation von in den Fahrzeugen sitzenden Personen war aufgrund der gewählten Auflösung nicht möglich. Die statistische Auswertung, die die HSE im Ergebnis bekommen sollte, sollte weder Kfz-Kennzeichen, noch Hashwerte oder Screenshots von Fahrzeugen enthalten.

Auch wenn diese und weitere ergriffene technische und organisatorische Maßnahmen in diesem Fall dazu geführt haben, dass es für Außenstehende nahezu unmöglich war, eine Zuordnung zu konkreten Personen vorzunehmen, blieb eine solche tatsächlich möglich. Daher musste auch den datenschutzrechtlichen Transparenzvorgaben und Informationspflichten Genüge getan werden, nicht zuletzt durch eine deutlich sichtbare und gut lesbare Hinweisbeschilderung vor Ort. Eine solche war, wie eine Begehung der Wellingsbütteler Landstraße am Tag der Verkehrszählung gezeigt hat, nur eingeschränkt vorhanden.

Für Erhebungen dieser Art stellt sich die grundsätzliche Frage, ob es möglich ist, diese in einer Art und Weise durchzuführen, dass eine Personenbeziehbarkeit der verarbeiteten Informationen komplett ausgeschlossen werden kann. Mit der HSE ist besprochen, dass der HmbBfDI bei Verkehrszählungen zukünftig bereits im Vorfeld einbezogen wird.

10. Auskünfte von Ärzten/Zahnärzten – aus der Fallpraxis

Zum Verhältnis zwischen dem Auskunftsrecht nach Art. 15 DSGVO und dem in § 630g BGB geregelten Recht auf Einsichtnahme in die Patientenakte hat der Bundesgerichtshof dem Europäischen Gerichtshof (EuGH) diverse Fragen vorgelegt (Beschluss vom 29. März 2022, VI ZR 1352/20). Die Antworten werden für die Beschwerden und Beratungsanfragen eine Rolle spielen, die der HmbBfDI regelmäßig zu diesem Themenkomplex erhält.

In seinem Tätigkeitsbericht Datenschutz 2018 hat der HmbBfDI einen Überblick gegeben über die meistgestellten Fragen zum Datenschutz in Arzt- und Zahnarztpraxen und über seine Antworten darauf (vgl. 27. TB, Kapitel V 5). Das waren Fragen zu Informationspflichten nach Art. 13 und 14 DSGVO, zum Erfordernis des Einholens einer Einwilligung durch die behandelnde Person für eine Übermittlung von Gesundheitsdaten der Patient:innen an Dritte, zu einer möglichen Behandlungsverweigerung wegen Nichtquittierens der Datenschutzinformationen oder Nichterteilung einer Einwilligungserklärung, zur Art und Weise der Übermittlung von Daten von Patient:innen und zur Notwendigkeit der Benennung einer/eines Datenschutzbeauftragten.

Vier Jahre später lässt sich mit Blick auf die beim HmbBfDI im Berichtsjahr eingegangenen Beschwerden und Beratungsanfragen feststellen, dass jene Fragen nicht an Aktualität verloren haben. Als typische weitere Fallkonstellationen hinzu kommen Eingaben zu nicht oder nicht vollständig erteilten Auskünften aus der Patientenakte sowie dazu, dass Arzt-/Zahnarztpraxen mit Blick auf die Regelung des § 630g Bürgerliches Gesetzbuch (BGB) zur Einsichtnahme in die Patientenakte zur Abholung von oder zur Erstattung von Kosten für Kopien aus einer Patientenakte auffordern. Dabei geht es also darum, inwieweit das Auskunftsrecht nach Art. 15 DSGVO

Beschränkungen erfährt durch das Recht auf Einsichtnahme in die Patientenakte nach § 630g BGB.

Dazu ist zunächst festzustellen, dass betroffenen Personen gegenüber Arzt-/Zahnarztpraxen ein Auskunftsrecht nach Art. 15 DSGVO zusteht. Gemäß Erwägungsgrund 63 zur DSGVO schließt Art. 15 DSGVO das Recht betroffener Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Nach Art. 15 Abs. 3 DSGVO stellt der Verantwortliche der betroffenen Person eine Kopie der personenbezogenen Daten zur Verfügung, die Gegenstand der Verarbeitung sind. Bei der Beantwortung von Auskunftsersuchen haben Arzt-/Zahnarztpraxen die Vorgaben des Art. 12 DSGVO zu beachten, wie die Monatsfrist des Art. 12 Abs. 3 DSGVO, innerhalb derer ein Auskunftsersuchen grundsätzlich beantwortet werden muss. Nach Artikel 12 Abs. 5 DSGVO ist jedenfalls die erste Auskunft unentgeltlich zur Verfügung zu stellen.

Dem Auskunftsrecht nach Art. 15 DSGVO steht die ältere Regelung des § 630g BGB gegenüber, wonach ein(e) Patient:in Einsicht nehmen kann in ihre bzw. seine vollständige Patientenakte. Gemäß Abs. 2 können auch elektronische Abschriften von der Patientenakte verlangt werden. Die entstandenen Kosten sind zu erstatten. Beschränkt werden kann das Einsichtsrecht nach § 630g Abs. 1 S. 1 BGB, soweit erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen.

Letzteres, die Rechte Dritter, finden auch im Rahmen von Art. 15 Abs. 4 DSGVO Berücksichtigung. Danach darf das Recht auf Erhalt einer Kopie gemäß Abs. 3 die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Eine Beschränkung erfährt das Auskunftsrecht nach Art. 15 DSGVO durch die Regelung des § 630g BGB auch insoweit, als über Art. 23 Abs. 1 lit. i) DSGVO zum Schutz der betroffenen Person – bei Vorliegen erheblicher therapeutischer Gründe im Sinne des

§ 630g BGB – unter Umständen keine bzw. keine vollständige Auskunft erteilt werden muss. Eine Beschränkung des datenschutzrechtlichen Auskunftsrechts durch die Regelung zur Kostentragung in § 630g Abs. 2 S. 2 BGB ist jedoch im Regelfall unzulässig. Das heißt, dass zumindest die erste Kopie im Sinne von Art. 15 Abs. 3 DSGVO grundsätzlich unentgeltlich zur Verfügung zu stellen ist.

Mit dieser und weiteren Fragen zu Reichweite und Ausnahmen des Auskunftsanspruchs nach Art. 15 DSGVO wird sich nun aber noch einmal der EuGH befassen. Insbesondere wird das Gericht etwas dazu sagen, wie es sich auswirkt, wenn die Kopie einer Patientenakte nicht angefordert wird, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können (Erwägungsgrund 63 S. 1), sondern aus datenschutzfremden, wenngleich legitimen Gründen. Auch der Umfang dessen, was als Kopie nach Art. 15 Abs. 3 S. 1 DSGVO aus einer Patientenakte herauszugeben ist, wird durch den EuGH festgelegt werden.

Die Antworten des EuGHs werden in die Beratungspraxis des HmbBfDI bzw. in das Vorgehen im Fall von Beschwerden einfließen.

11. Auskunftsansprüche bei Identitätsdiebstählen

Der HmbBfDI beobachtet einen spürbaren Anstieg von Identitätsdiebstählen im Internet. Zur Stärkung der Betroffenenrechte unterstützt er diese bei der Durchsetzung ihrer Auskunftsrechte auch in Bezug auf Daten, die vermeintlich den Täter:innen zuzuordnen sind.

Bei einem Identitätsdiebstahl können den betroffenen Personen leicht hohe Schäden entstehen. Häufig werden dafür persönliche Daten, wie zum Beispiel Name, Geburtsdatum, Anschrift, E-Mail-Adresse und Kontodaten, benutzt, um sich auf fremde Kosten bei Online-Diensten anzumelden oder Verträge abzuschließen. Derarti-

ge Fälle werden dem HmbBfDI regelmäßig zugetragen. In einem Fall, der den HmbBfDI Anfang 2022 erreichte, teilte eine betroffene Person mit, dass eine unbekannte Person ihre Identität zur Teilnahme an einem Online-Glücksspiel genutzt habe. Hierfür sei unter Verwendung des Namens und der Anschrift des Betroffenen ein Nutzerkonto bei der verantwortlichen Stelle angelegt worden.

In der Folge richtete die betroffene Person einen Auskunftsanspruch gem. Art. 15 DSGVO an den Verantwortlichen, den Veranstalter des Glücksspiels, um mehr über die verarbeiteten Daten und ggf. die Täter:innen zu erfahren. Die verantwortliche Stelle hatte eine Auskunft bis zum Einschreiten des HmbBfDI noch nicht erteilt und die betroffene Person an die „zuständigen Ermittlungsbehörden" (Polizei und Staatsanwaltschaft) verwiesen. Problematisch war zudem, ob der Auskunftsanspruch auch solche Daten umfasst, die zunächst den Täter:innen zugeordnet werden konnten.

Nach Kontaktaufnahme durch den HmbBfDI wurde zunächst eine Auskunft durch den Verantwortlichen zugesichert, welche aber keine Täter:innendaten enthalten sollte. Im Rahmen einer telefonischen Rücksprache konnte der HmbBfDI die rechtliche Vertretung der verantwortlichen Stelle dazu bewegen, dass auch die mit dem Account in Verbindung stehenden Daten der Täter:innen herauszugeben waren.

Der Auskunftsanspruch nach Art. 15 Abs.1 DSGVO beschränkt sich dem Wortlaut nach auf personenbezogene Daten, die die Auskunft verlangenden Betroffenen betreffen. Im zu Grunde liegenden Fall ging der Verantwortliche rechtsirrtümlich davon aus, einen (weiteren) Datenschutzverstoß zu begehen, wenn er Auskunft über Täter:innendaten erteilen würde. Unklar sei, welcher betroffenen Person welche Daten (z.B. Informationen über verwendete Kreditkarten, IP-Adressen oder die getätigten Spiele) zuzuordnen waren und ob der Auskunftsanspruch sämtliche umfasse.

Art. 15 DSGVO bildet zusammen mit den Art. 13 und Art. 14 DSGVO die Grundlage für die weitere Ausübung von Betroffenenrechten und

ggf. auch anderer Rechtsmittel. Der Verantwortliche hat im Fall eines Auskunftsantrags keine Entscheidungsfreiheit darüber, inwieweit eine Auskunft sinnvoll oder zweckmäßig ist. Sofern die rechtlichen Voraussetzungen für die Auskunftserteilung vorliegen, ist diese zwingend und vollumfänglich zu erteilen.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Bezogen auf die Herausgabe von Täter:innendaten, die dem Benutzerkonto zugeordnet werden können, besteht nach Auffassung des HmbBfDI grundsätzlich eine – zumindest mittelbare – Verbindung zwischen den verarbeiteten Daten und den geschädigten betroffenen Personen, da deren Identität für eine Datenverarbeitung von vermeintlichen Straftäter:innen missbraucht wurde. Die hierbei verarbeiteten Daten stehen inhaltlich in direktem Zusammenhang mit der begangenen Straftat und können Rechtsfolgen wie z.B. Zahlungsansprüche gegenüber den geschädigten betroffenen Personen auslösen. Die Interessen der Täter:innen sind auch nicht im Rahmen des Art. 15 Abs. 4 DSGVO zu berücksichtigen, weil sie aufgrund des deliktischen Verhaltens nicht schutzwürdig sind. Insofern ist es rechtmäßig, eine vollumfängliche Beauskunftung im Sinne des Art. 15 DSGVO zur Vorbereitung weiterer Rechtsmittel zu ermöglichen, um die Interessen der Geschädigten zu wahren. Dieser bereits langjährig angewandten Position des HmbBfDI hat sich nun auch der Europäische Datenschutzausschuss angeschlossen (EDSA Guidelines 01/2022 on data subject rights – Right of access vom 18.1.2022, S. 2; in der öffentlichen Konsultationsversion, S. 34).

12. Drittes Geschlecht in Kundendatenbanken

Der Grundsatz der Richtigkeit erfordert, dass Unternehmen Angaben zum Geschlecht, die im Zusammenhang mit der Erfüllung eines Vertra ges oder für vorvertragliche Maßnahmen von Personen erhoben werden, korrekt verarbeitet werden können. „Korrekt" meint den Eintragungs möglichkeiten nach dem Personenstandsgesetz entsprechend: weiblich, männlich, divers, keine Angabe.

Im Zusammenhang mit einer Beschwerde, die beim HmbBfDI im Berichtsjahr eingelegt wurde, weil ein Energieversorger mit Sitz in Hamburg eine Auskunft nach Art. 15 DSGVO nicht erteilt hatte, hat der HmbBfDI gegenüber dem Unternehmen die richtige Verarbeitung von Angaben zum Geschlecht thematisiert. Entsprechende Informationen verarbeitet jener Versorger von allen Personen, die mit ihm einen Vertrag abschließen wollen.

Zu dieser Thematik hat es in der jüngeren Vergangenheit zivilgerichtliche Entscheidungen gegeben, unter anderem von den Oberlandesgerichten (OLG) Karlsruhe und Frankfurt (OLG Karlsruhe, Urteil vom 14. Dezember 2021, Az. 24 U19/21 und OLG Frankfurt, Urteil vom 21. Juni 2022, Az. 9 U 92/20). Diese lassen sich zurückführen auf eine Entscheidung des Bundesverfassungsgerichts (BVerfG) aus dem Jahr 2017 (BVerfG, Beschluss vom 10. Oktober 2017, BvR 2019/16). Das BVerfG hatte eine Verletzung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (geschlechtliche Identität) und einen Verstoß gegen das Diskriminierungsverbot des Art. 3 Abs. 3 S. 1 Grundgesetz darin gesehen, dass Personen, die sich dauerhaft weder dem männlichen noch dem weiblichen Geschlecht zuordnen lassen, durch das Personenstandsrecht dazu gezwungen wurden, das Geschlecht registrieren zu lassen, es aber keinen anderen positiven Geschlechtseintrag gab als weiblich oder männlich. In der Folge ist das Personenstandsgesetz

(PStG) Ende 2018 geändert worden. Neben der Möglichkeit, eine Zuordnung weder zum weiblichen noch zum männlichen Geschlecht vorzunehmen, besteht seitdem auch die Option des Eintrags mit der positiven Angabe „divers“, § 22 Abs. 3 PStG.

Die OLG Karlsruhe und Frankfurt haben sich mit der Ausgestaltung von Onlineshops, der alleinigen Möglichkeit der Registrierung unter Angabe der Anrede „Frau“ oder „Herr“, einer damit einhergehenden Benachteiligung im Sinne des Allgemeinen Gleichbehandlungsgesetzes und daraus resultierenden Unterlassungs- sowie Schmerzensgeldansprüchen befasst. Der Beschluss des BVerfG aus 2017 und § 22 Abs. 3 PStG in der aktuellen Fassung haben aber auch Auswirkungen auf die Datenverarbeitung. Wenn Unternehmen auf die Erhebung des Geschlechts von Personen, zu denen sie in vorvertraglicher oder vertraglicher Beziehung stehen, nicht komplett verzichten wollen, dann muss ihnen die korrekte Verarbeitung der Informationen dazu möglich sein. Denn gemäß Art. 5 Abs. 1 lit. d) DSGVO müssen personenbezogene Daten sachlich richtig sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (Grundsatz der „Richtigkeit“).

Der Energieversorger aus Hamburg hat, veranlasst durch das Tätigwerden des HmbBfDI, sein Webformular für Vertragsanfragen überarbeitet und die notwendige Anpassung im dahinter liegenden Customer Management System in die Wege geleitet.

13. Elektronische Auskunft im Versandhandel

Auskunftsersuchen, die in elektronischer Form gestellt werden, sind regelmäßig nicht postalisch, sondern in elektronischer Form zu beantworten, wobei stets die Anforderungen an die Sicherheit dieser Datenübermittlung erfüllt werden müssen. Durch das Tätigwerden des HmbBfDI hat ein Hamburger Versandhandelsunternehmen den Prozess der Auskunftserteilung dergestalt verändert, dass Auskünfte nach Art. 15 DSGVO nunmehr auch in elektronischem Format aus dem Kundenkonto heraus abgerufen werden können.

Anträge auf Auskunft nach Art. 15 DSGVO werden heutzutage regelmäßig in elektronischer Form an die jeweiligen Verantwortlichen gestellt, beispielsweise über ein Kontaktformular oder per E-Mail. Aus Art. 12 Abs. 3 und Art. 15 Abs. 3 DSGVO ergibt sich, dass bei solchen elektronisch gestellten Anträgen die daraufhin zu erteilenden Auskünfte in einem gängigen elektronischen Format an die antragstellende Person zur Verfügung zu stellen sind, sofern dies den jeweiligen Verantwortlichen möglich ist. Diese Vorgabe stellt eine Präzisierung des in Art. 12 Abs. 1 DSGVO genannten Grundsatzes dar, dass sämtliche zu erteilenden Informationen in leicht zugänglicher Form zu übermitteln sind. Auch der Europäische Datenschutzausschuss (EDSA) legte sich im Januar 2022 mit einer veröffentlichten Guideline zum Recht auf Datenzugang auf diese Rechtsauffassung fest.

Diese Vorgabe stellt insbesondere solche Verantwortliche häufig vor Herausforderungen, die umfangreiche Bestände personenbezogener Daten verarbeiten. In der Regel liegen zwar sämtliche über eine betroffene Person vorliegenden personenbezogenen Daten in elektronischer Form vor und können in einem gängigen elektronischen Format abgespeichert werden, beispielsweise als PDF-Datei. Es besteht allerdings Unsicherheit bezüglich der Frage, wie diese Datei auf elek-

tronischem Wege an die antragsstellende Person übermittelt werden kann. Die zweifellos einfachste Lösung ist hierbei der Versand per E-Mail. Hierbei ist jedoch zu beachten, dass Verantwortliche verpflichtet sind, durch geeignete Maßnahmen sicherzustellen, dass die in der Auskunft enthaltenen Daten nicht an Dritte gelangen. Dies ergibt sich aus dem Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO) in Verbindung mit den Anforderungen an die Sicherheit der Verarbeitung (Art. 32 DSGVO). Um diese Pflicht in der konkreten Fallgestaltung umzusetzen, muss einerseits der Transportweg gegen Zugriffe Dritter hinreichend gesichert sein, andererseits muss auch die Identität der Person verifiziert werden, die den Antrag stellt bzw. Empfänger:in der erteilten Auskunft ist. Beides ist bei einem Versand per E-Mail nur bedingt möglich oder gestaltet sich technisch anspruchsvoll. Die Anforderungen an diese Maßnahmen sind zudem umso höher, je sensibler die enthaltenen Daten sind. Dabei werden nicht nur besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO – wie beispielsweise Gesundheitsdaten – als sensibel eingestuft, sondern auch große Datenmengen.

Gerade bei großen Versandhandelsunternehmen sind nicht nur personenbezogene Daten der Kunden wie Name, Anschrift, Geburtsdatum, E-Mail-Adresse und Telefonnummer gespeichert. Aufgrund der ebenfalls von der Auskunft umfassten Bestellhistorie liegen möglicherweise auch Daten vor, die geeignet sind, Rückschlüsse auf private Interessen und Lebensumstände zu erlauben. Es bestehen in diesen Fällen daher erhebliche datenschutzrechtliche Bedenken, eine derart umfangreiche elektronische Auskunft und damit eine potentiell sehr detailreiche Zusammenstellung personenbezogener Daten per E-Mail zu versenden. Eine Ende-zu-Ende-Verschlüsselung der E-Mail würde den Anforderungen an die Sicherheit zwar genügen, allerdings ist dieses Verfahren nach Erfahrungen des HmbBfDI selbst für technisch versierte Personen nicht trivial. Die sich ergänzend aus Art. 12 Abs. 1 Satz 1 DSGVO ergebende Anforderung, dass u.a. Auskünfte nach Art. 15 DSGVO in leicht zugänglicher Form zu übermitteln sind, wäre mit dieser Lösung daher nicht erfüllt.

Als Ergebnis kommen Verantwortliche in einigen Fällen zu dem Ergebnis, dass die beiden Anforderungen nicht miteinander zu vereinen sind und ihnen das Erteilen einer elektronischen Auskunft aufgrund der zu beachtenden Sicherheitsanforderungen daher nicht möglich ist. In der Folge verzichten sie auf das Erteilen einer elektronischen Auskunft und erteilen die Auskunft lediglich postalisch in Papierform. Ein verschlossener Brief ist durch das Postgeheimnis geschützt und wird an eine von der antragstellenden Person selbst gewählte postalische Anschrift zugestellt. Sowohl die Sicherheit des Transportweges als auch die Verifikation der Identität der Person lässt sich damit sicherstellen, zudem bestehen keine technischen Hürden bei der Beantragung oder der Beauskunftung.

Den HmbBfDI erreichte zu diesem Thema die Beschwerde einer betroffenen Person über einen deutschlandweiten Marktführer im Bereich Versandhandel. Trotz der ausdrücklich geforderten elektronischen Auskunft erhielt die betroffene Person lediglich eine Auskunft auf dem Postweg sowie die Information, dass eine elektronische Beauskunftung nicht möglich sei. Nach Herantreten des HmbBfDI kam es zunächst zu einem gegenseitigen Austausch von Rechtsansichten mit dem Unternehmen. Dabei vertrat der HmbBfDI die Ansicht, dass gerade große Unternehmen, die zudem erhebliche Mengen personenbezogener Daten verarbeiten, trotz der bestehenden Schwierigkeiten Möglichkeiten zu schaffen haben, Auskünfte in elektronischer Form erteilen zu können. Auch wenn hiermit gegebenenfalls finanzielle Investitionen verbunden sind, sei dies angesichts der Art und des Umfangs der verarbeiteten Daten sowie der in der DSGVO normierten Pflicht zur Erteilung elektronischer Auskünfte erforderlich.

Aufgrund der Kooperationsbereitschaft des Unternehmens konnte der HmbBfDI auch ohne den Erlass einer förmlichen Maßnahme erreichen, dass dieses Unternehmen als Folge dieses Austausches umfangreiche Vorkehrungen getroffen hat, um eine elektronische Beauskunftung zu ermöglichen. Ein entsprechender Antrag kann nunmehr im Kund:innenkonto gestellt werden. Die beantragte Aus-

kunft wird sodann als PDF-Datei zum Download im Kund:innenkonto zur Verfügung gestellt. Mit dieser Lösung können sämtliche gesetzlichen Anforderungen erfüllt werden. Einerseits wird der Versand von umfangreichen Datensammlungen per E-Mail vermieden, andererseits kann durch geeignete Login-Maßnahmen auch sichergestellt werden, dass nur die jeweiligen Kontoinhaber:innen auf die Daten zugreifen können. Da grundsätzlich die bestehende Infrastruktur des Kund:innenkontos verwendet wird, ist der Abruf der elektronischen Auskunft auch hinreichend leicht zugänglich. Darüber hinaus bleibt weiterhin die Möglichkeit für Kund:innen bestehen, ein Auskunftsersuchen per E-Mail oder postalisch an das Unternehmen zu richten, so dass mit der Neuerung keine Einschränkungen verbunden sind. Der HmbBfDI hält diese Lösung daher für gelungen.

14. Maklerfragebögen für Wohnungsinteressent:innen

Im Bereich der Wohnungswirtschaft ist die Datenerhebung von Mietin teressent:innen ein datenschutzrechtlicher Dauerbrenner. Im Rahmen einer Prüfaktion nimmt der HmbBfDI daher die Praxis der Datenverar beitungen von Maklern systematisch unter die Lupe.

Der Wohnungsmarkt in Hamburg ist bekanntermaßen erheblich angespannt. Wohnungssuchende haben große Schwierigkeiten, eine Mietwohnung zu finden. Oftmals stellt schon die Vereinbarung von Besichtigungsterminen für Mietbewerber:innen eine Herausforderung dar.

Der HmbBfDI erhält regelmäßig Anfragen, Hinweise und Beschwerden von Betroffenen, die die Einholung von Selbstauskünften der sich bewerbenden Mietinteressent:innen betreffen. Dabei geht es um die Frage, welche Informationen bei den Wohnungssuchenden abgefragt werden dürfen, zu welchem Zeitpunkt welche Auskünfte

bei wem eingeholt und welche Nachweise von den Bewerber:innen angefordert werden dürfen. Moniert wird häufig, dass mehr Daten abgefragt werden, als zum Zeitpunkt der Bewerbung um eine Wohnung erforderlich sind.

Vor diesem Hintergrund hat der HmbBfDI eine Prüfaktion bei Hamburger Immobilienmaklern zur Einhaltung der datenschutzrechtlichen Anforderungen bei der Datenerhebung von Mietinteressent:innen bei der Anbahnung von Wohnraummietverhältnissen und insbesondere zu den dabei von Mietbewerber:innen eingeholten Selbstauskünften eingeleitet.

Während der Corona-Pandemie war es zeitweise nachvollziehbar, dass Besichtigungstermine auf das unbedingt notwendige Minimum zu reduzieren waren und deshalb eine intensive Auswahl bereits im Vorfeld notwendig war. Dieses Argument ist mittlerweile weggefallen, sodass der HmbBfDI wieder zu den etablierten rechtlichen Maßstäben zurückkehrt. Die Anforderungen für die datenschutzgerechte Erhebung von Daten von Personen, die sich um eine Mietwohnung bemühen, sind in der „Orientierunghilfe zur Einholung von Selbstauskünften bei Mietinteressent:innnen" niedergelegt, die von der Datenschutzkonfererenz (DSK), dem gemeinsamen Gremium der Datenschutzaufsichtsbehörden des Bundes und der Länder, im Jahr 2018 veröffentlicht wurde. Danach sind bei der Anbahnung eines Wohnraummietverhältnisses drei Phasen zu unterscheiden, in denen zulässigerweise Daten von Mietinteressent:innen verlangt und verarbeitet werden dürfen.

Zum Zeitpunkt der Kontaktaufnahme und der Vereinbarung eines Besichtigungstermins ist es nicht erforderlich, dass Informationen zu Einkommen oder Bonität mitgeteilt werden. Diese Informationen dürfen erst erhoben werden, wenn nach der Besichtigung das Interesse der betroffenen Person, die Wohnung anzumieten, tatsächlich besteht.

Einkommensnachweise dürfen in der Regel erst verlangt werden, wenn ein beiderseitiges Interesse an der Anbahnung eines Miet-

verhältnisses besteht und der Vermieter sich für einen bestimmten Mietinteressenten entscheidet.

Im Rahmen der Prüfaktion fordert der HmbBfDI insbesondere die von Wohnungsmaklern verwendeten Selbstauskunftsformulare an, die von Mietinteressent:innen ausgefüllt werden sollen. Er überprüft sie auf Vereinbarkeit mit den in der Orientierungshilfe dargelegten Anforderungen und wird im Fall datenschutzwidriger Verarbeitungen von den ihm nach der DSGVO zur Verfügung stehenden Befugnissen Gebrauch machen.

15. Privatanschriften im Amtlichen Anzeiger

Durch einen Programmierfehler waren Wohnanschriften der meisten Kandidat:innen zu Wahlen im Internet frei abrufbar. Diese Sicherheitslücke wurde geschlossen.

Wer für die Wahl zum Deutschen Bundestag oder einer Bezirksversammlung kandidiert, dessen Namen und Anschrift werden im Amtlichen Anzeiger der Freien und Hansestadt Hamburg veröffentlicht. Die Herstellung der Printexemplare führt eine privatwirtschaftliche Druckerei aus. Diese übernimmt auch die Onlineveröffentlichung unter www.luewu.de/anzeiger in eigener datenschutzrechtlicher Verantwortlichkeit.

Dieses Vorgehen ist gesetzlich vorgeschrieben. In den Rechtsgrundlagen wird dabei zwischen der gedruckten Variante und der Onlineversion unterschieden. Bei Bundestagswahlen sind die Anschriften der Kandidat:innen in der Papierform zu veröffentlichen (§§ 34 Abs. 1 Satz 2 Nr. 1, 38 Satz 3, 39 Abs. 1 Satz 1 Nr. 2, 86 Abs. 1 BWO), während online nur Wohnort zu nennen ist, nicht aber Straße und Hausnummer (§ 86 Abs. 3 S. 3 BWO) Bei Bezirkswahlen müssen die Anschriften ebenfalls im allgemeinen Anzeiger abge-

druckt werden (§ 21 Abs. 1 S. 2 BezVWG), sind aber im Internet nach 6 Monaten zu löschen (§ 32a Abs. 1 BezWO). Die Anschriften der Kandidat:innen für die Wahl zur Hamburgischen Bürgerschaft sind weder online noch offline zu veröffentlichen. Allerdings stehen Kandidat:innen für die Bürgerschaft oftmals auch zur Wahl für die anderen beiden Gremien, sodass sich die Kontaktdaten der Bürgerschaftsabgeordneten vielfach aus diesem Grund im Amtlichen Anzeiger befinden.

Diese Differenzierungen werden in der Praxis dadurch umgesetzt, dass der Verlag die Adressangaben in den betreffenden PDF-Seiten des Onlineangebots schwärzt. Internetnutzer:innen können so den PDF-Dokumenten entnehmen, wer zur Wahl antritt, ohne die private Wohnanschrift zu lesen zu bekommen. Durch den Hinweis eines Bürgers wurde der HmbBfDI jedoch darauf aufmerksam gemacht, dass es dennoch möglich war, die Straßen und Hausnummern anzuzeigen. Bei Nutzung der Suchfunktion des Onlinearchivs wurden Vorschauansichten mit Auszügen der Seiten des Anzeigers generiert, die den Suchbegriff enthielten. Diese Seitenauszüge waren ungeschwärzt. Gab man also zum Beispiel die Namen beliebiger Abgeordneter oder Kandidat:innen ein, so wurde in der Vorschauansicht die vollständige Postanschrift wiedergegeben. Beim Klick auf die Vorschau öffnete sich die betreffende Seite des amtlichen Anzeigers, auf der diese Daten wiederum geschwärzt waren.

Überwiegend handelt es sich bei den Adressdaten im Amtlichen Anzeiger um die Privatanschrift. Nach den Recherchen des HmbBfDI wurden nur in Einzelfällen das Wahlkreisbüro oder eine Parteianschrift verwendet. Vor dem Hintergrund medialer Berichte über bundesweite Angriffe oder Drohungen gegenüber Politiker:innen sind Kanditat:innen zu Wahlen sowie deren Familien besonderen Gefahren ausgesetzt. Eine einfach abrufbare Liste mit Wohnanschriften birgt hohes Missbrauchspotenzial. Die Bundes- und Landesgesetzgeber sind dem bewusst begegnet, indem sie die Onlineveröffentlichungen der Anzeiger stark eingeschränkt haben.

Nach einer Beweissicherung hat der HmbBfDI den Verlag kontaktiert. Auf sein Betreiben hin hat dieser schnell reagiert. Als Sofortlösung hat er die Suchfunktion über Dokumente des Amtlichen Anzeigers vollständig von der Internetseite entfernt. Für eine dauerhafte Lösung hat er eine externe Firma damit beauftragt, die Adressdaten aus den PDF-Dokumenten rückstandslos zu entfernen. Bei einer Nachkontrolle der Internetseite im Dezember 2022 stellte der HmbBfDI fest, dass die Suchfunktion wieder aktiviert war, ohne dass die Dateien bereinigt gewesen waren. Auf seine Aufforderung hin deaktivierte der Verlag die Suche erneut. Als Grund dafür, die Sicherheitslücke wieder geöffnet zu haben, gab er eine versehentliche Reaktivierung infolge von Wartungsarbeiten an. Er kündigte an, die bereinigten PDF-Dateien Ende Januar zu veröffentlichen, sodass dann auch die Suchfunktion wieder genutzt werden könne.

Aufgrund der kooperativen Reaktion wurde von einer Sanktion zunächst abgesehen. Auch wurde berücksichtigt, dass die ungeschwärzten Informationen in der Printversion für die Allgemeinheit verfügbar sind. Der HmbBfDI wird die weitere Umsetzung kontrollieren.

BERICHTE III.

III. Einzelfälle

1. Verfassungsbeschwerde gegen § 49 PolDVG

Der HmbBfDI wurde im Rahmen einer Verfassungsbeschwerde gegen die Norm § 49 PolDVG als Sachverständiger Dritter vom Bundesverfassungsgericht zur Abgabe einer Stellungnahme auf gefordert und zur mündlichen Verhandlung geladen. Der HmbBfDI hat beide Gelegenheiten zur Äußerung wahrgenommen und auf datenschutzrechtliche Bedenken gegen die Norm, auch im Gefü ge der polizeilichen Praxis in Hamburg, aufmerksam gemacht, die das BVerfG in der Entscheidung vom 16.2.2023 weitgehend teilte.

Im Rahmen der umfassenden Novellierung des PolDVG im Jahr 2019 hat der Hamburgische Gesetzgeber den § 49 PolDVG – der der Hessischen Norm § 25a SOG nachempfunden ist – neu eingeführt. Bei beiden Regelungen handelt es sich um landesgesetzliche Ermächtigungen der Polizei zur Auswertung von Daten mittels einer automatisierten Anwendung. § 49 PolDVG lautet wie folgt:

> (1) Die Polizei darf in begründeten Einzelfällen in polizeilichen Dateisystemen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenauswertung verarbeiten, wenn dies zur vorbeugenden Bekämpfung von in § 100a Absatz 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist.
>
> (2) Im Rahmen der Verarbeitung nach Absatz 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu

bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(3) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung nach Absatz 1 erfolgen durch Anordnung der Polizeipräsidentin oder des Polizeipräsidenten oder der Vertretung im Amt. Die oder der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen.

Nach den Äußerungen des Senats der Freien und Hansestadt Hamburg sind – anders als in Hessen – bisher keine Daten auf Basis von § 49 PolDVG verarbeitet worden. Dies könnte sich zukünftig im Hinblick auf das Bund-Länder-Vorhaben „Polizei 2020" ergeben. Im Rahmen dieses Projektes, durch das das polizeiliche Informationswesen in Bund und Ländern neu aufgestellt werden soll, wurde bereits federführend durch das Bayerische Landeskriminalamt der Zuschlag an das Unternehmen Palantir Technologies GmbH (deutsche Tochter des US-Datenunternehmens „Palantir") für ein neues Verfahrensübergreifendes Recherche- und Analysesystem" (VeRa) erteilt. Das Ziel sei, die Analysefähigkeit der Polizei zur Bekämpfung von Kriminalität und Terrorismus erfolgreicher und schneller zu machen. Auf Grundlage des geschlossenen Rahmenvertrags und ohne ein zusätzliches Vergabeverfahren können andere Länder und der Bund dieses Analysesystem nutzen. Nach eigenen Angaben hat die Polizei Hamburg Bereitschaft zur Mitwirkung an dem Vorhaben erklärt (Bü.-Drs. 22/1758, S. 1). Ein Einsatz in Hamburg käme wohl auf der Grundlage des hier gegenständlichen § 49 PolDVG in Betracht. Die Polizei hat ihr Interesse an VeRA bekundet (vgl. Bü.-Drs. 22/5324, S. 5), aber noch keine Entscheidung getroffen (vgl. Bü.-Drs. 22/7701).

Sowohl gegen § 49 PolDVG als auch gegen die Hessische Norm wurden am 20. Dezember 2022 Verfassungsbeschwerden beim Bundesverfassungsgericht (Az.: 1 BvR 2634/20 und 1 BvR 1547/19) ver-

handelt. Die Beschwerdeführenden machten in Karlsruhe insbesondere geltend, dass die Normen eine Rechtsgrundlage schafften, um bei Vorliegen der gesetzlichen Voraussetzungen eine softwaregestützte Auswertung polizeilicher bzw. der für die Polizei verfügbaren Datenbestände vornehmen zu können. Hierin liege ein intensiver und nicht gerechtfertigter Grundrechtseingriff, da die Befugnisse die Auswertung umfangreicher Datenbestände unter Nutzung komplexer informationstechnischer Programme gestatteten, ohne hierfür dem Grundrechtsschutz genügende Anforderungen vorzusehen.

Der HmbBfDI hat auf seine datenschutzrechtlichen Bedenken gegen die Norm bereits im Rahmen des Gesetzgebungsverfahrens und wiederholt im Innenausschuss der Hamburgischen Bürgerschaft aufmerksam gemacht (vgl. z.B. Protokoll des Innenausschusses der Hamburgischen Bürgerschaft Nr. 21/39, insb. S. 5). Sowohl in der schriftlichen Stellungnahme als auch im Rahmen der mündlichen Verhandlung vor dem BVerfG hat der HmbBfDI die rechtlichen Bedenken der Beschwerdeführenden an der Norm im Wesentlichen geteilt.

§ 49 PolDVG weist nach den Grundsätzen der Rechtsprechung des BVerfG eine hohe Eingriffsintensität auf. Zunächst sieht die Norm auf Rechtsfolgenseite die nunmehr gemeinsame Weiterverarbeitung von vormals getrennt genutzten und zu verschiedenen Zwecken erfassten personenbezogenen Daten vor. Völlig ungeklärt und problematisch ist dabei insbesondere das Verhältnis zu Daten aus den sog. Vorgangsbearbeitungssystemen. Diese sollen ausschließlich der Dokumentation polizeilichen Handelns dienen und werden ausdrücklich nicht für die spätere Verwendung zu gefahrenabwehrrechtlichen und/oder ermittlungsrechtlichen Zwecken errichtet. Im Hinblick auf die datenschutzrechtlichen Grundsätze zur Zweckänderung und hypothetischen Datenneuerhebung erscheint dies grundrechtlich höchst bedenklich.

Ferner erlaubt der weite Wortlaut der Norm komplexe – ggf. intelligente – Analysen der Dateisysteme, ohne gleichzeitig dafür angemessen hohe Eingriffsschwellen festzulegen. Eine besondere Beschränkung der Methodik der Verarbeitung ist in § 49 PolDVG

nicht ersichtlich. Soweit die Polizei in Hessen von komplexen Auswertungsmethoden gegenwärtig keinen Gebrauch macht und die Polizei Hamburg nach eigener Aussage lediglich ein System avisiert, das die Abfrage mehrerer Dateisysteme in einer Abfragemaske und eine händische Auswertung dieser gesammelten Erkenntnisse durch die Polizei erlaube, spiegelt die dafür durch die Bürgerschaft beschlossene Norm diesen beschränkten Anwendungsbereich jedenfalls nicht wider. Aus welchem Grund die Normen in dieser Frage nicht begrenzter sind, konnten die in Karlsruhe anwesenden Vertreter der Stadt Hamburg oder des Landes Hessen dem verhandelnden Senat allerdings nicht beantworten.

Im Rahmen der mündlichen Verhandlung hat der HmbBfDI zudem auch die Gelegenheit genutzt, darauf aufmerksam zu machen, wie die momentane polizeiliche Praxis in die Nutzung des § 49 PolDVG hineinspielen würde. Ein Augenmerk wurde insbesondere auch auf die Prüfungsergebnisse des HmbBfDI bei den heimlichen und besonders eingriffsintensiven Maßnahmen gelenkt (vgl. II 1). Mangels Protokollierung nach § 64 PolDVG und Kennzeichnung nach § 65 PolDVG erscheint die tatsächliche Einhaltung der Grundsätze der Zweckbindung bei einem Einsatz von § 49 PolDVG mehr als fraglich, eigentlich als bereits technisch unmöglich.

Die Entscheidung des Bundesverfassungsgerichts fiel per Urteil vom 16.02.2023. § 49 Abs. 1 Alt. 1 PolDVG verstößt gegen das allgemeine Persönlichkeitsrecht in seiner Ausprägung als informationelle Selbstbestimmung und wurde daher für nichtig erklärt.

Informationelle Selbstbestimmung und legitime Sicherheitsinteressen sind nun bei der Neufassung durch den Gesetzgeber in Einklang zu bringen. Das Urteil des Bundesverfassungsgerichtsmacht hierfür umfangreiche Vorgaben. Die durch neue Datenauswertungstechnologien möglichen schweren Grundrechtseingriffe dürfen nur aufgrund eindeutiger rechtlicher Grundlagen erfolgen. Der HmbBfDI begrüßt das Urteil (vgl. im Einzelnen auch die Pressemitteilung des HmbBfDI vom 16.2.2023).

Dies könnte als Anlass für eine umfassendere Reform des Datenschutzrechts im Hamburger Gefahrenabwehrrecht genommen werden. So zeigt sich das PolDVG an einigen Stellen bereits nach wenigen Jahren als veraltet (vgl. beispielsweise § 27 Abs. 5 PolDVG, dessen dynamische Verweisung durch Änderung des TKG völlig leer läuft) und in anderen Bereichen als in dieser Form dysfunktional (vgl. § 64 PolDVG, der sich inhaltlich zu nah an § 63 PolDVG orientiert, obwohl die zu protokollierenden Vorgänge gänzlich anderer Natur sind). Weitere Normen erscheinen verfassungsrechtlich jedenfalls grenzwertig (bspw. § 78 Abs. 1 PolDVG mit einer unbefristeten Übergangsregelung hinsichtlich der Übermittlung personenbezogener Daten ohne hinreichende Kennzeichnung). Hinzu kommen verfassungsrechtliche Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 9.12.22 zum Polizeirecht im Mecklenburg-Vorpommern, die jedenfalls teilweise auch Auswirkungen auf die Beurteilung des Hamburgischen Rechts haben dürften. Zudem ist wegen der nur eingeschränkten Aufsichtsbefugnisse des HmbBfDI gegenüber der Polizei Hamburg ein Vertragsverletzungsverfahren der Europäischen Kommission anhängig. Die gesamte Regelungs- und Verweisstruktur des PolDVG warf zudem während der mündlichen Verhandlung vor dem Bundesverfassungsgericht immer wieder schwer zu klärende Fragen auf, die durch Klarstellungen aufgelöst werden könnten und müssten.

2. Gesetzesänderung HmbDSG zum TTDSG

Die Bürgerschaft hat die Kompetenzen des HmbBfDI bei der Anwendung des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) erweitert. Damit wird der HmbBfDI in die Lage versetzt, Abhilfemaßnahmen und ggf. Bußgelder gegenüber Telemedienanbietern in Hamburg zu erlassen.

Das Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) ist am 1.12.2021 in Kraft getreten. Darin gebündelt wurden diverse datenschutzspezifische Vorschriften, die zuvor u. a. im Telekommunikationsgesetz (TKG) enthalten waren. Das TTDSG setzt mit § 25 TTDSG vor allem aber auch erstmalig Vorgaben aus der Datenschutzrichtlinie für elektronische Kommunikation (sog. ePrivacy-Richtlinie) um. Der Bundesgesetzgeber hatte es bis zum Inkrafttreten des TTDSG versäumt, die Nachschärfungen der ePrivacy-Richtlinie aus 2009 bzgl. der grundsätzlichen Einwilligungsbedürftigkeit von Cookies und ähnlichen Technologien in deutsches Recht umzusetzen. Die vormaligen Regelungen im Telemediengesetz (TMG, dort §§ 12 ff.), die mit Inkrafttreten des TTDSG entfallen sind, stellten keine europarechtskonforme Umsetzung dieser Vorgaben der ePrivacy-Richtlinie dar.)

Das TTDSG enthält selbst keine eigenständigen Regelungen über die Aufsicht im Bereich privatwirtschaftlicher Telemedien. Vielmehr bleibt die Aufsicht durch die nach Landesrecht zuständigen Behörden und § 40 des Bundesdatenschutzgesetzes (BDSG) unberührt.

Das TTDSG schafft Kompetenzen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI): So ordnet § 29 Abs. 2 TTDSG die Überwachung der Einhaltung des § 25 TTDSG bei öffentlichen Stellen des Bundes und Anbietern von Telekommunika-

tionsdiensten dem BfDI zu. Ferner bestimmt § 28 Abs. 3 Nr. 2 TTDSG, dass der BfDI im Fall von Verstößen gegen § 25 Abs. 1 Satz 1 TTDSG Bußgelder für Ordnungswidrigkeiten verhängen kann. Das TTDSG gleicht ferner die Untersuchungs- und Abhilfebefugnisse des BfDI im Hinblick auf Sachverhalte des TTDSG an seine Befugnisse innerhalb der DSGVO an (§ 29 Abs. 3 TTDSG). Der BfDI kann schon aufgrund des TTDSG Verwarnungen oder Anordnungen aussprechen.

Der Bundesgesetzgeber war indes daran gehindert, vergleichbare Regelungen für die Landesbehörden zu treffen, da die Länder das TTDSG als eigene Angelegenheit ausführen und über die Gesetzgebungskompetenz für den Bereich der Aufsicht von Telemedien verfügen. Entsprechende Zuweisungen können daher nur durch Landesgesetz erfolgen.

Der HmbBfDI hat daher den Landesgesetzgeber um entsprechende Umsetzung im Landesrecht gebeten. In ihrer Sitzung am 18.1.2023 hat die Hamburgische Bürgerschaft § 19 Abs. 7 HmbDSG erlassen. Dieser erklärt den HmbBfDI zur zuständigen Aufsichtsbehörde für Telemedien in Hamburg, weist dem HmbBfDI die Befugnis zur Verhängung von Bußgeldern nach dem TTDSG zu und gibt dem HmbBfDI die Untersuchungs- und Abhilfebefugnisse aus Art. 58 DSGVO. Der HmbBfDI wird dadurch in die Lage versetzt, seiner Aufsichtsfunktion wirksam nachzukommen. Er kann also in seinem Zuständigkeitsbereich Warnungen, Verwarnungen oder Anordnungen aussprechen sowie Geldbußen verhängen.

Auf Grundlage dieser Befugnisse wird der HmbBfDI 2023 beginnen, Telemedienangebote von Hamburger Unternehmen auf deren Vereinbarkeit mit den Vorgaben des TTDSG zu prüfen.

3. Einsatz der Videokonferenzsoftware Zoom in der Freien und Hansestadt Hamburg

In seinem 30. Tätigkeitsbericht 2021 (30. TB, 4.6) informierte der HmbBfDI über eine gegenüber der Senatskanzlei der Freien und Hansestadt Hamburg (FHH) ausgesprochene Warnung aufgrund des damals geplanten Einsatzes der Videokonferenzsoftware Zoom. Diese wurde schon 2021 durch die Senatskanzlei gerichtlich angegriffen. Im Jahr 2022 gab es keine Entwicklungen in diesem Verfahren. Die Hoffnung des HmbBfDI, eine schnelle Grundsatzentscheidung herbeizuführen, ist damit nicht eingetreten.

Die ausgesprochene Warnung fußte auf dem mit dem Einsatz von Zoom untrennbar verbundenen Drittlandtransfer personenbezogener Daten in die USA. Zu den Details wird auf den genannten Tätigkeitsbericht 2021 verwiesen.

Im Tätigkeitsbericht 2021 hatte der HmbBfDI berichtet, dass Nutzende des Programms bei Teilnahme an einer Ende-zu-Ende-verschlüsselten Videokonferenz über ein Konto und verifizierte Kontaktangaben verfügen müssen. Korrekterweise kann nun davon ausgegangen werden, dass Personen, die an einer solchen Konferenz lediglich teilnehmen wollen, kein Konto benötigen und auch unter Angabe eines Pseudonyms teilnehmen können. Dieser Umstand führt jedoch nicht zu einer insgesamt abweichenden Bewertung.

Aus Sicht des HmbBfDI sind die rechtlichen Argumente im verwaltungsgerichtlichen Verfahren weitgehend ausgetauscht. Es obliegt nunmehr dem Gericht, zu einer Entscheidung zu gelangen. Leider ist das Verfahren im Jahr 2022 nicht vorangeschritten. Der HmbBfDI hätte eine handlungsanweisende Entscheidung in der Sache begrüßt, zumal die FHH den Einsatz von ZOOM weiter ausbaut.

Weitere Maßnahmen gegenüber öffentlichen Stellen in der FHH hat der HmbBfDI mit Blick auf das schwebende Verfahren aber bisher nicht getroffen. Solange die wesentliche Kernfrage, die Zulässigkeit oder Unzulässigkeit des Drittlandtransfers beim konkreten Einsatz von Zoom, nicht geklärt ist, ist auch die Wirkmacht weiterer Maßnahmen entsprechend begrenzt.

Derzeit zeichnet sich ab, dass die EU-Kommission im Jahr 2023 einen neuen Angemessenheitsbeschluss treffen wird (siehe Kapitel V 4). Der Aspekt des Drittlandtransfers wäre beim Einsatz von Zoom dann nicht mehr kritisch. Es könnte somit eine Erledigung des Verfahrens eintreten.

Nichtsdestotrotz ist dem HmbBfDI an der gerichtlichen Klärung weiter gelegen. Eine vormals rechtswidrige Datenübermittlung kann nicht dadurch geheilt werden, dass nach Jahren eine neue Rechtslage eintritt. Insbesondere auch, da die vom Europäischen Gerichtshof bemängelten staatlichen Überwachungstätigkeiten in dieser Zeit fortgeführt wurden.

4. Zensus 2022

Auch nach Abschluss der Befragungen muss die datenschutzgerechte Durchführung des Zensus 2022 sichergestellt werden. Der HmbBfDI wird insbesondere die Einhaltung der gesetzlichen Löschfristen für die identifizierenden Hilfsmerkmale überwachen.

Der HmbBfDI hat die Volkszählung Zensus 2022 von Anfang an intensiv und kritisch begleitet. Eigens für den Zensus 2022 wurde eine Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder einberufen. Bereits in der Vorbereitungsphase wurden Datenschutzaspekte diskutiert und datenschutzrelevante Bedenken und Änderungsvorschläge gegenüber dem Gesetzgeber und der

amtlichen Statistik vorgebracht, welche – wie berichtet (vgl. 30. TB, 3.5) – nicht in vollem Umfang Berücksichtigung fanden.

In der Kritik stand insbesondere der erst nachträglich in das Zensusvorbereitungsgesetz eingefügte § 9a. Dieser regelt einen Testlauf für den Zensus 2022, um die Übermittlungswege und die Qualität der zu übermittelnden Daten im Vorfeld des Zensus zu überprüfen. Hierfür sollen an einem Stichtag zu sämtlichen in den deutschen Melderegistern gespeicherten Personen umfangreiche Meldedaten mit Klarnamen an die Statistischen Ämter und schließlich in die zentrale Datenbank beim Statistischen Bundesamt übermittelt werden. Hier stellte sich die Frage der Erforderlich- und Verhältnismäßigkeit. Einen von der Gesellschaft für Freiheitsrechte (GFF) gegen diesen Test mit Echtdaten gestellten Antrag auf Erlass einer einstweiligen Anordnung lehnte das Bundesverfassungsgericht (BVerfG) im Februar 2019 ab (vgl. 1 BvQ 4/2019). Den Ausgang eines Verfassungsbeschwerdeverfahrens bezeichnete das BVerfG ausdrücklich als offen. Dabei verwies es darauf, dass im Gesetzgebungsverfahren zum Teil umstritten geblieben sei, ob und in welchem Umfang eine zentrale Analyse der nicht anonymisierten oder pseudonymisierten Meldedaten zum Zweck der Erreichung der mit der Pilotdatenlieferung verfolgten Zwecke erforderlich sei und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bis zuletzt Bedenken erhoben hatte. Die daraufhin erhobene Verfassungsbeschwerde nahm das BVerfG nach Angaben der GFF im Januar 2022 dann mit Verweis auf den Subsidiaritätsgrundsatz und die fehlende Beschreitung des fachlichen Rechtswegs nicht zur Entscheidung an.

Der Zensus 2022 erfolgte als registergestützte Erhebung (vgl. 30. TB, 3.5). Mit dem Zensusstichtag, dem 15. Mai 2022, begann die Phase der Datenerhebung. Zu diesem Stichtag übermittelten die Verwaltungsbehörden, wie etwa Meldebehörden oder die Bundesagentur für Arbeit, ihre Datensätze an die Statistischen Ämter. Auch die Befragungen der Bürger:innen begannen an diesem Tag. Im Rahmen der Gebäude- und Wohnungszählung (GWZ) wurden sämtliche Eigentümer:innen und Verwalter:innen von Gebäuden und Wohnun-

gen postalisch aufgefordert, online oder postalisch Auskünfte zu erteilen. In der ergänzenden Haushaltsstichprobe wurden in Hamburg ca. 60.000 Haushalte und in Schleswig-Holstein ca. 220.000 Haushalte befragt. Zusätzlich wurden an Anschriften mit Sonderbereichen die Bewohner:innen von Wohnheimen befragt und in Gemeinschaftsunterkünften und Justizvollzugsanstalten die Daten der Bewohner:innen bzw. der Insass:innen bei den Hausleitungen erhoben.

Mit Beginn der Befragungen haben sich viele Bürger:innen mit Anfragen und Beschwerden an den HmbBfDI gewandt. Um dem massiven Informationsbedürfnis der Betroffenen nachzukommen, hat der HmbBfDI Informationen zum Zensus 2022 und Antworten auf die meist gestellten Fragen (FAQ) auf seiner Homepage veröffentlicht.

Der HmbBfDI steht seit Beginn des Zensus 2022 mit dem Statistischen Amt für Hamburg und Schleswig-Holstein in engem Kontakt. Dabei wurden in mehreren Gesprächen datenschutzrechtliche und technische Fragestellungen bei der Durchführung des Zensus 2022 behandelt. Den Anfragen und Beschwerden in der Erhebungsphase lagen aufgetretene Probleme und Fragestellungen zugrunde wie zum Beispiel Fehladressierungen, Anschreiben an Verstorbene, Datenerhebungen über Dritte sowie der unberechtigte Versand von Erinnerungsschreiben an Auskunftspflichtige, welche bereits von der Möglichkeit der Online-Beantwortung Gebrauch gemacht hatten. Des Weiteren wurden Fragen zu Geltung und Reichweite des Auskunftsanspruchs der Betroffenen nach Art. 15 DSGVO vor dem Hintergrund der besonderen statistikrechtlichen und landesrechtlichen Regelungen und die Anforderungen an eine sicherere Identifizierung der auskunftsbegehrenden Person thematisiert. Gravierende datenschutzrechtliche Mängel konnten durch den HmbBfDI hier jedoch nicht festgestellt werden. Bei den Erörterungen zum Zensus 2022 zeigte das Statistische Amt für Hamburg und Schleswig-Holstein erfreulicherweise insgesamt ein hohes Maß an Sensibilität für die Anforderungen des Datenschutzrechts.

Beim Zensus 2022 oblag dem Statistischen Bundesamt die Verantwortung für die zentrale technische Infrastruktur und die Ver-

waltung des Gesamtdatenbestands. Insbesondere bei der Gebäude- und Wohnungszählung verfolgte der statistische Verbund eine Online-First-Strategie. Dazu hatte das Statistische Bundesamt mit zensus2022.de eine eigene Webseite zur Datenerfassung live geschaltet, welche vom Informationstechnikzentrum Bund (ITZ Bund) gehostet wurde. Die Auskunftspflichtigen erhielten postalisch einen personalisierten Code, mit dem sie sich auf der Webseite des Zensus 2022 für den online-Fragebogen anmelden konnten. Hier kam es zu Beschwerden und gerichtlichen Verfahren von Betroffenen, als bekannt wurde, dass Technik des US-amerikanischen Content-Delivery-Network-Dienstleisters Cloudflare in die Infrastruktur der Website zum Zensus 2022 eingebunden war. Es wurde befürchtet, dass Unbefugte Kenntnis von personenbezogenen Daten des Online-Fragebogens zur GWZ erhalten könnten. Nach Prüfung des Sachverhalts durch den BfDI, teilte dieser mit, dass die Einbindung von Cloudflare nur den öffentlichen Bereich der Webseite zensus2022.de betroffen habe und „zu keinem Zeitpunkt eine Gefahr für die in dem Fragebogen eingegebenen personenbezogenen Daten bestanden" hätte. Sehr wohl seien aber Metadaten – „z. B. Datum und Uhrzeit des Abrufs, übertragene Datenmenge, Herkunftsverweise und IP-Adresse" – an Cloudflare gegangen. Ob das rechtmäßig war, werde von Seiten des BfDI noch geprüft. Für die Sicherheit der nach der Anmeldung eingegebenen Daten habe das aber keine Folgen. Nach der Intervention des BfDI sei die Übermittlung der Metadaten beim Aufruf der Seite abgestellt worden.

Ende November waren die Erhebungen einschließlich aller Rückfragen und vorgesehenen Wiederholungsbefragungen abgeschlossen und die Erhebungsstellen wurden geschlossen. Nach Abschluss der Erhebungen haben die Statischen Ämter des Bundes und der Länder mit der Aufbereitung und Auswertung der Zensusdaten begonnen.

Nach Abschluss der Erhebungsphase liegt aus datenschutzrechtlicher Sicht das Augenmerk auf der Einhaltung der gesetzlichen Löschfristen, insbesondere für die Hilfsmerkmale. Dies sind Angaben zur technischen Durchführung der Statistik, wie beispielsweise

Name und Anschrift einer Person. Diese sind zum frühestmöglichen Zeitpunkt von den eigentlichen, dauerhaft gespeicherten statistischen Daten, den sogenannten Erhebungsmerkmalen, zu trennen. Sie müssen nach § 31 Abs. 1 Satz 2 Zensusgesetz 2022 (ZensG 2022) gelöscht werden, sobald die Überprüfung der Erhebungsdaten auf ihre Vollständigkeit und Schlüssigkeit hin erfolgt ist und sie für die Durchführung und Kontrolle der Erhebungen nicht mehr benötigt werden. Die Löschung der Hilfsmerkmale und Erhebungsunterlagen hat nach § 31 Abs. 1 Satz 3 ZensG 2022 spätestens vier Jahre nach dem Zensusstichtag zu erfolgen. Zentrale Frage ist dabei, ab wann die Hilfsmerkmale für die Durchführung und Kontrolle der Erhebungen nicht mehr erforderlich sind. Der HmbBfDI hat vom Statistischen Amt für Hamburg und Schleswig-Holstein ein Löschkonzept angefordert, um Klarheit über das Verfahren zur Löschung der Hilfsmerkmale zu erhalten und diese überwachen zu können.

5. Abfragen bei ehemaligen Arbeitgeber:innen im Rahmen des Bewerbungsverfahrens

Im Rahmen von Bewerbungsfahren kommt es immer wieder zu (telefonischen) Erkundigungen über Bewerber:innen bei ehemaligen Arbeitgeber:innen. Seit Geltungsbeginn der DSGVO ist bereits eine gesteigerte Sensibilisierung der Arbeitgeber:innen festzustellen, dennoch erreichen den HmbBfDI immer noch Anfragen, ob und in welchem Umfang Erkundigungen eingeholt werden können.

Abfragen potentieller Arbeitgeber:innen im Bewerbungsverfahren, die nicht bei Bewerber:innen selbst, sondern bei ehemaligen Arbeitgeber:innen erfolgen, stellen regelmäßig einen tiefen Eingriff in das Persönlichkeitsrecht der Bewerber:innen dar. Auch wenn die DSGVO und das BDSG den Vorrang der Direkterhebung nicht explizit erwähnen, gebieten die aus Art. 5 Abs. 1 lit. a DSGVO folgenden Grundsätze von Treu und Glauben sowie der Transparenz, dass bei

solchen Abfragen im besonderen Maße darauf geachtet wird, die Grenzen des Erforderlichen nicht zu überschreiten und den Prozess im Bewerbungsverfahren möglichst nachvollziehbar zu gestalten. Die Frage, wann und in welchem Umfang Abfragen bei ehemaligen Arbeitgeber:innen zulässig sein können, wird von den Aufsichtsbehörden unterschiedlich beurteilt. Der HmbBfDI arbeitet deshalb in der Datenschutzkonferenz auf die Erstellung eines gemeinsamen Papiers hin. Bis dahin hat er die enorme Praxisrelevanz dieser Frage im Bewerbungsverfahren zum Anlass genommen und im Jahr 2022 die Vereinbarkeit der verschiedenen Positionen im Lichte der DSGVO und des BDSG geprüft. Nach Auffassung des HmbBfDI ist eine Abfrage unter Umständen sowohl nach § 26 Abs. 1 BDSG als auch nach Einholung einer Einwilligung gemäß § 26 Abs. 2 BDSG vertretbar.

Gemäß § 26 Abs. 1 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Dies ist in Anlehnung an die Rechtsprechung des Bundesarbeitsgerichts bei Bewerbern der Fall, wenn es ein bereits gekündigtes Arbeitsverhältnis betrifft (BAG, Urt. v. 18.12.1984, Az. 3 AZR 389/83). Abfragen bei ungekündigten Arbeitsverhältnissen kann § 26 Abs. 1 BDSG hingegen nicht rechtfertigen, da aktuelle Arbeitgeber:innen auf diese Weise erfahren könnten, dass Beschäftigte sich auf eine andere Stelle bewerben. Diese Differenzierung folgt bereits aus dem obiter dictum der BAG-Entscheidung. Im Hinblick auf die Gefahr eines „ungefilterten Informationsaustausches“ sind an etwaige Abfragen bei ehemaligen Arbeitgeber:innen der Bewerber:innen jedoch strenge Anforderungen zu stellen. So werden die Fragen an ehemalige Arbeitgeber:innen nicht weiter gehen dürfen als das, was zulässiger Inhalt eines Arbeitszeugnisses sein kann. Spontanäußerungen ehemaliger Arbeitgeber:innens, welche den Rahmen des Zulässigen überschreiten, sowie die Problematik der Nachweisbarkeit der Einhaltung dieser Grenzen (Art. 5 Abs. 2 DSGVO) legen den Schluss nahe, dass solche Abfragen idealerweise schriftlich erfolgen.

Da die vorstehenden Einschränkungen den Zweck von Abfragen bei ehemaligen Arbeitgeber:innen regelmäßig unterlaufen dürften, wird in der arbeits- und datenschutzrechtlichen Praxis im Ergebnis auf eine Einwilligung gemäß § 26 Abs. 2 BDSG abzustellen sein. Neben der teils schwierigen Frage der Freiwilligkeit muss der Einhaltung der Transparenzvorschriften (Art. 13, 14 DSGVO) besondere Beachtung geschenkt werden. Die Gewährung einer Stellungnahmemöglichkeit zu den eingeholten Auskünften kann Transparenzdefiziten entgegenwirken.

6. Die einrichtungsbezogene Impfpflicht zum Schutz vulnerabler Gruppen

Zum 31. Dezember 2022 ist die einrichtungsbezogene Impfpflicht gem. § 20a IfSG ausgelaufen. Pandemiebedingte Datenverarbeitungen auf dieser Grundlage sind damit nicht mehr zulässig und bestehende Da tensätze müssen spätestens mit Wegfall der Rechtsgrundlage gelöscht werden.

Mit dem Gesetz zur Stärkung der Impfprävention gegen COVID-19 und zur Änderung weiterer Vorschriften im Zusammenhang mit der COVID-19-Pandemie vom 10. Dezember 2021 (BGBl. I S. 5162) hat der Bundesgesetzgeber in § 20a Infektionsschutzgesetz (IfSG) die einrichtungsbezogene Impfpflicht normiert. In Anlehnung an die Regelungen zur Masernimpfpflicht regelte der neu eingefügte § 20a IfSG in gesetzlich bestimmten Einrichtungen und Unternehmen aus dem Gesundheitsbereich, dass alle Personen, die in den betroffenen Einrichtungen und Unternehmen tätig sind, bis zum Ablauf des 15. März 2022 gegenüber der Leitung den erforderlichen Nachweis erbringen, dass sie gegen das Coronavirus SARS-CoV-2 geimpft oder von diesem genesen sind oder bei ihnen eine medizinische Kontraindikation hinsichtlich einer Impfung gegen das Coronavirus SARS-CoV-2 vorliegt. Nach Ablauf des 15. März 2022 mussten sie

den Nachweis auch der zuständigen Behörde vorlegen, wenn sie dazu aufgefordert werden.

Weit vor Geltungsbeginn dieser Regelung erreichten den HmbBfDI eine Vielzahl an Beratungsanfragen von betroffenen Einrichtungen und Personen. Während die betroffenen Personen vornehmlich an der Prüfung der datenschutzrechtlichen Zulässigkeit einer einrichtungsbezogenen Impfpflicht interessiert waren, lag der Schwerpunkt bei den betroffenen Einrichtungen in der praktischen Umsetzung der Datenverarbeitung. Die Datenschutzkonferenz (DSK) hat die Anfragen zum Anlass genommen und eine bereits im Dezember erarbeitete Anwendungshilfe (Stand 20.12.2021), die häufige Fragestellungen zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie erläutert, mit einem Beschluss "Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht" (Stand: 13.04.2022) erweitert. Diese sollten für den praktischen Vollzug als Hilfestellung im Anwendungsbereich der DSGVO dienen. Mit Erfolg, denn schon kurz nach Veröffentlichung der Anwendungshilfe zur einrichtungsbezogenen Impfpflicht pendelte sich die Beratung ein.

Übrig blieben in der Beratungspraxis Personen mit grundsätzlichen Vorbehalten gegenüber den Impfungen/Auffrischungsimpfungen, die sich an den HmbBfDI wandten und die Rechtmäßigkeit dieser Datenerhebungen (datenschutzrechtlich) in Frage stellten. Der HmbBfDI konnte in diesen Konstellationen jedoch keine ungerechtfertigten Datenschutz- bzw. Verletzungen des allgemeinen Persönlichkeitsrechts erkennen. Diese durch den HmbBfDI vertretene Position wurde gestärkt durch einen Beschluss des Bundesverfassungsgerichts (BVerfG) vom 27. April 2022 (1 BvR 2649/21). Hiernach waren die Regelungen des 20a IfSG, soweit Sie in die Grundrechte der Beschwerdeführerin eingriffen, verfassungsrechtlich gerechtfertigt: *„Der Gesetzgeber hat im Rahmen des ihm zustehenden Einschätzungsspielraums einen angemessenen Ausgleich zwischen dem mit der Nachweispflicht verfolgten Schutz vulnerabler Menschen vor einer Infektion mit dem Coronavirus SARS-CoV-2 und den Grund-*

rechtsbeeinträchtigungen gefunden. Trotz der hohen Eingriffsintensität müssen die grundrechtlich geschützten Interessen der im Gesundheits- und Pflegebereich tätigen Beschwerdeführenden letztlich zurücktreten." (BVerfG-Beschluss vom 27. April 2022).

Unabhängig von einer Löschpflicht nach Artikel 17 Abs. 1 lit. a DSGVO sah § 20a Abs. 7 S. 7 IfSG vor, dass die im Zusammenhang mit der Meldepflicht und Beurteilung der Gefährdungslage anhand von Impfquoten verarbeiteten Daten spätestens am Ende des sechsten Monats nach ihrer Erhebung gelöscht werden müssen. Jedenfalls muss eine Löschung aller auf Grundlage des § 20a IfSG verarbeiteten Daten spätestens mit Ablauf der Rechtsgrundlage am 31. Dezember 2022 erfolgen, soweit sie nicht im Einzelfall für arbeitsrechtliche Auseinandersetzungen infolge der nicht erbrachten Nachweise erforderlich sind.

Hinweise auf eine weitere Speicherung von Daten auf Grundlage des § 20a IfSG wird der HmbBfDI mit Nachdruck verfolgen.

7. Wegfall der Maßnahmen zur Pandemiebekämpfung

Die Corona-Pandemie war eine Ausnahmesituation, in der beispiellose Grundrechtseingriffe geboten waren. Die meisten Verarbeitungsbefug nisse zur Eindämmung der Corona-Pandemie sind bis zum April 2022 weggefallen, sodass gesammelte Daten zu löschen waren. Der HmbBfDI hatte zu einem digitalen Frühjahrsputz aufgerufen.

Die Covid-19-Pandemie hatte weitgehende Eingriffe in das Recht auf informationelle Selbstbestimmung zur Folge. Arbeitgeber:innen, Gaststätten und viele weitere Einrichtungen erhielten Befugnisse, die zuvor undenkbar gewesen wären. Diese Maßnahmen waren besondere staatliche Reaktionen auf eine außergewöhnliche pandemi-

sche Bedrohungslage. Alle damit verbundenen Datenverarbeitungen unterlagen einer strengen Zweckbindung. Mit dem Wegfall dieser Befugnisse sind die Grundrechtseingriffe zu beenden. Versuche, die in den letzten drei Jahren eingeführten Maßnahmen in die Zukunft zu retten, indem sie auf andere Rechtsgrundlagen oder Betriebsvereinbarungen gestützt werden, werden regelmäßig scheitern. Jetzt nicht mehr erforderliche Daten dürfen auch nicht für den Zweck aufbewahrt werden, dass sie bei einer erneuten verschärften pandemischen Lage wieder benötigt würden. Eine solche Vorratsdatenhaltung wäre auch wenig sinnvoll, da beispielsweise Informationen über den Impfstatus aus dem vorletzten Jahr ohnehin nur noch bedingt aussagekräftig sind. Bei der Löschung bzw. Vernichtung der Unterlagen ist darauf zu achten, dass es sich zum größten Teil um besonders schützenswerte Gesundheitsdaten handelt. Die Dokumente dürfen daher nicht einfach in den Papierkorb geworfen werden, sondern sie müssen fachgerecht entsorgt bzw. geschreddert werden.

In Hamburg war ein wesentlicher Meilenstein der Überwindung der Pandemielage der 30.04.2022. Zu diesem Datum ist die Hotspot-Regelung ausgelaufen. Fast alle Eindämmungsmaßnahmen, die Datenerhebungen umfassten, sind spätestens zu diesem Zeitpunkt ausgelaufen. Verbliebene Masken- und Isolationspflichten haben nur noch einen mittelbaren Datenschutzbezug. Der HmbBfDI hat deshalb zu einem digitalen Frühjahrsputz aufgerufen. Arbeitgeber:innen, Geschäftsinhaber:innen und andere Stellen wurden angehalten, eine Inventur der bei Ihnen noch vorhandenen Covid-bezogenen Daten vorzunehmen und zum Datenbestand der Zeit vor der Pandemie zurückzukehren. Der Aufruf hat breite mediale Aufmerksamkeit erhalten. Zudem hat der HmbBfDI Kontakt mit Kammern und Verbänden aufgenommen, die den Appell an ihre Mitgliedsunternehmen weitergetragen haben.

Für Arbeitgeber:innen bestand Handlungsbedarf vor allem in Hinblick auf die Dokumentation des Impf- oder Teststatus der Beschäftigten. Bereits seit dem 20.03.2022 besteht keine „3G-Nachweispflicht“ am Arbeitsplatz mehr. Grund hierfür ist eine Änderung des

Infektionsschutzgesetzes und der Wegfall des § 28b IfSG a.F. Dies bedeutet, dass Arbeitgeber:innen keine 3G-Daten (geimpft, genesen, getestet) mehr von Ihren Beschäftigten abfragen dürfen. Mit dem Wegfall der Rechtsgrundlage sind auch die darauf basierenden Aufzeichnungen zu löschen. Die inzwischen entfallene Regelung sah eine Löschfrist von maximal sechs Monaten vor, die mittlerweile abgelaufen ist. Es besteht damit keine Rechtsgrundlage für die weitere Speicherung der 3G-Daten. Auch zum Nachweis, dass die 3G-Erfassung im Winter 2021/2022 rechtskonform erfolgt ist, ist keine weitere Aufbewahrung der personenbezogenen Informationen mehr notwendig. Hierfür genügen allgemeine Dokumentationen der damaligen Abläufe. Auch die Gesundheitsdaten der im Zeitraum 15.03. - 31.12.2022 gültigen einrichtungsbezogenen Impfpflicht sind mittlerweile zu löschen. Krankenhäuser und ähnliche konkret benannte Einrichtungen hatten gemäß § 20a IfSG zu überprüfen, ob ihre Beschäftigten gegen das Coronavirus geimpft waren. Diese Regelung ist außer Kraft getreten, sodass kein Grund mehr für die weitere Aufbewahrung besteht, soweit die nicht erfolgte Impfung keine arbeitsrechtliche Auseinandersetzung zur Folge hatte (siehe Kap. III 6). Sofern Beschäftigte danach befragt wurden, ob sie einer Risikogruppe angehören, war dies auch während der Pandemie nur auf Basis einer individuellen Einwilligung zulässig. Hier ist eine weitere Aufbewahrung der Informationen nur denkbar, wenn die Daten für die tatsächlichen Auswirkungen der Pandemie auf den/die Mitarbeitende/n weiter benötigt werden und diese von einer nicht widerrufenen Einwilligung abgedeckt sind (z.B. für besondere, individuelle Arbeitsschutzmaßnahmen). Soweit die Maskenpflicht in den Betrieben wegfällt, sind zudem alle Angaben über Befreiungsgründe zu löschen. Dies ist mittlerweile überall außer im Personennahverkehr der Fall.

Für Gaststätten, Kulturstätten und andere Einrichtungen mit Publikumsverkehr bestand überwiegend Handlungsbedarf hinsichtlich der Kontaktdatenerhebung. Seit dem 05.02.2022 ist die Pflicht zur Registrierung aller Besucher:innen ausgelaufen. Damit dürfen diese Daten nicht mehr erhoben werden. Dies gilt sowohl für die Erfas-

sung auf Papier als auch für digitale Verfahren (z.B. via der Luca-App). Sollten diese ohnehin jeweils nach vier Wochen zu löschenden Daten noch vorliegen, sind sie unverzüglich zu vernichten. Die Gesundheitsämter werten mittlerweile weder die papierbasierten noch die über eine App erfassten Kontakte aus, sodass für die erhobenen Informationen kein praktischer Nutzen mehr besteht. Das Personal der besuchten Einrichtungen darf daher nicht mehr verlangen, dass sich die Gäste mit einer App einchecken. Eventuell noch vorhandene QR-Code-Aufkleber sollten entfernt werden, um nicht den Anschein zu erwecken, die Einrichtung würde weiter zur Nutzung auffordern. Sie können gegebenenfalls durch QR-Codes der Corona-Warn-App des Robert-Koch-Instituts ersetzt werden. Die datenschutzfreundliche und freiwillig nutzbare Corona-Warn-App informiert auch weiterhin Personen, die einen Risikokontakt hatten.

Zeitgleich zur öffentlichen Sensibilisierung wurden Kontrollen von Corona-Testzentren verstärkt. Dabei aufgedeckte Missstände wurden teilweise sanktioniert (siehe Kap. IV 1 und 5).

8. Jugendschutz im Netz: Die KI als Türsteher im Internet

Von Gewaltdarstellungen bis Pornographie schwer jugendgefährdende Inhalte dürfen im Internet nicht ohne Weiteres verbreitet werden. Für die Altersverifikation der Nutzer:innen sind verschiedene technische Lösungen auf dem Markt, deren datenschutzkonformer Einsatz heraus fordernd ist.

Wer schwer jugendgefährdende Inhalte veröffentlicht, hat den Zutritt nur durch Erwachsene sicherzustellen. Es ist kein Geheimnis, dass die Durchsetzung nicht flächendeckend gelingt, aber die Rechtslage ist klar. Altersverifikation ist ein wichtiges Element des Jugendschutzes. Ein digitaler Türsteher ist für deutsche Anbieter unabdingbar. Hier beginnen zugleich die Herausforderungen des

Datenschutzes. Es versteht sich von selbst, dass die Besucher:innen von Ü18-Portalen ein besonderes Bedürfnis haben, unerkannt zu bleiben. Weder Anbieter selbst noch Dritte sollten bei den legitimen, aber typischerweise schambehafteten Ansinnen Kenntnis über die Identitäten der Nutzer:innen haben. Selbst im eigenen Umfeld besteht ein gesteigertes Anonymitätsbedürfnis. Klassische Modelle, bei denen der Personalausweis in einer Filiale vorgezeigt wird, um dann einen Codebrief an die Familienanschrift zu erhalten, werden für viele Konsument:innen keine realistische Option sein.

Die technischen Lösungen für eine Altersverifikation im Internet sind vielfältig. Zur Orientierung haben die Medienanstalten der Länder sogenannte Positivbewertungen zu 101 Systemen abgegeben. Es handelt sich nicht um rechtlich bindende oder notwendige Akkreditierungen, sondern um behördliche Öffentlichkeitsarbeit im Rahmen des Beratungsauftrags. Die genau für diesen Zweck konzipierte und datenschutzfreundlich ausgestaltete Altersbestimmung mittels der Schnittstelle des elektronischen Personalausweises ist leider nicht dabei. Die meisten Ansätze zielen darauf ab, dass Nutzer:innen ihren Personalausweis vor der Nutzung des Dienstes vorzeigen oder dass an eine vorherige Ausweiskontrolle etwa bei Eröffnung eines Bankkontos oder Abschluss eines Mobilfunkvertrags angeknüpft wird. Neben der persönlichen Vorlage können Ausweisdokumente auch über eine Webcam vorgezeigt und mit dem Gesicht abgeglichen werden. Diese Videoidentifizierung hat dabei ihre Schwachstellen. Jüngst hat der Chaos Computer Club nachgewiesen, dass auf diesem Weg gefälschte Ausweise relativ leichtes Spiel haben.

Die Vorstellung, sich bei Betreten eines Erotikportals persönlich und namentlich bei einer Servicekraft vorzustellen, löst vielfach Unbehagen aus. Um Vertrauen zu schaffen, ist es essenziell, hier auf strengen Datenschutz zu pochen. Genau das blenden die Medienanstalten bei ihren Positivbewertungen jedoch weitestgehend aus. In ihrem Kriterienkatalog, dem sogenannten AVS-Raster, findet sich lediglich der rudimentäre Hinweis, dass Personendaten „unter Beachtung datenschutzrechtlicher Vorgaben erfasst“ werden müssen. Eine ernst-

hafte, in diesem sensiblen Bereich gebotene Prüfung anhand der Datenschutzgrundverordnung unternehmen die Medienanstalten nicht, bevor sie einem System bescheinigen, ein geeigneter Dienst zu sein.

Vor diesem Hintergrund überrascht es, dass kürzlich drei KI-Systeme ohne nähere datenschutzrechtliche Betrachtung durchgewunken wurden. Diese Altersverifikationsservices kommen vollständig ohne eine Sichtkontrolle durch Menschen aus. In einem Videotelefonat mit einer künstlichen Intelligenz schätzt diese anhand der Gesichtszüge eigenständig ein, ob das Individuum am anderen Ende der Leitung volljährig ist. Was zunächst nach einer Dystopie à la Hollywood klingt, bei der eine Maschine den Menschen bewertet und ihm Zugang zu Medien verwehrt, muss aus Datenschutzsicht gar kein schlechter Ansatz sein. Schließlich kommen diese Verfahren als einzige ohne Ausweisdokumente aus. Name und Anschrift der Nutzer:innen bleiben damit der KI als Entscheidungsträgerin verborgen. Das Missbrauchspotenzial ist jedoch gewaltig. Einmal erstellte biometrische Muster lassen sich für Identitätsdiebstahl vom Bankbetrug bis zum gefälschten Nacktvideo zweckentfremden. Zudem darf es nicht sein, dass Individuen einer nicht von Menschen revidierbaren Entscheidung unterworfen und so zum Spielball einer gegebenenfalls undurchsichtigen Software werden.

Der Teufel steckt wie so oft im Detail der konkreten Umsetzung. Vollautomatisierte Systeme ohne menschliche Mitwirkung sind in schambehafteten Bereichen oftmals im Interesse der Betroffenen. Dabei muss aber garantiert sein, dass diskriminierungsfreie Alternativen für skeptische oder durch das Erkennungsraster fallende Personen bestehen und die Datenverarbeitung sicher und abgeschottet erfolgt. Eine KI wendet erlernte Muster an und denkt notgedrungen in Schubladen. Dennoch muss Raum für Diversität bleiben. Wer körperliche Fehlbildungen oder ein jugendliches Aussehen hat, darf nicht deshalb von Services ausgeschlossen werden. Bei der Verarbeitung ist auf ein geschlossenes System zu achten, das eine Verkettung der erhobenen Biometrie- oder Ausweisdaten mit den konsumierten Inhalten ausschließt. Nach erfolgter Altersverifikation sind keine

Daten aufzubewahren außer der Erkenntnis, dass die betreffenden Zugangsdaten zu einer volljährigen Person gehören. Insbesondere ist darauf zu achten, dass die Videodateien realer Kund:innen nicht ungefragt zum Training des KI-Modells herangezogen werden. Die Information der Inanspruchnahme eines Ü18-Dienstes ist zu sensibel, um dauerhaft im Gedächtnis einer künstlichen Intelligenz zu bleiben.

Diese Anforderungen können die Medienanstalten auf Basis ihrer Prüfkriterien nicht gewährleisten. Ihnen geht es ausschließlich darum, dass ein Service zweifelsfrei imstande ist, die Volljährigkeit nachzuweisen. Dass die Dienste rechtlich sicher eingesetzt werden können, wird durch die Positiventscheidung der Medienanstalten nicht bestätigt. Es besteht keine Garantie, dass die Datenschutzbehörden nicht mit empfindlichen Sanktionen gegen den Einsatz vorgehen würden. Plattformen, die solche Dienste vorschalten, haben sich im Rahmen einer Datenschutz-Folgenabschätzung selbst zu vergewissern, dass die DSGVO nicht verletzt wird. Sie können sich weder auf die Anbieter noch die Einstufung durch die Medienanstalten verlassen und werden in den meisten Konstellationen für Rechtsverstöße haften müssen.

Dem Irrglauben, die staatlicherseits angepriesenen Systeme seien rechtlich einwandfrei, muss begegnet werden, indem Datenschutz von Anfang an mitgedacht wird. In dem Spannungsfeld divergierender rechtlicher Vorgaben dürfen die Portalbetreiber:innen nicht alleine gelassen werden. Hier braucht es einen Dialog zwischen Medienanstalten und Datenschutzbehörden, um die Expertisen aus unterschiedlichen Bereichen zusammenzubringen. Der Datenschutz wird dabei nicht die Rolle des Blockierers übernehmen – steht er doch vor ähnlichen Herausforderungen. Denn auch die Datenschutzgrundverordnung kennt das Institut der Altersverifikation. Die Einwilligung gegenüber Internetangeboten für Nutzer unter sechzehn erfordert die Beteiligung der Eltern. Wie die Anbieter die hierfür notwendige Alterskontrolle wirksam vornehmen können, ist im Datenschutzrecht bislang weitgehend unerforscht. Klar ist lediglich: Die

einfache Abfrage des Alters oder des Geburtsdatums genügt den gesetzlichen Anforderungen nicht. Die Aufträge der jeweiligen Regierungsbehörden gehen hier also Hand in Hand. Es ist an der Zeit, die Debatte der bislang kaum beleuchteten Thematik aufzunehmen, um Jugendschutz und Privatsphäre in Einklang zu bringen.

In einem Umfeld, in dem weder die Anbieter noch die Nutzer (und in diesem Fall häufig auch nicht einmal die Träger der elterlichen Verantwortung) ein gesteigertes Interesse an einer wirksamen Umsetzung gesetzlicher Anforderungen haben, obliegt es den Aufsichtsbehörden als Hüter der datenschutzrechtlichen Grundsätze, durch entsprechende Initiativen mehr Rechtstreue sowohl einzufordern als auch praktisch zu ermöglichen. Gemeinsam mit erfahrenen Kooperationspartnern kann dies am besten gelingen.

9. Übergabe Cafe im Rahmen der Einschulung

Im Rahmen einer Beratungsanfrage hat sich der HmbBfDI mit der Frage befasst, ob und unter welchen Voraussetzungen Erziehungsberechtigte in einen Informationsaustausch zwischen Kindertagesstätte und Grund schule im Rahmen der Einschulung wirksam einwilligen können.

Im Zusammenhang mit der Einschulung eines Kindes kommt es in Hamburg zu verschiedenen Datenverarbeitungsvorgängen, die jeweils getrennt entweder durch die Kindertagesstätte oder durch die Grundschule vorgenommen werden. Auf der Seite der Schule werden Daten im Rahmen der sog. Viereinhalbjährigen Untersuchung gemäß § 42 Absatz 1 HmbSG und der Schuleingangsuntersuchung gemäß § 34 Absatz 5 HmbSG erhoben.

Für einen direkten Austausch von Informationen zwischen Mitarbeiter:innen von Kindertagesstätten und den Lehrer:innen der Grundschule fehlt eine gesetzliche Grundlage. Aus datenschutzrechtlicher Sicht wäre diese, soweit ein Informationsaustausch auf eine

Grundlage im Sinne von Art. 6 Absatz 1 Satz1 lit. e DSGVO gestützt werden soll, jeweils für die Weitergabe von Informationen durch die Kindertagesstätte in den sozialrechtlichen Vorschiften und für die Abfrage/Erhebung dieser Daten durch die Grundschule in den schulrechtlichen Vorschriften erforderlich. Das Auseinanderfallen der Regelungsregime ist dabei ein Umstand, der das Auffinden, bzw. ggf. die Schaffung einer gesetzlichen Grundlage nicht einfacher macht.

Um die Zusammensetzung von Klassen planen zu können, haben die Grundschulen aber ein Interesse daran, möglichst aktuelle, d.h. zum Einschulungszeitpunkt zeitnah erhobene Daten über den Entwicklungsstand eines Kindes (z.B. was den Sprachstand angeht) zu bekommen, gerade um durch die Zusammensetzung einer Klasse besondere Förderungsschwerpunkte erkennen und förderbar zu machen. Die Informationen aus den beiden genannten Eingangsuntersuchungen geben aufgrund des zeitlichen Versatzes kein ganz aktuelles Bild über den Entwicklungsstand der einzuschulenden Kinder, so dass die Informationen der Erzieher:innen aus den Kindertagesstätten mehr als nur hilfreich sind. Aus pädagogischer Sicht können diese Versatzzeiten durchaus relevant für die Entwicklung eines Kindes sein.

Da sich für diesen Informationsaustausch als Datenverarbeitungsvorgang keine gesetzliche Grundlage findet, ist eine im Bildungsbereich engagierte Stiftung an den HmbBfDI herangetreten, um die Möglichkeiten einer Einwilligung in diesen Informationsaustausch durch die Sorgeberechtigten prüfen zu lassen und erörtern zu können. Für diesen Austausch wurde ein Entwurf eines Einwilligungsformulars vorgelegt, was zeigte, dass sich dort bereits intensiv mit datenschutzrechtlichen Fragestellungen beschäftigt wurde. Dementsprechend entstand ein fruchtbarer und offener Dialog.

In der Sache war aus den eingangs dargestellten Gründen zunächst darauf zu verweisen, dass Einwilligungserklärungen jeweils von der Grundschulschule und der Kindertagesstätte einzuholen sind. Weiter war zu betonen, dass es für die Wirksamkeit einer Einwilligung im

Sinne von Art. 6 Absatz 1 Satz 1 lit. a DSGVO nach der Legaldefinition in Art. 4 Nr. 11 DSGVO entscheidend darauf ankommt, dass die Erklärung zur Einwilligung tatsächlich freiwillig und in informierter Art und Weise abgegeben wird. Zudem war auf Art. 9 Absatz 2 lit. a DSGVO hinzuweisen, da gerade der Informationsaustausch zum Entwicklungsstand von Kindern auch sensible Daten im Sinne von Art. 9 Absatz 1 DSGVO umfassen kann.

Der Schwerpunkt der Beratung verlagerte sich auf die Frage, ob gegenüber der Grundschule und der Kindertagesstätte überhaupt eine echte Freiwilligkeit der Einwilligungserteilung gegeben sein kann. Dem Erwägungsgrund 43 zur DSGVO zufolge kann bei einem Machtungleichgewicht zwischen einer betroffenen Person und einer verantwortlichen Stelle die notwendige Wahlfreiheit fehlen, was insbesondere bei einer Behörde als verantwortlicher Stelle der Fall sein kann. Hinzukommt, dass Sorgeberechtigte aufgrund des im vorgelegten Formularentwurf angegebenen Zwecks des Datenaustauschs, nämlich individuelle Fördermöglichkeiten der Kinder berücksichtigen und als Auswahlkriterien für die Klassenzusammensetzung heranzuziehen zu können, nachvollziehbare Sorgen hinsichtlich von Lern- und Fördernachteilen bei Nichterteilung einer Einwilligung haben könnten. Bei der Beschulung des Kindes handelt es sich letztlich um die Inanspruchnahme einer staatlichen Leistung im Rahmen der Schulpflicht. Die Qualität der staatlichen Leistung könnte aus den genannten Gründen von der Erteilung einer Einwilligung abhängig scheinen, was gegen das Vorliegen einer echten Freiwilligkeit sprechen könnte.

Diesen Sorgen von Erziehungsberechtigten könnte ggf. dadurch Rechnung getragen werden, dass in ein Einwilligungsformular nachvollziehbare und detaillierte Ausführungen aufgenommen werden, aus denen der/die Erklärende erkennen kann, dass ihm/ihr bei fehlender Abgabe der Einwilligungserklärung keine Nachteile in Bezug auf die Förderung und Beschulung des einzuschulenden Kindes entstehen und die Erfüllung des staatlichen Bildungsauftrages nicht gefährdet ist.

Aufgrund des unabhängig davon bestehenden staatlichen Über- und Unterordnungsverhältnisses blieben aber trotzdem Zweifel, ob Sorgeberechtigte tatsächlich von einer echten Wahlmöglichkeit ausgehen können. Diesen Zweifeln und den Bedenken an einer wirksamen Einwilligungserteilung könnte durch die Schaffung einer gesetzlichen Grundlage im Sinne von Art. 6 Absatz 1 Satz lit. e DSGVO, ggf. in Verbindung mit Art. 9 Absatz 2 lit. g DSGVO, begegnet werden, die unter angemessener Berücksichtigung der Interessen der Betroffenen Rechtmäßigkeitsvoraussetzungen für einen Datenaustausch zwischen Grundschule und Kindertagesstätte unter Beschränkung auf klar benannte und abgrenzbare Verarbeitungswecke formuliert. In diesem Zusammenhang müssten dann insbesondere auch Vorgaben zu Dokumentationspflichten und Vertraulichkeitsanforderungen und an dem Regelungszweck orientierte Aufbewahrungsfristen geregelt werden.

Eine entscheidende Bedeutung kommt aber in jedem Fall Transparenzanforderungen zu. Der Übergang zur Grundschule stellt einen entscheidenden Schritt dar, der die Weichen für die weitere sprachliche, geistige, körperliche und seelische Entwicklung des Kindes stellt. Informationsflüsse, die diese Weichenstellung vorbereiten, sollten für die Betroffenen ohne Weiteres erkennbar, nachvollziehbar, verständlich und überprüfbar sein. Daher muss den Informationspflichten aus den Art. 13, 12 DSGVO und der Erfüllbarkeit/Erfüllung von Betroffenenrechten, wie z.B. Auskunftsrechten gemäß Art. 15 DSGVO, eine besondere Bedeutung zukommen, unabhängig davon auf welche Rechtsgrundlage ein Informationsaustausch gestützt wird.

10. Datenschutzkonforme Verarbeitung von Gesundheitsdaten in der medizinischen Forschung

Die datenschutzgerechte Ermöglichung von Forschungsvorhaben ins besondere im medizinischen Bereich ist ein Kernanliegen des HmbBfDI sowie der Datenschutzkonferenz (DSK). Eine neu gegründete Taskforce setzt hier wichtige Impulse, deren Zwischenstand in der „Petersberger Erklärung" festgehalten wurden.

Die Bundesregierung misst der datenschutzgerechten Gesundheitsforschung eine hohe Bedeutung bei. Mehrere Gesetzesvorhaben sollen den Rahmen für eine rechtssichere Zusammenführung und Auswertung vorhandener Patient:innen-Daten schaffen. Im aktuellen Koalitionsvertrag ist der Erlass eines Forschungsdatenschutzgesetzes vorgesehen. Die Inhalte und Zielrichtung sind noch relativ offen. Hinzu kommt ein geplantes Registergesetz für den Forschungsbereich. Auf europäischer Ebene ist der European Health Data Space im Zusammenspiel mit einem Data Act und einem Data Governance Act geplant.

Der HmbBfDI ist gemeinsam mit der DSK entschlossen, diese bedeutsamen Entwicklungen mitzugestalten. Ziel ist, die Datenschutzrechte der Betroffenen zu wahren und gleichzeitig verbindlich aufzuzeigen, wie Forschungsvorhaben unter welchen Voraussetzungen auszugestalten sind. Zu diesem Zweck haben sich mehrere deutsche Aufsichtsbehörden zur Taskforce Forschungsdaten zusammengefunden. Im Zuge eines arbeitsteiligen Vorgehens hat sich der HmbBfDI zusammen mit den Kolleg:innen aus Baden-Württemberg, Bayern, Schleswig-Holstein und Mecklenburg-Vorpommern dem Arbeitspaket „Forschungsdatenschutzgesetz – Anforderungen an den Datenschutz" gewidmet. Weitere Bundesländer haben die Bereiche „Registergesetz – Anforderungen an den Datenschutz", „Anonymisieren im Bereich der Forschung" und „Forschungsdatengeheimnis" bearbeitet.

Die Beiträge des HmbBfDI sind wesentlich in die „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“ der DSK vom 24.11.2022 eingeflossen. Die DSK hat sich darin proaktiv positioniert, wie ein künftiges Forschungsdatenschutzgesetz datenschutzgerecht ausgestaltet sein sollte. Wichtig ist, dass der Mensch im Mittelpunkt der Forschung steht. Er ist stets einzubeziehen durch adressatengerechte Information und Widerspruchsmöglichkeiten. Verschlüsselung, Pseudonymisierung, Anonymisierung und anderen technischen Schutzmaßnahmen ist ein hoher Stellenwert einzuräumen. Darüber hinaus spricht sich die DSK für vom Klinikbetrieb und von den Forschungseinheiten getrennte Vertrauensstellen aus. Diese sollten durch besondere Unabhängigkeit sowie ein strafrechtlich abgesichertes Forschungsgeheimnis und Beschlagnahmeverbot abgesichert sein. Das dort zu organisierende Zusammenführen von Daten aus mehreren Quellen ist an klare Regeln zu knüpfen.

Die Schlüsselfrage im Diskurs ist die rechtliche Grundlage medizinischer Forschung. Während vielfach strikt auf die freiwillige Zustimmung der Betroffenen gesetzt wird, hat sich der HmbBfDI gegen eine zu starke Einwilligungszentrierung ausgesprochen. Sinnvoller wären klare gesetzliche Regelungen, was erlaubt ist und was nicht. Auf Betreiben des HmbBfDI hin mahnt die Petersberger Erklärung an, dass es Aufgabe des Gesetzgebers ist, im Allgemeininteresse liegende Forschung mit Gesundheitsdaten zu ermöglichen und zugleich ihre Grenzen festzulegen und die Interessen der betroffenen Personen zu wahren. Der Gesetzgeber darf diese komplexen Fragestellungen demnach nicht vollständig auf die betroffenen Personen und die Forschenden verlagern. Patient:innen in einer persönlichen Ausnahmesituation sollten nicht mit der Entscheidung konfrontiert und alleine gelassen werden, welche Datenbestände für den medizinischen Fortschritt notwendig und angemessen sind. Zudem schafft nur ein gesetzlich abgesteckter Rahmen die erforderlichen methodischen und strukturellen Garantien, die der Einzelne im Rahmen der Erklärung seiner Einwilligung nicht wird fordern können. Gleichwohl sind individuelle Bedürfnisse durch ein wirksames Widerspruchs-

recht zu berücksichtigen, das eine umfassende und allgemeinverständliche Information der Betroffenen voraussetzt.

Ein weiterer Schwerpunkt der Taskforce sind internationale Forschungskooperationen. Vorzugswürdig sind in diesem Kontext Datenübermittlungen auf Grundlage von Standardvertragsklauseln und anderen Instrumenten, die rechtliche Garantien im Drittstaat schaffen. Wo dies nicht praktikabel ist, wird im Gesundheitsbereich häufig auf die Einwilligung gemäß der Ausnahmevorschrift des Art. 49 DSGVO gesetzt. Die DSK engagiert sich darin, konstruktive Lösungen und Kriterien zu finden, unter welchen Umständen die Einwilligung als Übermittlungsgrundlage genutzt werden kann. Wichtig ist, dass die Einwilligung nicht zu pauschal abgegeben wird, sondern gegebenenfalls im Einzelfall noch einmal spezifisch wiederholt wird. Zudem ist im Rahmen eines Transfer Impact Assessment die Notwendigkeit zusätzlicher technisch-organisatorischer Maßnahmen zu prüfen. Die Kernfrage ist, inwieweit ein in der Forschung ansonsten teilweise möglicher „Broad Consent“ ohne Festlegung der genauen Zwecke und Verarbeitungen auch für Drittstaatentransfers herangezogen werden kann. Dieser Frage wird im Rahmen einer engen Zusammenarbeit mit der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. näher nachgegangen. Beispielsweise wird im Jahr 2023 ein gemeinsamer Workshop mit dem Verein zu Drittstaatentransfers stattfinden, in den sich der HmbBfDI einbringen wird.

Im Übrigen unterstützt die Taskforce bei der Erstellung und Harmonisierung von Einwilligungstexten etwa der Medizininformatik-Initiative sowie bei der Festlegung geeigneter Methoden zur Anonymisierung von Patientendaten wie etwa Röntgenbildern. Auch die enge Beratung des Radiological Cooperative Network (RACOON) zum Aufbau einer bundesweiten Infrastruktur zur strukturierten Erfassung radiologischer Daten von COVID-19-Fällen inklusive der teilweise erforderlichen Anpassung gesetzlicher Grundlagen gehört zum Tätigkeitsspektrum der Taskforce.

11. Koordinierte Medienprüfung

Die Prüfung von Medienunternehmen durch den HmbBfDI hatte im Ergebnis unter anderem zur Folge, dass eine Umstellung der eingesetzten Consent-Banner auf das sogenannte „Pur Abo-Modell" erfolgt ist.

Bereits im 30. Tätigkeitsbericht wurde bemängelt, dass schon durch den ersten Aufruf der Webseite einwilligungsbedürftige Drittdienste und Cookies eingebunden werden, ohne dass die Nutzer:innen zuvor die Möglichkeit hatten, überhaupt eine Einwilligung zu erteilen. Diese Prüfergebnisse wurden den verantwortlichen Medienunternehmen übermittelt und um Stellungnahme gebeten.

Dabei wurde von den verantwortlichen Medienunternehmen insbesondere der Einsatz des Interactive Advertising Bureau Europe (IAB) TCF 2.0 Consent Framework vorgetragen. Hierbei handelt es sich um einen Industriestandard, der von den Publishern (Webseitenbetreibern) zur Einholung von notwendigen Einwilligungen für das Ausspielen von personalisierter Werbung in die Webseiten eingebaut wird. Problematisch bei diesem Standard ist unter anderem, dass Drittdienstleiter, die Cookies auf der Webseite der Publisher setzen möchten, selbst entscheiden können, auf welcher Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO sie eine Datenverarbeitung vornehmen. So ist es vielfach zu Situationen gekommen, nach denen die Datenverarbeitung zwingend eine Einwilligung erforderte, eine Verarbeitung tatsächlich aber auf Grundlage einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO stattgefunden hat. Die Prüfung des HmbBfDI sowie der Umstand, dass zum Ende des Jahres 2021 das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten ist, haben die verantwortlichen Unternehmen schließlich zum Anlass genommen, die im Consent-Banner hinterlegten Vendoren bzw. aufgeführten Rechtsgrundlagen systematisch zu überprüfen, insbesondere wenn diese sich auf andere Rechtsgrundlagen als eine Einwilligung stützten. Soweit Vendoren bis dahin für

ihre Verarbeitungen nicht ausdrücklich die Einwilligung als Rechtsgrundlage auswählbar machten, sind die verantwortlichen Unternehmen auf einzelne Vendoren zugegangen und haben diese aus ihrem Consent-Banner gestrichen bzw. die Rechtsgrundlage für den jeweiligen Zweck entzogen.

Das ist aus Sicht des HmbBfDI grundsätzlich begrüßenswert, da auch die belgische Datenschutzaufsichtsbehörde eine Verarbeitung im TCF-Standard auf Grundlage des berechtigten Interesses aufgrund des hohen Risikos, das von Tracking-basierter personalisierter Werbung ausgeht, für nicht zulässig erachtet. Hier überwiegen nach Ansicht der belgischen Aufsichtsbehörde die berechtigten Interessen der Betroffenen. Zudem wurde eine Reihe von Datenverarbeitungsvorgängen durch die für IAB Europe zuständige belgische Aufsichtsbehörde für rechtswidrig erklärt. Weiterhin würden demnach unwirksame Einwilligungen eingeholt, eine ausreichende Datensicherheit nicht abgebildet und nur mangelnde Informationen der Nutzer:innen bestehen (https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf). Ob dieses Framework eine Zukunft hat, wird der EuGH entscheiden, da das belgische Handelsgericht einzelne Rechtsfragen zur Entscheidung der belgischen Datenschutzaufsichtsbehörde zur Vorabentscheidung diesem nun vorgelegt hat.

Eine weitere Konsequenz des Handelns durch den HmbBfDI ist die Umstellung der Consent-Banner auf das sogenannte „Pur"-Abo-Modell. Die verantwortlichen Medienunternehmen stellen die Nutzer:innen nunmehr vor die Wahl, entweder ein „Pur"-Abo abzuschließen und damit den Inhalt der Webseite trackingfrei nutzen zu können oder ihre Zustimmung in die Datenverarbeitung zur Ausspielung von personalisierter Werbung zu erteilen und den Inhalt der Webseite zu nutzen. Die Wirksamkeit von Einwilligungen von Nicht-Abonnenten ist bei den „Pur"-Abo-Modellen gleichwohl sicherzustellen. Soweit mehrere Verarbeitungszwecke vorliegen, die wesentlich voneinander abweichen, müssen die Anforderungen der Granularität der Einwilligung umgesetzt werden. Dies bedeutet, dass Nutzer:innen die

Möglichkeit haben müssen, die einzelnen Zwecke, zu denen eine Einwilligung eingeholt werden soll, selbst und aktiv auswählen zu können (Opt-In). Nur wenn Zwecke in einem sehr engen Zusammenhang stehen, kann eine Bündelung von Zwecken in Betracht kommen. Eine pauschale Gesamteinwilligung in insoweit verschiedene Zwecke kann nicht wirksam erteilt werden.

Die Möglichkeit einer solchen feingranularen Einstellung im Rahmen des „Pur"-Abo-Modells ist von den verantwortlichen Medienunternehmen bisher noch nicht umgesetzt, wenngleich der HmbBfDI mit diesen Anforderungen bereits an die Medienunternehmen herangetreten ist. Kurz vor Fertigstellung des Berichts haben den HmbBfDI Ankündigungen erreicht, wonach dem HmbBfDI weitere Anpassungen am Consent-Banner vorgestellt werden sollen. Vor der Entscheidung, ob aufsichtsrechtliche Maßnahmen zu ergreifen sind, wird daher die Gelegenheit dazu eingeräumt.

12. Fachprüfung eines Konformitätsbewertungsprogramms

Der Weg zur Zertifizierung von Verarbeitungsvorgängen als wünschens wertem Instrument der Selbstregulierung und zur Erhöhung der Trans parenz ist weit und mühselig. Der HmbBfDI geht ihn gemeinsam mit ei nem hier ansässigen Unternehmen.

Die Datenschutz-Grundverordnung (DSGVO) hat in allen europäischen Mitgliedstaaten die Möglichkeit der Zertifizierung von Verarbeitungsvorgängen eröffnet, die allen Marktteilnehmern zugänglich ist. Verantwortliche sollen auf Grundlage von Art. 42 und 43 DSGVO die Konformität mit der Verordnung formal belegen können, um dadurch ihren Kunden oder anderen Interessierten insoweit vertrauenswürdig begegnen zu können.

Das mit der DSGVO etablierte System sieht ein komplexes Zusammenspiel verschiedener Akteure vor. Bevor ein Verarbeitungsvorgang zertifiziert werden kann, müssen Zertifizierungsstellen eingerichtet und für diese Tätigkeit akkreditiert werden. Dies erfolgt in Deutschland durch die jeweils örtlich zuständige Datenschutzaufsichtsbehörde in Kooperation mit der Deutschen Akkreditierungsstelle DAkkS. Die Zertifizierungsstellen müssen sich dabei eines anerkannten Zertifizierungsprogramms bedienen, das sie entweder selbst erstellt haben oder von Dritten lizenzieren. Auch diese Konformitätsbewertungsprogramme werden fachlich von den zuständigen Aufsichtsbehörden geprüft und dabei sichergestellt, dass die nationalen Kriterien eingehalten werden, die auf Grundlage von Art. 43 Abs. 3 DSGVO festgelegt und genehmigt wurden. In Deutschland sind dies einheitlich die „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“, die von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) veröffentlicht wurden.

Auf dieser Grundlage hat der HmbBfDI im Berichtszeitraum ein eingereichtes Konformitätsbewertungsprogramm überprüft und dessen Übereinstimmung mit den genannten Anforderungen festgestellt. Hierfür war eine Reihe von Anpassungen und Ergänzungen des Programms erforderlich, die dem Antragsteller in mehreren Runden aufgegeben wurden. Die Zusammenarbeit mit dem Antragsteller als Autor des Programms verlief kooperativ, so dass schließlich ein Ergebnis vorgelegt wurde, bei dem keine kritischen Abweichungen von den gesetzlichen Bestimmungen und den nationalen Kriterien mehr feststellbar waren.

An diese nationale fachliche Prüfung wird sich nun noch ein europäischer Prozess anschließen. Der Europäische Datenschutzausschuss (EDSA) befasst sich auch mit Programmen, auf deren Grundlage keine Erteilung eines europäischen Datenschutzsiegels gem. Art. 42 Abs. 5 angestrebt wird, um ein Auseinanderfallen der verschiedenen nationalen Siegel und Standards zu verhindern. Dies entspricht dem Harmonisierungsgedanken der DSGVO und dem Auftrag an

den EDSA aus Art. 70 DSGVO, deren einheitliche Anwendung sicherzustellen.

In der praktischen Umsetzung ist dieser Schritt mit erheblichen zusätzlichen Aufwänden verbunden. Diese bestehen zunächst darin, sämtliche relevante Unterlagen in englischer Sprache zur Verfügung zu stellen. Bei Programmen, die allein oder überwiegend auf den heimischen Markt zielen, ist dies sowohl für die Programmeigner als auch für die zuständige Aufsichtsbehörde eine nicht unerhebliche Mehrarbeit. Sodann schließt sich ein Verfahren an, bei dem zwei Aufsichtsbehörden aus dem Kreis des EDSA gemeinsam mit der zuständigen Aufsichtsbehörde in einen Review-Prozess eintreten. Ziel ist es, die Genehmigungsfähigkeit des Programms durch den EDSA zu erreichen. Dabei werden im Austausch mit dem Programmeigner weitere Anpassungen des Programms vorgenommen, bis es auch aus Sicht dieses Review-Teams den Anforderungen entspricht, auch soweit sie sich aus dem Vergleich mit anderen Programmen ergeben, die vom EDSA bereits genehmigt wurden. Die zuvor abgeschlossene nationale fachliche Bewertung bzw. Genehmigung steht daher unter dem Vorbehalt der entsprechenden Genehmigung auf europäischer Ebene.

Die insgesamt zu durchlaufenden Prozesse von der Einreichung eines entsprechenden Antrags und Programms bei der DAkkS bis zu dessen Verwendbarkeit im Rahmen der Zertifizierung eines konkreten Verarbeitungsvorgangs sind komplex und langwierig. Es ist daher nicht überraschend, dass die erste EDSA-Genehmigung eines nationalen Programms erst im Juni 2022 erfolgte (https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en), mehr als vier Jahre nach Wirksamkeit der DSGVO. Mehrere Programme, auch aus Deutschland, sind in verschiedenen Stadien auf dem Weg zu entsprechenden Entscheidungen des EDSA. Es ist zu erwarten, dass im Jahr 2023 mehrere Programme, darunter das dem HmbBfDI vorliegende, zur Anwendung kommen können.

13. Konsultationsverfahren zur Orientierungshilfe Telemedien

Die Orientierungshilfe für Anbieter:innen von Telemedien hat durch das Konsultationsverfahren keine rechtlichen Anpassungen aber hilfreiche Ergänzungen erfahren und ist nunmehr in der Version 1.1 auf der Webseite der Datenschutzkonferenz abrufbar.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte mit Pressemitteilung vom 14. Januar 2022 ein Konsultationsverfahren zu ihrer Orientierungshilfe für Anbieter:innen von Telemedien eingeleitet. Die Orientierungshilfe ist im Dezember 2021 aufgrund der mit dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) am 1. Dezember 2021 in Kraft getretenen Rechtsänderungen nach vollständiger Überarbeitung veröffentlicht worden und stellt Anforderungen an den Betrieb von Webseiten und Apps dar.

Im Rahmen des Konsultationsverfahrens wurde Vertreter:innen aus Politik, Wirtschaft, Wissenschaft, Gesellschaft und Verwaltung Gelegenheit gegeben, zu der Orientierungshilfe Telemedien 2021 Stellung zu nehmen. Das Verfahren diente der Überprüfung und möglicherweise der Fortentwicklung der Orientierungshilfe, berührte jedoch nicht ihre Geltung und Anwendung in der aufsichtsrechtlichen Praxis. Die Stellungnahmen konnten bis zum 15. März 2022 eingereicht werden. Insgesamt sind 14 Stellungnahmen eingegangen, die sämtlich in die Auswertung eingeflossen sind.

Die Stellungnahmen wurden unter Federführung des HmbBfDI, des LfD Niedersachsen und des LDA Bayern ausgewertet. Dies erfolgte themenbezogen, das bedeutet, dass die angesprochenen Themen in den Stellungnahmen zunächst herausgearbeitet, anschließend der Bezug zur Orientierungshilfe – sofern dieser vorlag – hergestellt

und schließlich eine rechtliche Bewertung vorgenommen wurde. Insgesamt konnten dabei drei Themen, „vom Nutzer ausdrücklich gewünschter Telemediendienst – Differenzierung Basis- und Zusatzfunktionen“, „Tatbestandsmerkmal ‚unbedingt erforderlich‘„ und „Ablehnbutton auf erster Ebene“ identifiziert werden, denen aufgrund der zahlreichen Bezugnahmen in den Stellungnahmen eine besonders hohe Bedeutung zukam.

Die Auswertung der Stellungnahmen führte im Ergebnis zu keiner Änderung der rechtlichen Bewertung in der Orientierungshilfe. Hilfreich waren die Stellungnahmen jedoch in der Hinsicht, dass einige Punkte eine Konkretisierung erfahren haben und zwei komplett neue Kapitel V (Gestaltung von Einwilligungsbannern) und VI (Betroffenenrechte) eingefügt wurden. Erstmals gibt die Orientierungshilfe nun auch Hilfestellungen zur konkreten Gestaltung von Einwilligungsbannern.

Das Konsultationsverfahren endete mit der Veröffentlichung eines umfangreichen Auswertungsberichts des Arbeitskreises Medien der DSK (https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Auswertung_Konsultation_zur_Orientierungshilfe_fuer_Anbieter_von_Telemedien_final.pdf) und der daraus resultierten angepassten Orientierungshilfe für Anbieter:innen von Telemedien im Dezember 2022 (https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf). Insgesamt hat sich das erste Konsultationsverfahren auf DSK-Ebene bewährt. Es hat sowohl Interesse und entsprechende Beteiligung im Kreis der Adressaten aufgezeigt als auch zu hilfreichen Ergänzungen der Orientierungshilfe geführt. Eine Nutzung dieses partizipativen Instruments ist auch in künftigen geeigneten Fällen vorstellbar.

14. Facebook Fanpages

Der Betrieb von Facebook-Fanpages ist zurzeit nicht datenschutzkonform möglich. Das ist die Quintessenz der aktuellen Rechtsprechung, die durch aktuelle Kurzgutachten der DSK Taskforce Facebook Fanpages bekräftigt wird. Dies gilt auch, wenn die sog. Insights Funktion vonseiten Facebooks deaktiviert wird. Die Durchsetzung dieser Rechtsansicht ge genüber öffentlichen Stellen ist ein bundesweiter Prozess, der andauert. Seit Oktober 2022 hat Hamburg den Vorsitz der Taskforce.

Nachdem der Europäische Gerichtshof (EuGH) auf Vorlage des Bundesverwaltungsgerichts (BVerwG) bereits im Juni 2018 entschieden hatte, dass eine gemeinsame Verantwortlichkeit von Facebook und sogenannten Fanpage-Betreiber:innen besteht, wurde das Verfahren vom EuGH zunächst zurück an das BVerwG und durch dieses dann an das Oberverwaltungsgericht Schleswig-Holstein (OVG Schleswig) zurück verwiesen. Das OVG Schleswig hat auf Grundlage der Vorabentscheidung des EuGH und der Entscheidung des BVerwG mit Urteil vom November 2021 endgültig in der Sache entschieden, dass die Deaktivierungsanordnung der schleswig-holsteinischen Aufsichtsbehörde aus Dezember 2011 gegen den Betreiber einer Fanpage rechtmäßig war und damit das über 10 Jahre dauernde Verfahren beendet.

Zur Vorbereitung darauf aufbauender, abgestimmter behördlicher Maßnahmen der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen Betreiber:innen von Facebook-Fanpages wurde im März 2022 die erste Version eines Kurzgutachtens veröffentlicht, das sich schwerpunktmäßig mit Fragen der Rechtskonformität des Betriebs von Facebook-Fanpages vor dem Hintergrund des 2021 in Kraft getretenen Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) beschäftigt. Im Herbst 2022

wurde eine Aktualisierung des Kurzgutachtens vorgenommen, die den zwischenzeitlichen tatsächlichen und rechtlichen Entwicklungen Rechnung trägt. Die aktualisierte Version 1.1 des Kurzgutachtens wurde im November 2022 von der DSK beschlossen und anschließend veröffentlicht (https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Kurzgutachten_Facebook-Fanpages_V1_1_clean.pdf).

Das Kurzgutachten stellt die abgestimmte Rechtsauffassung der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder dar und ist somit Grundlage für diesbezügliche Aufsichtstätigkeit der Behörden.

Nach Veröffentlichung der ersten Version des Kurzgutachtens hatte die DSK bereits im März 2022 den Beschluss gefasst, dass die deutschen Datenschutzaufsichtsbehörden im Rahmen ihrer Zuständigkeit die obersten Landes- bzw. Bundesbehörden über den Inhalt des Kurzgutachtens zeitnah informieren und überprüfen, ob Landes- bzw. Bundesbehörden Facebook-Fanpages betreiben sowie darauf hinwirken werden, dass von Landes- bzw. Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können.

Der HmbBfDI hat in Umsetzung dieses DSK-Beschlusses die Senatskanzlei schriftlich auf das Kurzgutachten hingewiesen.

Das Kurzgutachten stellt in der im November 2022 aktualisierten Version nunmehr klar, dass nach Auffassung der Aufsichtsbehörden eine gemeinsame Verantwortlichkeit auch dann anzunehmen ist, wenn die sog. Insights-Funktion deaktiviert wird. Der EuGH hatte im Rahmen der o. a. Vorlageentscheidung geurteilt, dass insbesondere durch die Nutzung der sog. Insights (Statistiken über die Nutzung der Fanpage, die von Facebook auf Grundlage der Nutzungsdaten erstellt und an die Betreiber:innen ausgespielt werden) eine gemeinsame Verantwortlichkeit der Betreiber von Fanpages gemeinsam mit Facebook besteht. Dazu führt das Kurzgutachten aus:

„Eine gemeinsame Verantwortlichkeit besteht auch dann, wenn die Statistiken für Fanpage-Betreiber:innen deaktiviert werden. Durch die Deaktivierung verändert sich nämlich die relevante Datenverarbeitung beim Betrieb einer Fanpage kaum. Den Betreiber:innen werden lediglich aus den – nach wie vor – verarbeiteten Nutzungsdaten keine Statistiken mehr ausgespielt. […]

Auch wenn Meta keine Statistiken mehr übermittelt, findet beim Aufrufen der Fanpage und dem Interagieren mit der Fanpage eine Erhebung personenbezogener Daten und Nutzung der Daten durch Facebook statt, welche es ohne den Betrieb der Fanpage nicht gäbe. Bei diesem Prozess entscheiden die Betreiber:innen und Meta gemeinsam über Mittel und Zwecke der Datenverarbeitung. Hinsichtlich der Mittel genügt es, dass die Betreiber:innen die Fanpage in dem Wissen betreiben, dass sie zum Erheben und Übermitteln personenbezogener Daten an Meta dient. Damit beeinflussen die Betreiber:innen der Fanpage entscheidend das Erheben und Übermitteln der Daten der Besucher:innen dieser Seite an Meta, die ohne die Fanpage nicht erfolgen würden. Hinsichtlich der Zwecke kommt es darauf an, dass beide Seiten von den genannten Verarbeitungsvorgängen profitieren, was hier der Fall ist: Die Betreiber:innen erhöhen auf diese Weise ihre Reichweite, da sie sich die Möglichkeiten und den Netzwerkeffekt von Facebook zunutze machen. Meta profitiert von den Fanpages, weil anhand der dortigen Interaktionen Profile über Besucher:innen der Fanpage angelegt und weiter ausdifferenziert werden können und damit die auf dem Netzwerk bereitgestellte zielgerichtete Adressierung und Ausspielung von Werbebotschaften optimiert werden kann. Die Zwecke der Betreiber:innen der Fanpage und von Meta ergänzen sich daher gegenseitig. Dies ist für die Annahme eines gemeinsamen Zweckes i.S.v. Art. 26 DSGVO ausreichend."

Neben den entsprechenden Tätigkeiten der Datenschutzaufsichtsbehörden auf Länderebene ist aktuell vor allem das vom Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) auf

Bundesebene eingeleitete aufsichtsbehördliche Verfahren gegen das Bundespresseamt von wegweisender Bedeutung. Landes- und Bundesbehörden zögern momentan noch mit Blick auf den weiteren Verlauf dieses Verfahrens mit weiteren Schritten und einer umfassenden Abkehr von noch bestehenden Fanpages, auch weil ein einheitliches Vorgehen gewünscht ist. Es ist daher davon auszugehen, dass der Ausgang des Verfahrens auf Bundesebene entscheidende Impulse in die Länder hineintragen wird. Der HmbBfDI stimmt sich im Rahmen der Taskforce mit den Kolleg:innen der Länder und dem BfDI fortwährend ab, erhofft sich eine zügige rechtliche Klärung und erwartet eine entsprechende Reaktion nach Abschluss des Verfahrens.

15. Google Suchmaschine

In der Google Suchmaschine werden automatisiert Inhalte angezeigt. Dabei handelt es sich nicht nur um Suchergebnisse, sondern auch um von Google erstellte Infoboxen, die neben den Suchergebnissen eingeblendet werden. Im Rahmen seiner Zuständigkeit als Aufsichtsbehörde prüft der HmbBfDI nicht nur, ob einzelne Suchergebnisse auszulisten sind, sondern z.B. auch, ob Informationen in Infoboxen angezeigt werden dürfen. Wir stellen einige der im Berichtszeitraum bearbeiteten Beschwerden betroffener Personen dar.

Um eine Infobox (sog. Knowledge Graph) zu erstellen, bedient sich Google verschiedenster Quellen, nicht nur solcher, die im Internet veröffentlicht und damit frei zugänglich sind. Das Unternehmen erwirbt auch Lizenzen, beispielsweise von Verlagen mit Bezug auf Informationen zu Büchern. Sind solche Informationen unrichtig, wie in einem vom HmbBfDI im Berichtszeitraum untersuchten Fall, besteht für die Person, über die Google die unrichtige Information verbreitet, ein Löschungs- oder Korrekturanspruch. Gegenstand des gegen die Google LLC aufgrund der Beschwerde einer betroffenen Person

geführten Verwaltungsverfahrens ist hier u.a. der Umstand, dass Meldungen über die von Google bereitgestellte Feedback-Funktion nach Ansicht des HmbBfDI nicht adäquat bearbeitet wurden. In dem der Beschwerde zugrunde liegenden Fall waren die von einem Buchverlag erhaltenen Informationen über eine Buchveröffentlichung offensichtlich unrichtig. Die Beschwerdeführerin meldete an Google bereits im Jahr 2018, dass sie das Buch niemals veröffentlicht hatte, woraufhin eine Löschung der Angaben erfolgte. Im Jahr 2021 erhielt Google die gleiche, nach Auffassung des HmbBfDI offensichtlich unrichtige Information vom Verlag und veröffentlichte diese – automatisiert – erneut. Da die betroffene Beschwerdeführerin eine Löschung hier nicht erzielen konnte, erwirkte der HmbBfDI die Löschung der Angaben und vertritt zudem die Auffassung, dass die erneute Anzeige der Falschinformation durch geeignete Maßnahmen bei Google hätte verhindert werden können. Der HmbBfDI hat aufgrund des Sachverhalts gegenüber Google eine Verwarnung ausgesprochen.

Wenn bei der Suche des eigenen Namens in der Google Suche Ergebnisse mit anstößigen, sexuellen Inhalten angezeigt werden, ist dies für betroffene Personen eine starke Belastung. Dem HmbBfDI liegen mehrere Beschwerden vor, in denen solche Suchergebnisse, in denen es zu einer missbräuchlichen Namensnutzung kommt, an Google gemeldet wurden. Dabei wird z.T. der Name sogar in der Seitenvorschau (Snippet) in der Ergebnisliste der Google Suche angezeigt. Bleibt es bei vereinzelten Suchergebnissen, kann das sog. notice-and-take-down-Verfahren Abhilfe schaffen, bei dem die betroffene Person das Suchergebnis meldet und Google es aus der angezeigten Ergebnisliste bei einer Namenssuche entfernt. Dem HmbBfDI liegt allerdings die Beschwerde einer betroffenen Person vor, für welche die Meldung aufgrund der Vielzahl der immer wieder auftauchenden anstößigen Suchergebnisse unter missbräuchlicher Verwendung ihres Namens nicht mehr zumutbar ist. Der HmbBfDI ist der Auffassung, dass eine Verpflichtung Googles besteht, derartige – von Google selbst als Porn Spam bezeichnete – Suchergebnisse zu unterbinden, ohne dass die Beschwerdeführerin jedes neue

Suchergebnis zu melden hat. Die vom HmbBfDI eingeforderten und umgesetzten Bemühungen Googles, derartige Suchergebnisse mittels einer Verbesserung der Technologie zur Spam-Unterdrückung zu verhindern, haben sich aus Sicht des HmbBfDI als nicht effektiv genug erwiesen. Auch in diesem Fall ist die Prüfung aufsichtsrechtlicher Maßnahmen gegen die Google LLC zum Berichtszeitpunkt im Wesentlichen abgeschlossen.

Es kommt vor, dass beschwerdeführende Personen den HmbBfDI für verpflichtet halten, wegen der Weigerung Googles, einzelne Suchergebnisse zu löschen, gegen das Unternehmen einzuschreiten. Lehnt der HmbBfDI eine Anordnung gegen Google ab, da er kein Vorliegen eines Löschungsanspruchs aus Art. 17 DSGVO fest stellen konnte, besteht die Möglichkeit, den ablehnenden Bescheid des HmbBfDI vor dem Verwaltungsgericht Hamburg (VG) anzugreifen. Im Berichtszeitraum wurde ein solcher ablehnender Bescheid des HmbBfDI gerichtlich angegriffen. Google hatte sich geweigert, Suchergebnisse auszulisten, in denen über ein gegen den Beschwerdeführer in einem asiatischen Land geführtes Gerichtsverfahren wegen Kindesmissbrauchs und seine Verurteilung berichtet wird. Der Beschwerdeführer beanstandet die Berichterstattung u.a. als unrichtig. Bei seiner Entscheidung wird das VG auch die Entscheidung des Europäischen Gerichtshofs (EuGH) vom 8.12.2022 (C-460/20) zu berücksichtigen haben. Die Entscheidung erging aufgrund einer Vorlage des Bundesgerichtshofs (BGH VI ZR 476/18) . Danach obliegt es der die Auslistung begehrenden Person nachzuweisen, dass in einem Suchergebnis enthaltene Informationen offensichtlich unrichtig sind. Der EuGH betont, dass es nicht erforderlich sei, die Unrichtigkeit von Informationen in einem gerichtlichen Verfahren gegen den Inhalteanbieter selbst, etwa ein Pressemedium, zu belegen. Doch müssten dem Suchmaschinenbetreiber andere „relevante und hinreichende" Nachweise für die Unrichtigkeit der Behauptungen vorgelegt werden. Der BGH hatte sich im Jahr 2020 (VI ZR 405/18) von einem ähnlich strengen Maßstab abgewandt zugunsten einer umfassenden Grundrechtsabwägung unter Geltung der DSGVO. Dem ersten Anschein nach

stellt der EuGH nunmehr (wiederum) höhere Anforderungen an betroffene Personen, eine für den Suchmaschinenbetreiber erkennbare Rechtsverletzung darzulegen. Die Auswirkungen dieser Rechtsprechung auf die Auslistungspraxis Googles bleiben abzuwarten.

IV. BUSSGELDER, ANORDNUNGEN GERICHTSVERFAHREN

IV. Bußgelder, Anordnungen, Gerichtsverfahren

1. Übersicht über Bußgeldverfahren

Im Berichtszeitraum hat der HmbBfDI eine Reihe von Ordnungswidrigkeitenverfahren durchgeführt.

Eine neue Fallgruppe ist im Zusammenhang mit der Verarbeitung von Gesundheitsdaten durch Corona-Testcenter zu Tage getreten. Die überwiegende Zahl der Testcenter hat datenschutzrechtliche Vorgaben beachtet. In einigen Fällen, denen wir aufgrund von Beschwerden nachgegangen sind, mussten wir jedoch Mängel feststellen. In einem Teil dieser Fälle war die Einleitung von Ordnungswidrigkeitenverfahren angezeigt (s. hierzu unter IV 5).

Auch in diesem Berichtszeitraum kam es wieder in mehreren Fällen zu Abfragen personenbezogener Daten von Bürger:innen aus polizeilichen Datenbanken zu privaten Zwecken durch Polizeibeamt:innen. Dabei ist es mittlerweile geübte Praxis des HmbBfDI, ohne weitere Zwischenschritte Ordnungswidrigkeitenverfahren einzuleiten. An dieser Praxis wird der HmbBfDI auch in Zukunft festhalten. Polizist:innen der Freien und Hansestadt Hamburg stehen Hoheitsrechte zu, welche den Zugang zu sensiblen Datenverarbeitungssystemen einschließen. Die Ausnutzung dieser besonderen Zugriffsrechte für private Zwecke ist geeignet, das erforderliche Vertrauen in die Sicherheitsbehörden zu erschüttern.

Regelmäßig müssen auch solche Unternehmen mit der Einleitung von Ordnungswidrigkeitenverfahren rechnen, die hartnäckig Betroffenenrechte, wie etwa Auskunftsansprüche oder Löschungsersuchen, ignorieren. Geldbußen sind insbesondere angezeigt, wenn eine Vielzahl personenbezogener Daten verarbeitet wird und eine konstruktive Zusammenarbeit mit dem HmbBfDI zur Abhilfe von datenschutzwidrigen Zuständen nicht erfolgt. Im Berichtszeitraum hat der HmbBfDI dementsprechende Bußgelder verhängt.

Weiterhin hat der HmbBfDI ein Ordnungswidrigkeitenverfahren im Zusammenhang mit der Nutzung einer Dash-Cam im Straßenverkehr durchgeführt (s. hierzu detailliert unter IV 2), ebenso bei fehlerhaften Entsorgungen von Zustellerlisten durch ein Logistik-Unternehmen (s. hierzu IV 3) sowie bei der Verarbeitung personenbezogener Daten von Kindern in einer Badesituation durch das Filmen mit einer Handykamera. Letzteres Verfahren war aus tatsächlichen Gründen einzustellen. Der HmbBfDI wird indes bei gleichgelagerten Fällen, in denen vulnerable Gruppen in besonderen Situationen gefilmt werden, Ordnungswidrigkeitenverfahren einleiten.

2. Bußgeld wegen des Betriebs einer Dashcam im Straßenverkehr

Der Betrieb einer Dashcam in einem Kraftfahrzeug zur Dokumentation von Unfallhergängen oder dem Fehlverhalten anderer Verkehrsteilnehmer:innen ist nur anlassbezogen zulässig. Bei einem anlasslosen Dauerbetrieb einer Dashcam im Straßenverkehr droht ein empfindliches Bußgeld.

Im Berichtszeitraum verhängte der HmbBfDI erstmalig ein Bußgeld wegen des rechtswidrigen Betriebs einer Dashcam.

Zu Beginn des Jahres 2022 erhielt der HmbBfDI eine Ordnungswidrigkeitenanzeige von der Polizei Hamburg. Polizeibeamt:innen hatten bei einer Fahrzeugkontrolle festgestellt, dass in der Windschutzscheibe eines Pkw eine Dashcam angebracht und eingeschaltet war. Der Fahrzeugführer räumte gegenüber den Polizeibeamt:innen ein, dass die Kamera während der gesamten Fahrt aufzeichnen würde. Dies wurde durch die Auswertung der beschlagnahmten Dashcam-Speicherkarte auch belegt. Bei jedem Starten des Fahrzeugs wurde eine neue Videodatei erzeugt und gespeichert. Auf nahezu allen gespeicherten Videos waren Kfz-Kennzeichen anderer Verkehrsteilnehmer:innen sowie Fußgänger:innen und Radfahrer:innen deutlich zu erkennen, also durchweg personenbezogene Daten von Bürger:innen verarbeitet worden.

Eine durchgängige und anlasslose Videoaufzeichnung des Verkehrsgeschehens ist schon nicht erforderlich, um ein Beweissicherungsinteresse von Fahrzeugführer:innen (z. B. für die Beweissicherung im Falle eines Unfalls oder einer Beschädigung des eigenen Fahrzeugs) zu wahren. Hierfür genügt es, wenn ausschließlich die relevante Situation dauerhaft festgehalten wird. Ferner überwiegt grundsätzlich das Interesse anderer Verkehrsteilnehmer:innen, im öffentlichen Straßenraum nicht permanent Gegenstand von Videoaufzeichnungen zu sein, zumal sie die Videoaufzeichnung in der Regel nicht einmal erkennen können und durch ihr Verhalten auch keinen Anlass für die Aufzeichnung gegeben haben. Eine permanente und anlasslose Aufzeichnung des Verkehrsgeschehens im öffentlichen Raum mit einer Dashcam ist daher auch nach der Rechtsprechung des Bundesgerichtshofs unzulässig (BGH, Urt. v. 15.5.2018 – VI ZR 233/17).

Wer eine Kamera in seinem Fahrzeug in Betrieb hat, muss somit sicherstellen, dass diese Kamera lediglich anlassbezogen das Geschehen im öffentlichen Straßenraum in Form eines Videos dauerhaft speichert. Schon seit geraumer Zeit unterstützen viele Dashcam-Modelle eine anlassbezogene Speicherung von Aufnahmen. Die Aufnahmen werden in einem Ringspeicher abgelegt, der in kurzen Abständen durch Überschreiben immer wieder gelöscht wird, wenn kein Anlass für eine dauerhafte Speicherung gegeben ist. Durch integrierte Sensoren kann etwa bei starkem Abbremsen oder ähnlichem eine dauerhafte Speicherung des Videos ausgelöst werden. Diese Funktion hatte auch die Dashcam des Fahrzeugführers. Er hatte sie jedoch nicht aktiviert.

Der HmbBfDI hat wegen dieses Verstoßes ein Bußgeld im mittleren dreistelligen Bereich verhängt. Der Fahrzeugführer legte Einspruch ein. Nach Erörterung der Sach- und Rechtslage in der Hauptverhandlung vor dem Amtsgericht Hamburg nahm der Fahrzeugführer den Einspruch gegen den Bußgeldbescheid zurück. Die Vorsitzende Richterin erläuterte ferner, dass jede abgeschlossene Fahrt eine Tat im Sinne des Ordnungswidrigkeitenrechts sei und die Fahrten folglich tatmehrheitlich zu behandeln seien. Eine massenhafte und ggf. über Jahre andau-

ernde Speicherung von Videodateien des öffentlichen Straßenraums kann somit zu einem erheblichen Bußgeld führen, da für jede anlasslos gespeicherte Fahrt ein gesondertes Bußgeld festzusetzen wäre.

3. Bußgeld wegen Fehlentsorgung bei Logistik-Unternehmen

Der HmbBfDI hat gegen ein hamburgisches Logistikunternehmen einen Bußgeldbescheid erlassen. Anlass der Sanktion waren wiederholte Ent sorgungen sog. Zustellerlisten in öffentlichen Abfallbehältnissen sowie ein mangelhaftes Entsorgungskonzept. Der Bußgeldbescheid ist noch nicht rechtskräftig.

Mitarbeiter:innen eines hamburgischen Logistikunternehmens hatten in zwei Fällen sog. Zustellerlisten in frei zugänglichen, öffentlichen Abfallbehältern entsorgt. Unberechtigte Dritte konnten diese somit einsehen. Die Listen enthielten die Vor- und Nachnamen von Abonnent:innen, die Adressen, abonnierten Zeitungen sowie besondere Zustellhinweise, etwa zur Lage von Briefkästen und etwaigen Beschwerden der Empfänger:innen. Die Listen enthielten dadurch eine nicht unbeträchtliche Zahl von detaillierten Informationen über die Personen auf der Liste.

Bei der Prüfung wurde darüber hinaus festgestellt, dass das Konzept zur Entsorgung derartiger Listen unzureichend war. Insbesondere war es den Zusteller:innen überlassen, die Listen selbstständig zu entsorgen, ohne dass ein Rücklauf der Zustellerlisten vorgesehen war. Eine wirksame Kontrolle einer ordnungsgemäßen Entsorgung war dem Unternehmen damit nicht möglich. Es bestand folglich auch nicht die Möglichkeit, verlässlich den Meldepflichten aus Art. 33 und 34 DSGVO nachzukommen, die eine Meldung bei Datenpannen erfordern.

Das Unternehmen hat damit einerseits im Hinblick auf die konkreten Entsorgungen gegen Art. 32 Abs. 1 DSGVO verstoßen, anderer-

seits war das fehlerhafte Entsorgungskonzept zu sanktionieren. Eine Geldbuße war auch deshalb angezeigt, da bereits 2019 aufgrund eines gleichgelagerten Sachverhalts eine Verwarnung im Sinne des Art. 58 Abs. 2 lit. b) DSGVO gegenüber dem Unternehmen ausgesprochen wurde.

Gleichwohl hat das Unternehmen mit dem HmbBfDI zur Aufklärung der Verstöße zusammengearbeitet, was bei der Bußgeldbemessung in erheblicher Weise zu berücksichtigen war. Darüber hinaus wurden die Informationsmaterialien für die Zusteller:innen zur datenschutzkonformen Entsorgung von Zustelllisten überarbeitet, um künftigen Verstößen besser vorzubeugen. Ein wirtschaftlicher Schaden der Abonnent:innen war letztlich nicht feststellbar. Auf der anderen Seite zog das Unternehmen einen wirtschaftlichen Vorteil aus dem mangelhaften Entsorgungskonzept in Form ersparter Kosten für eine eigene ordnungsgemäße Entsorgung der Listen. Die Geldbuße war insofern moderat zu bemessen. Gegen den Bußgeldbescheid hat das Unternehmen Einspruch eingelegt.

4. Anordnung einer Auskunftserteilung

Ein Unternehmen erhielt einen Antrag auf Übermittlung einer Datenkopie hinsichtlich bestimmter personenbezogener Daten der antragstellenden Person, reagierte jedoch weder hierauf noch auf entsprechende Aufforderungen des HmbBfDI. Der HmbBfDI erließ daher eine Anweisung zur Erteilung dieser Datenkopie unter Androhung eines Zwangsgeldes bei Nichtumsetzung.

Ein Unternehmen erhielt einen Antrag auf Übermittlung einer Datenkopie hinsichtlich bestimmter personenbezogener Daten der antragstellenden Person, reagierte jedoch weder hierauf noch auf entsprechende Aufforderungen des HmbBfDI. Der HmbBfDI erließ daher eine Anweisung zur Erteilung dieser Datenkopie unter Androhung eines Zwangsgeldes bei Nichtumsetzung.

Den HmbBfDI erreichte eine Beschwerde, nach welcher ein Unternehmen einen Antrag auf Auskunft und Datenkopie nach Art. 15 Abs. 1 und 3 DSGVO ignoriert habe. Diese Datenkopie bezog sich auf Daten über Buchungsvorgänge, die das Unternehmen in seinem Finanzbuchhaltungssystem zu dem Beschwerdeführer gespeichert hatte. Da sich diese Daten auf den Beschwerdeführer und auch die jeweiligen Buchungsvorgänge unter dem namentlich zum Beschwerdeführer angelegten Buchungskonto bezogen, zählen auch diese Daten zu den personenbezogenen Daten im Sinne von Art. 4 Nr. 1 DSGVO. Nachdem der HmbBfDI das Unternehmen schriftlich auf die Pflicht zur Beachtung geltend gemachter Betroffenenrechte hingewiesen hat, erteilte das Unternehmen dem Beschwerdeführer eine Auskunft nach Art. 15 Abs. 1 DSGVO. In der Folge reagierte das Unternehmen jedoch auf weitere schriftliche Kommunikationsversuche und Aufforderungen des HmbBfDI, dem Beschwerdeführer ergänzend auch die begehrte Datenkopie zukommen zu lassen, nicht mehr.

Der HmbBfDI erließ daher eine Anweisung nach Art. 58 Abs. 2 lit. c) DSGVO und forderte das Unternehmen darin auf, eine Kopie der vom Beschwerdeführer nach Art und Zeitraum genau konkretisierten Daten an diesen herauszugeben. Für den Fall der Nichtumsetzung der Maßnahme binnen 2 Wochen wurde ein Zwangsgeld in Höhe von 5.000,00 Euro angedroht. Diese Maßnahme hatte Erfolg. Das Unternehmen setzte sich nach Erhalt des Bescheides umgehend mit dem HmbBfDI zur Erfüllung der Anweisung mit dem Ziel der Abwendung der Zwangsgeldzahlung in Verbindung. Die Zusammenarbeit verlief daraufhin sehr kooperativ. Das Unternehmen leitete alle erforderlichen Maßnahmen in die Wege, um dem Beschwerdeführer sämtliche zu ihm in dem Finanzbuchhaltungssystem vorliegenden Daten in Kopie herauszugeben. Den ausgelösten behördlichen Aufwand hatte das Unternehmen durch eine erhöhte Bearbeitungsgebühr zu tragen.

5. Bußgeldverfahren bzgl. Covid-Testcenter

Während der pandemischen Lage wurden eine Vielzahl sog. Coro na-Testcentren eingerichtet und betrieben. Nicht alle Testcentren haben dabei datenschutzrechtlichen Mindeststandards entsprochen. In weni-gen Fällen hatten die Verstöße ein Ausmaß erreicht, das die Durchfüh rung von Ordnungswidrigkeitenverfahren erforderlich machte.

Die Testcenter waren unterschiedlicher Natur. Bei einigen handelte es sich um Arztpraxen, die zusätzlich zur regulären Versorgung von Patient:innen auch Testungen anboten. In einer solchen Praxis hatten Beschäftigte schriftliche Nachweise über positive und negative Covid-19 Antigen Rapid Testergebnisse von Patient:innen in einem Müllsack neben einem öffentlichen Altglascontainer abgestellt. Es gab keinerlei Schutz gegen eine Kenntnisnahme durch Dritte. Zwar hat der HmbBfDI berücksichtigt, dass in der grassierenden Pandemie zahlreiche Arztpraxen geschlossen hatten oder zumindest nur noch eingeschränkt geöffnet waren. Durch die angespannte Lage kam es zu einer deutlichen Mehrbelastung auch der hier betroffenen Praxis. Aufgrund der Tatsache, dass hier mit Gesundheitsdaten im Sinne von Art. 9 DSGVO sorglos umgegangen wurde und eine Vielzahl von Personen betroffen war, konnte der HmbBfDI dennoch nicht von der Durchführung eines Ordnungswidrigkeitenverfahrens absehen. Es wurde eine Geldbuße in Höhe von 1.000 € verhängt, die von der Praxis auch akzeptiert wurde.

In einem anderen Fall hatte der HmbBfDI Beschwerden über ein reines Testcenter vorliegen, das sich dem Recht auf Löschung von getesteten Personen konsequent verweigerte. Nun führt längst nicht jeder Verstoß gegen ein Betroffenenrecht automatisch zur Verhängung eines Bußgelds, auch wenn Gesundheitsdaten im Sinne von Art. 9 DSGVO betroffen sind. In diesem Fall schien das Vorgehen aber Methode zu haben. Auch als der HmbBfDI sich bei dem Unternehmen

meldete und ein Verwaltungsverfahren einleitete, änderte sich nichts am Verhalten des Testcenters. Die Anfragen und Aufforderungen wurden konsequent ignoriert. Der HmbBfDI hat deshalb ein Bußgeld in Höhe von 1.000 € verhängt. Das Unternehmen hat diese Geldbuße akzeptiert. Verantwortliche, die massenhaft personenbezogene Daten verarbeiten und dabei Betroffenenrechte missachten, müssen auch in Zukunft mit der Einleitung von Ordnungswidrigkeitenverfahren durch den HmbBfDI rechnen.

In einem weiteren Fall hatte ein drittes Testcenter die Testergebnisse mittels URL zum Abruf bereitgehalten. Getesteten Personen wurde per unverschlüsselter E-Mail eine URL übermittelt, unter der ohne weitere Sicherungsmaßnahmen das Testergebnis abgerufen werden konnte. Der Abruflink war dabei in mindestens 189 Fällen so aufgebaut, dass der Pfad zum Download einer PDF-Datei führte und der Dateiname dem Nachnamen der getesteten Person entsprach. Mit Kenntnis des Verzeichnispfads war es daher möglich, Einsicht in Testergebnisse Dritter zu nehmen. Es musste einfach nur der Nachname durch einen beliebigen anderen Nachnamen ersetzt werden. Hierbei handelte es sich offensichtlich um einen Verstoß gegen die Pflicht zur ordnungsgemäßen Sicherung von personenbezogenen (Gesundheits-)Daten durch angemessene technisch-organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO. Der HmbBfDI hat diesen Verstoß mit einer Geldbuße in Höhe von 2.700 € geahndet.

Der letzte der hier beschriebenen Fälle betraf ein Testcenter, das sich gegenüber Nachfragen der Kassenärztlichen Vereinigung absichern wollte. Zu diesem Zweck wurden Vorder- und Rückseite von Personalausweisen getesteter Personen gescannt und auf einer externen Festplatte gespeichert. Allerdings wären zur Dokumentation allein diejenigen personenbezogenen Daten zu speichern gewesen, die in § 7 Abs. 5 Nr. 5 sowie §§ 2 bis 4b Coronavirus-Testverordnung aufgeführt sind. Für die übrigen Speicherungen bestand insofern keine rechtliche Verpflichtung i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c) DSGVO und sie war daher unzulässig, was dem Testcenter durch eine einfache Gesetzeslektüre auch hätte bekannt sein können und müs-

sen. Die Speicherung vollständiger Personalausweise ist nicht nur übertrieben, sondern birgt auch nicht unerhebliche Gefahren für die Betroffenen. Fallen diese Speicherungen in die falschen Hände sind den Missbrauchsmöglichkeiten kaum noch Grenzen gesetzt. Eine konstruktive Zusammenarbeit des Unternehmens mit dem HmbBfDI mit dem Ziel, die datenschutzwidrigen Zustände zu beseitigen, fand darüber hinaus nicht statt. Der HmbBfDI hat daher eine Geldbuße in Höhe von rund 1.400 € verhängt.

6. „Videmo" – Beschwerde gegen die Nichtzulassung der Berufung vor dem OVG Hamburg erfolgreich

Kurz vor Redaktionsschluss hat das OVG Hamburg seine Entscheidung im Verfahren „Videmo" bekannt und dem Antrag des HmbBfDI auf Zulassung der Berufung stattgegeben (OVG Hamburg Beschl. v. 15.12.2022 3 Bf 46/20.Z). Grundsatzfragen der Prüfbefugnisse des HmbBfDI gegenüber öffentlichen Stellen können nun höchstrichterlich geklärt werden.

Dem Verfahren liegt der Einsatz der Gesichtserkennungssoftware „Videmo" durch die Polizei Hamburg zugrunde. Zur Aufklärung von Straftaten rund um den G20-Gipfel im Jahre 2017 kam die Software zum Einsatz und erforderte die Verarbeitung massenhafter biometrischer Daten (s. hierzu die Darstellungen im TB Datenschutz 2020, Kapitel V 4 und TB Datenschutz 2021, Kapitel IV 7).

Das OVG Hamburg hat nunmehr festgestellt, dass die Vernichtung der Festplatten, auf denen sich die Referenzdatenbank befand, durch die Polizei Hamburg und die dadurch eingetretene Erledigung der streitgegenständlichen datenschutzrechtlichen Löschungsanordnung vom 18. Dezember 2018 das Rechtsschutzinteresse des HmbBfDI nicht entfallen ließen.

Insbesondere sei der HmbBfDI durch die für ihn nachteilige Entscheidung erster Instanz beschwert. Der HmbBfDI habe trotz der zwischenzeitlich eingetretenen Erledigung ein berechtigtes Interesse daran, dass eine gegen ihn ergangene ungünstige Entscheidung aufgehoben oder für unwirksam erklärt werde. Diese Folgerungen können nur erreicht werden, wenn die Berufung zugelassen werde.

Darüber hinaus sei der Zulassungsantrag auch begründet, da der HmbBfDI die Frage aufgeworfen habe, welcher Prüfungsumfang und welche Befugnisse ihm nach § 43 HmbJVollzDSG gegenüber anderen öffentlichen Stellen eingeräumt werden. Dies umfasse auch die Frage, welche Rechte ihm bei der Prüfung der der Datenverarbeitung zugrundeliegenden Rechtsgrundlage zukommen würden. Diese Rechtsfragen seien höchstrichterlich nicht geklärt und aufgrund der unionsrechtlichen Determinierung insbesondere unter Beachtung des einschlägigen unionsrechtlichen Primär- und Sekundärrechts und im Lichte der Rechtsprechung des Europäischen Gerichtshofs zu bewerten.

Wir werden über den Ausgang des Berufungsverfahrens in einem der nächsten Tätigkeitsberichte berichten.

GRENZÜBERSCHREITENDE THEMEN V.

V. Grenzüberschreitende Themen

1. Hacking-Fälle bei Facebook/Instagram

Stellen Sie sich vor, Sie sind der Inhaber eines kleinen Ladengeschäfts. Eines Morgens stehen Sie vor Ihrem Geschäft und stellen plötzlich fest, dass Ihr Schlüssel nicht mehr die Eingangstür öffnet. Verdutzt stellen Sie fest, dass sich ein unbefugter Dritter Zugang zu Ihrem Geschäft ver schafft hat und dieser offenbar das Türschloss ausgetauscht hat. Darü ber hinaus müssen Sie zur Kenntnis nehmen, dass dieser Dritte nunmehr Ihr Geschäft dazu nutzt, unter Ihrem Namen eigene, fragwürdige Pro dukte zu verkaufen und diese zugleich auch im Schaufenster zu bewer ben. So oder ähnlich ergeht es von Hacking betroffenen Nutzer:innen sozialer Netzwerke. Welche Möglichkeiten haben die Betroffenen hier? Kann der Datenschutz eine mögliche Lösung bieten?

Nachfolgend sollen hier ausschließlich die Möglichkeiten der Bearbeitung in Bezug auf gehackte Nutzerkonten bei den sozialen Netzwerken „Facebook“ und „Instagram“ dargestellt werden. Bei den genannten Netzwerken handelt es sich nicht nur um sehr weit verbreitete soziale Netzwerke mit jeweils über einer Milliarde Nutzer:innen. Im Zusammenhang mit der hiesigen Fallbearbeitung kommt mit der grenzüberschreitenden Verarbeitung der Daten der Nutzer:innen eine weitere erschwerende Komponente hinzu.

Art. 4 (23) DSGVO definiert die grenzüberschreitende Verarbeitung für folgende zwei Anwendungsfälle: der Verantwortliche hat Niederlassungen in mehreren Mitgliedstaaten und die Verarbeitung bezieht sich auf mehrere solche (a), oder die Verarbeitung bezieht sich nur auf eine Niederlassung, hat aber Auswirkungen in mehreren Mitgliedstaaten (b).

Zu gehackten Nutzerkonten auf diesen beiden sozialen Netzwerken erreichten den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) auch im Jahr 2022 nach wie vor eine Vielzahl von Beschwerden.

Verantwortlich für die Dienste Facebook und Instagram im Sinne der DSGVO ist die Meta Platforms Ireland Limited (Meta). Seit Geltung der DSGVO ist somit nicht der HmbBfDI, sondern die irische Datenschutzbehörde (Irish Data Protection Commission - IDPC) federführend für Meta zuständig.

Der HmbBfDI kann daher derartige Beschwerden mangels eigener Zuständigkeit nicht selbst bearbeiten, sondern muss diese der IDPC zur Entscheidung vorlegen. Dies umfasst u.a. die Übersetzung der von den Betroffenen eingereichten Unterlagen ins Englische, das Einstellen in ein gemeinsames Austauschportal der europäischen Aufsichtsbehörden, die anschließende Sichtung und Bearbeitung des jeweiligen Falls durch die IDPC, die Übermittlung von eventuellen Rückfragen der IDPC an die Betroffenen sowie die Rückübersetzung der letztlichen Entscheidung der IDPC und deren Übermittlung an die Betroffenen.

Auch aufgrund der Vielzahl der Beschwerden zu Facebook und Instagram ist dies für die Betroffenen mit erheblichen Wartezeiten verbunden. Erfahrungsgemäß ist mit einer Bearbeitungsdauer von circa zwei Jahren bis zu einer endgültigen Entscheidung durch die IDPC zu rechnen. Diese lange Bearbeitungsdauer ist für die Betroffenen, welche sich natürlich eine möglichst zeitnahe Lösung ihres Anliegens wünschen, äußerst frustrierend und belastend.

Wenn Betroffene jedoch möglichst schnell ihren Account ohne Prüfung wiedererlangen oder löschen möchten, hat der HmbBfDI gemäß des Erwägungsgrundes 131 DSGVO die Möglichkeit, Meta direkt zu kontaktieren und im Rahmen eines gütlichen Verfahrens zu versuchen, eine Einigung mit Meta zu erzielen. Die Erfahrungen des HmbBfDI mit diesem Verfahren waren in der Vergangenheit mehrheitlich positiv. Hier konnte der HmbBfDI in einer Vielzahl von Fällen ein für die Betroffenen positives und zeitnahes Ergebnis erreichen.

Voraussetzung für die Möglichkeit eines derartigen Verfahrens ist, dass eine andere Aufsichtsbehörde als federführende Aufsichtsbe-

hörde für die Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters fungieren sollte, der konkrete Gegenstand einer Beschwerde oder der mögliche Verstoß nur die Verarbeitungstätigkeiten des Verantwortlichen oder des Auftragsverarbeiters in dem Mitgliedstaat betrifft, in dem die Beschwerde eingereicht wurde oder der mögliche Verstoß aufgedeckt wurde, und die Angelegenheit keine erheblichen Auswirkungen auf betroffene Personen in anderen Mitgliedstaaten hat oder haben dürfte. Diese Voraussetzungen liegen in Hacking-Fällen in der Regel vor.

Nach deutschem Rechtsverständnis bedarf es zu einer derartigen Einigung zweier Willenserklärungen der Parteien. Die Einigung wird dem Verständnis des HmbBfDI nach ausschließlich zwischen Verantwortlichen und Betroffenen (und nicht etwa der Aufsichtsbehörde) erzielt. Daher ist in jedem Fall vor dem Versuch einer gütlichen Einigung eine ausdrückliche Einwilligung der betroffenen Person für dieses verfahrensbeendende Vorgehen einzuholen.

Bei einer erfolgreichen Einigung wird die Beschwerde ohne einen formalen Abschluss als erledigt angesehen. Sollte keine Einigung erzielt werden können, wird die Beschwerde wie oben beschrieben an die IDPC weitergeleitet. Ein erfolgloser Versuch einer gütlichen Einigung bringt den Betroffenen daher prozessual keinen Nachteil.

Allerdings gilt auch hier der Grundsatz, dass Betroffene die ihnen von der DSGVO zugeschriebenen Rechte zunächst selbst gegenüber dem verantwortlichen Unternehmen – hier Meta – wahrnehmen müssen. Sofern die Betroffenenrechte sodann von Meta nicht oder nicht vollständig erfüllt werden, kann eine Beschwerde beim HmbBfDI eingereicht werden.

2. Instagram-Bußgeld über 405 Mio Euro

Lange Zeit hatte Instagram auch Jugendlichen im Alter von 13 bis 17 Jahren sogenannte Businesskonten ohne Altersverifikation angeboten, mit der Folge, dass Kontaktdaten der Minderjährigen oft aus Unkenntnis weltweit für jedermann abrufbar waren. Diese Praxis wurde nach einigem Ringen auf europäischer Ebene nun als datenschutzwidrig eingestuft und mit einem Bußgeld in Höhe von 405 Mio Euro geahndet. Der HmbBfDI nahm dabei zwei entscheidende Weichenstellungen vor.

Instagram ist ein weltweit sehr beliebter Dienst, auch unter den Minderjährigen in Europa. Diese konnten ab 2016 das neu eingeführte Business-Konto anlegen bzw. dazu wechseln, da dieses unter anderem keine Altersbeschränkungen vorsah. Für die üblichen persönlichen Konten schreibt Instagram ein Mindestalter von 13 Jahren vor. Dieses wird durch die Abfrage des Geburtsdatums im Rahmen der Kontoregistrierung überprüft.

Bei Business-Konten müssen eine E-Mail-Adresse oder eine Telefonnummer als Kontaktinformation angegeben werden, während dies bei den persönlichen Konten nicht vorgesehen ist. Business-Konten sind per Einstellung öffentlich, während persönliche Konten so eingestellt werden können, dass nur sogenannte Follower das jeweilige Profil einsehen können.

Ein kanadischer Sicherheitsforscher stellte fest, dass die Kontaktinformationen von Business-Konten beim Aufruf per Web-Browser im Quellcode der Seite einsehbar waren. Erkennbar befanden sich darunter viele Nutzer:innen im Alter zwischen 13 und 17 Jahren. Die auffällige Menge der minderjährigen Nutzer:innen wies auf ein erhebliches Sicherheits- und Datenschutzproblem hin. Offenbar war vielen Nutzer:innen die Konsequenz des Wechsels von einem persönlichen zu einem Business-Konto nicht bewusst. Im Ergebnis waren die Kontaktdaten Minderjähriger ohne ihre Kenntnis oder Einwilligung damit für jedermann abrufbar.

Der Sicherheitsforscher meldete das Problem zunächst bei Instagram und reichte einen Hinweis auf eine Datensicherheitsverletzung bei der irischen Aufsichtsbehörde (kurz IDPC) ein. Nachdem er mit der dortigen Reaktion unzufrieden war, wandte er sich im Juli 2019 zusätzlich an den HmbBfDI, der sich im Rahmen der europäischen Zusammenarbeit umgehend an die IDPC als federführende Behörde für Instagram wandte. Daraufhin leitete die IDPC noch im August 2019 Untersuchungen von Amts wegen ein und legte schließlich im Dezember 2021 einen Beschlussentwurf vor. Dort kam sie zu dem Ergebnis, dass Instagram Jugendliche besser über die Voreinstellungen bei Business-Konten hätte aufklären müssen. Der Beschlussentwurf sah hierfür eine Verwarnung sowie Bußgelder für eine Reihe von Verstößen vor.

Der Beschlussentwurf blieb hinter den Erwartungen des HmbBfDI zurück. Das Kooperationsverfahren nach Art. 60 ff. DSGVO sieht vor, dass Entscheidungen von grenzüberschreitender Bedeutung unter den betroffenen europäischen Aufsichtsbehörden abgestimmt werden und dem Standpunkt der betroffenen Behörden gebührend Rechnung tragen. Dies war jedoch aus mehreren Gründen nicht der Fall. Dementsprechend legte der HmbBfDI gemeinsam mit anderen deutschen Aufsichtsbehörden einen koordinierten Einspruch nach Art. 60 Abs. 4 DSGVO gegen den Beschlussentwurf aus Irland ein. Unter anderem wurde geltend gemacht, dass ohne eine wirksame Einwilligung für die Verarbeitung der Daten von Minderjährigen keine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO bestand und daher auch dieser Verstoß gegen die DSGVO mit einem Bußgeld sanktioniert werden müsste, was bis dato fehlte. Ähnliche Einsprüche wurden auch von anderen europäischen Aufsichtsbehörden eingelegt.

Die IDPC ist den Einsprüchen zu ihrem Beschlussentwurf nicht gefolgt und legte ihn entsprechend dem Europäischen Datenschutzausschuss (EDSA) im Rahmen des Kohärenzverfahrens nach Art. 65 Abs. 1 Buchst. a DSGVO zur Klärung vor. Im Rahmen dieses Streitbeilegungsverfahrens prüft der Ausschuss zunächst, ob die Einsprüche die Vorgaben erfüllen, um als maßgebliche und begründete

Einsprüche gewertet werden zu können, und prüft in einem weiteren Schritt, ob die vorgebrachten Argumente überzeugen.

Der Einspruch aus Deutschland hatte beim EDSA im Wesentlichen Erfolg. Er bestätigte die fehlende Rechtsgrundlage und gab der IDPC im Rahmen eines verbindlichen Beschlusses auf, das ursprünglich vorgesehene Bußgeld entsprechend zu erhöhen (https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22022-dispute-arisen_de).

Dementsprechend hat die IDPC einen endgültigen Beschluss gefasst mit der Feststellung, dass Meta Platforms Ireland Limited (kurz Meta, ehemals Facebook) sich nicht auf Art. 6 Abs. 1 Buchst. b noch f DSGVO als Rechtsgrundlage für die Verarbeitung von Kontaktdaten hätte berufen können und so mangels Einwilligung gegen Art. 6 Abs. 1 DSGVO verstoßen hat. Zudem wurden die Bußgelder angepasst, wobei u. a. die von den deutschen Aufsichtsbehörden vorgebrachten Grundlagen und Kriterien zur Bußgeldbemessung zum Tragen kamen. Insgesamt wurden zehn Bußgelder zwischen 20 und 100 Mio. € und mit einer Gesamtsumme in Höhe von 405 Mio. € verhängt. Dagegen hat Meta bereits Rechtsmittel eingelegt.

3. Beschlussentwurf als federführende Aufsichtsbehörde

Der HmbBfDI hatte im Berichtszeitraum zum ersten Mal einer anderen betroffenen Aufsichtsbehörde einen Beschlussentwurf nach Art. 60 Abs. 3 DSGVO vorzulegen, da er als federführende Aufsichtsbehörde für eine Beschwerde mit grenzüberschreitendem Bezug zuständig war. Bei einem ablehnenden Beschlussentwurf wäre mit hoher Wahrscheinlichkeit mit einem Einspruch (Art. 60 Abs. 4 DSGVO) der polnischen Aufsichtsbehörde zu rechnen gewesen. In dem Verfahren konnte jedoch eine gütliche Einigung zwischen Beschwerdeführer und Verantwortlichem erzielt und im Beschlussentwurf festgestellt werden.

Für datenschutzrechtliche Beschwerden über in Hamburg mit Hauptsitz ansässige Unternehmen ist der HmbBfDI als federführende Aufsichtsbehörde (Lead Authority) nach dem sog. One-Stop-Shop-Verfahren (Art. 56 DSGVO) zuständig. Hat die Beschwerde einen grenzüberschreitenden Bezug, muss der HmbBfDI vor einer Entscheidung über die Beschwerde andere betroffene Aufsichtsbehörden konsultieren und sodann den anderen betroffenen Aufsichtsbehörden einen Entscheidungsentwurf (sog. Draft Decision) über die Beschwerde zur Kenntnis zu bringen.

Grundsätzlich haben andere betroffene Aufsichtsbehörden, sofern sie eine abweichende Auffassung vertreten, die Möglichkeit, gegen den Beschlussentwurf einen Einspruch zu erheben. Dies hätte eine Befassung durch den Europäischen Datenschutzausschuss (EDSA) zur Folge.

Der vom HmbBfDI zu erstellende Beschlussentwurf konnte sich darauf beschränken, eine gütliche Einigung (sog. amicable settlement) zwischen dem verantwortlichen Unternehmen und dem Beschwerdeführer festzustellen. Denn das verantwortliche Unternehmen mit Sitz in Hamburg war dem Löschungsbegehren des Beschwerde-

führers zwischenzeitlich nachgekommen. Gegen einen solchen Beschlussentwurf sui generis, welcher weder aufsichtsrechtliche Maßnahmen gegen die verantwortliche Stelle noch eine ablehnende Entscheidung gegenüber dem Beschwerdeführer vorsieht, sollte ein Einspruch durch andere betroffene Aufsichtsbehörden nach dem Verständnis des EDSA in der Regel entbehrlich sein (s. Rz. 40 der entsprechenden Leitlinie, https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202206_on_the_practical_implementation_of_amicable_settlements_en.pdf).

Dem Sachverhalt zugrunde lag die beim HmbBfDI eingelegte Beschwerde eines polnischen Beschwerdeführers über ein Unternehmen, das Registerinformationen in einer Datenbank mit Recherchefunktion veröffentlicht. In den veröffentlichten Informationen aus dem polnischen Handelsregister war im Jahr 2019 der Name des Beschwerdeführers als Geschäftsführer einer Gesellschaft mit der Initiale eines zweiten Vornamens abgebildet, was der Anbieter des Recherchetools in den von ihm erstellten Übersichten mit aufnahm. Die zusätzliche Vornamensinitiale wurde im Jahr 2020 mit Wirkung für die Zukunft aus den polnischen Handelsregistereinträgen entfernt. Die Änderung eines bisherigen Eintrags mit Wirkung für die Vergangenheit ist bei Registereinträgen dagegen nicht möglich.

Der Beschwerdeführer trug vor, die damalige Eintragung sei mit Bezug auf diese Vornamensinitiale fehlerhaft erfolgt. Er weigerte sich jedoch, ein offizielles Dokument vorzulegen, aus welchem sein vollständiger Name (einschließlich etwaiger weiterer Vornamen) hervorging. Der Recherchedienstanbieter hielt zunächst keine Löschung oder Korrektur in seinen Übersichten für angezeigt.

Da nach Auffassung des HmbBfDI der Recherchedienstbetreiber nicht verpflichtet ist, lediglich die aktuellsten Handelsregisterinformationen abzubilden, sondern durchaus auch die früheren Einträge abrufbar halten darf, hielt auch der HmbBfDI keinen Löschungs- oder Korrekturanspruch für gegeben, zumal nicht belegt war, dass die Vornamensinitiale unrichtig war. Er stellte dementsprechend

im Verfahren der informellen Konsultation nach Art. 61 Abs. 1 DSGVO einen Entwurf für einen das Beschwerdebegehren ablehnenden Bescheid in das Binnenmarktinformationssystem (Internal Market Information System, kurz IMI) ein. Hierzu äußerte die polnische Aufsichtsbehörde im Verfahren nach Art. 61 Abs. 1 DSGVO grundlegende Bedenken. Nach ihrer Auffassung hätten die Übersichten korrigiert und die Vornamensinitiale entfernt werden müssen. Hätte der HmbBfDI wie ursprünglich vorgesehen einen den Löschungsanspruch ablehnenden Beschlussentwurf im Verfahren nach Art. 60 Abs. 3 S. 2 DSGVO vorgelegt, wäre daher mit hoher Wahrscheinlichkeit mit einem Einspruch (Art. 60 Abs. 4 DSGVO) der polnischen Aufsichtsbehörde zu rechnen gewesen. Bei weiterhin bestehendem Dissens hätte dies einen verbindlichen Beschluss des EDSA nach Art. 65 Abs. 1 lit. a) DSGVO zur Streitbeilegung erforderlich gemacht.

Der HmbBfDI war als federführende Aufsichtsbehörde verpflichtet, sich im Rahmen des Kooperationsverfahrens um einen Konsens mit der betroffenen polnischen Aufsichtsbehörde zu bemühen. Schließlich erklärte sich der Recherchedienstbetreiber im weiteren Verlauf damit einverstanden, im Sinne einer unkomplizierten Lösung die Vornamensinitiale aus den erstellten Übersichten zu entfernen. Dem HmbBfDI blieb in dem vorzulegenden Beschlussentwurf die Feststellung der gütlichen Einigung. Ein Einspruch gegen den Beschlussentwurf wurde nicht eingelegt.

4. Neues Kapitel im transatlantischen Datenaustausch

Die Europäische Kommission hat einen Angemessenheitsbeschluss für die USA entworfen, nachdem die dortigen Geheimdienstbefugnisse ein geschränkt wurden. Datenübermittlungen würden damit sehr viel einfa cher möglich als in der Zeit nach der Schrems-II-Entscheidung.

Mit der Executive Order vom 07.10.2022 hat der US-Präsident eine Antwort auf die Schrems-II-Entscheidung des Europäischen Gerichtshofs gegeben. Der Rechtsakt adressiert erkennbar die wesentlichen Kritikpunkte des Gerichts an der Rechtslage der Vereinigten Staaten. Auf dieser Grundlage beabsichtigt die Europäische Kommission, den USA den Status eines Drittlands mit angemessenem Datenschutzniveau zuzuerkennen. Im Anschluss könnten Datenexporteure auf eigene rechtliche Lösungen wie Standardvertragsklauseln und gegebenenfalls auch technische Zusatzmaßnahmen verzichten. Wie schon bei vergleichbaren rechtlichen Lösungen in der Vergangenheit wird dabei nicht der Staat als Ganzes in den Genuss der Angemessenheitsentscheidung kommen. Teil des sogenannten Trans Atlantic Data Privacy Framework werden diejenigen Einrichtungen in den USA sein, die sich einer Reihe von festgelegten Datenschutzgarantien unterwerfen und in eine Liste des Handelsministeriums eintragen lassen. Die Einhaltung dieser Prinzipien werden die US-Behörden stichprobenartig überprüfen.

Ein die Angemessenheit feststellender entsprechender Beschlussentwurf ist dem Europäischen Datenschutzausschuss im Dezember 2022 zur Stellungnahme zugeleitet worden. Es ist davon auszugehen, dass die finale Beschlussfassung durch die Kommission im Laufe des Jahres 2023 erfolgen wird. Wenn der Rechtsakt Gesetzeskraft hat, gilt er. Datenexporteure können sich dann darauf berufen. Übermittlungen in die USA werden damit sehr viel einfacher möglich sein als bislang infolge der Schrems-II-Entscheidung des

Europäischen Gerichtshofs. Die Datenschutzbehörden haben keine Verwerfungskompetenz. Lediglich dann, wenn sie im Rahmen einer Einzelfallprüfung davon überzeugt sind, dass ein Angemessenheitsbeschluss rechtswidrig ist, haben sie gemäß § 21 BDSG das Verfahren auszusetzen und den EU-Rechtsakt gerichtlich anzugreifen. Es handelt sich um ein besonderes gerichtliches Schnellverfahren, um den Beschluss zügig zum Europäischen Gerichtshof zu bringen.

Die Frage, ob der Angemessenheitsbeschluss von dauerhafter Tragfähigkeit ist, hängt entscheidend davon ab, ob der Europäische Gerichtshof seine Kritikpunkte aus der Schrems-II-Entscheidung ausgeräumt sieht. Der Hauptkritikpunkt war die in den USA vorherrschende anlasslose Massenüberwachung durch die Sicherheitsbehörden. Die neue Executive Order greift den Punkt auf, indem sie geheimdienstliche Datenerhebungen unter einen Verhältnismäßigkeitsvorbehalt stellt. Hier zeigen die USA erstmals die Bereitschaft, den Umfang staatlicher Datenerhebungen zumindest einzugrenzen. Die Begriffsdefinition der Verhältnismäßigkeit in der Executive Order lehnt sich erkennbar an das europäische Verfassungsrecht an. Ein einzelfallbezogenes und überprüfbares Dokumentationserfordernis zwingt zudem zu einer jeweils sorgfältigen Abwägung. Problematisch ist hingegen, dass am Instrument der Massenüberwachung (bulk collection) ausdrücklich festgehalten wird. Inwieweit die neue Verhältnismäßigkeitsanforderung konkret die Massenüberwachung verändert, ist dem Text der Executive Order daher nicht eindeutig zu entnehmen. Wichtig sind deshalb engmaschige Überprüfungen der künftigen Anwendung im Hinblick auf etwaige Fehlentwicklungen.

Der zweite zentrale Kritikpunkt des Europäischen Gerichtshofs war der bislang mangelhafte Rechtsschutz europäischer Betroffener. Der neu eingerichtete Data Protection Review Court genießt eine Stellung wie ein Gericht, wird mit unabhängigen Richter:innen von außerhalb der Exekutive besetzt und kann unter anderem Datenlöschungen und Verarbeitungseinschränkungen anordnen. Werden im Rechtsschutzverfahren rechtswidrige Verarbeitungen ermittelt, verpflichtet die Executive Order, diese zu beseitigen. Zu beachten

ist jedoch, dass für die Kläger:innen das Verfahren in der Sache vielleicht effektiv, aber kaum transparent und nachvollziehbar ist. So ist nicht vorgesehen, in den Urteilen darüber zu informieren, ob und welche Maßnahmen ergriffen wurden.

Ob der Angemessenheitsbeschluss auch nach einer zu erwartenden gerichtlichen Überprüfung dauerhaft Bestand haben kann, wird voraussichtlich von der praktischen Umsetzung abhängen. Entscheidend ist, ob der neue Verhältnismäßigkeitsvorbehalt auch tatsächlich eine signifikante Einschränkung der bisherigen Massenüberwachung zur Folge hat. Auch die Wirksamkeit des Rechtsschutzes wird aufgrund der neu einzurichtenden Gremien und Verfahren stark von der Verfahrensführung in der Praxis abhängig sein. Wichtig ist deshalb eine tiefgreifende Überprüfung der tatsächlichen Umsetzung durch die EU. Nur so kann sichergestellt werden, dass die teilweise relativ offenen Rechtsbegriffe in der Executive Order in einer mit dem europäischen Grundrechtsverständnis zu vereinbarenden Weise ausgelegt werden. Erfreulich ist deshalb, dass die Kommission bereits nach einem Jahr ein erstes Review durchführen wird, bevor sie in den üblichen Vier-Jahres-Rhythmus übergeht. Üblich ist eine erste Überprüfung erst nach zwei Jahren. Dies lässt hoffen, dass die in diesem Fall besonders wichtige nachträgliche Auswertung der Praxis ernst genommen wird. Entwickelt sich die Umsetzung in eine vom europäischen Verständnis abweichenden Weise oder werden die für die Kontrollen erforderlichen Einblicke nicht gewährt, wird die EU reagieren können und auch müssen. Dasselbe gilt im Fall von Änderungen des Sicherheitsrechts der USA vor dem Hintergrund des relativ unkompliziert zu revidierenden Rechtsinstruments der Executive Order.

Bis der Angemessenheitsbeschluss endgültig erlassen und wirksam ist, bleibt die Rechtslage für Datenübermittlungen unverändert. Die Executive Order sieht eine Übergangsfrist von bis zu einem Jahr vor. So lange haben die achtzehn Geheimdienste der USA Zeit, die im Rechtsakt vorgesehenen Garantien in die praktische Arbeit zu integrieren. Nach Informationen des HmbBfDI werden zahlreiche dieser Dienste für die Umsetzung noch mehrere Monate benötigen. Dies

betrifft insbesondere die neue Anforderung, Datenzugriffe auf das verhältnismäßige Maß einzugrenzen. Solange die Verhältnismäßigkeit nicht Einzug in die Geheimdienstpraxis gefunden hat, ist weiterhin von einer Datenauswertung auszugehen, die den Wesensgehalt des Datenschutzgrundrechts verletzt. Dasselbe gilt für die institutionellen Garantien durch Schaffung einer Beschwerdestelle und eines Datenschutzgerichts. Diese Gremien befinden sich noch im Aufbau. Die Arbeitsfähigkeit wird erst in mehreren Monaten gewährleistet sein.

Derzeit verfasste Transfer Impact Assessments müssten deshalb nach wie vor zu dem vom Europäischen Gerichtshof vorgezeichneten Ergebnis kommen. Die staatlichen Zugriffsbefugnisse in den USA gehen weiterhin über das in einer demokratischen Gesellschaft erforderliche Maß hinaus. Für die Zukunft ist ein neues Kapitel des transatlantischen Datenaustauschs in Sicht. Vor dem Hintergrund der dargestellten rechtlichen Unsicherheiten handelt es sich jedoch um eine fragile Übermittlungsgrundlage. Da nicht gesichert ist, ob und wie lange das Rechtsinstrument bei einer gerichtlichen Überprüfung Bestand hat, bietet es sich für langfristige Planungen weiter an, wo möglich auf Dienstleister aus dem europäischen Wirtschaftsraum zu setzen.

5. Koordinierte Prüfung der Taskforce Schrems II

Dass die USA erstmals die Geheimdienstüberwachung Europas beschränken wollen, ist ein Erfolg des anhaltenden Vollzugsdrucks. Die deutschen Umsetzungsaktivitäten der Schrems-II-Entscheidung hat der HmbBfDI koordiniert.

Die geplanten Einschränkungen der US-amerikanischen Geheimdienstaktivitäten auf ein verhältnismäßiges Maß (siehe Kap. V 4) sind ein Erfolg der europäischen Datenschutzaufsicht. Auch wenn sich die tatsächliche Wirksamkeit erst in der Praxis zeigen wird, sind die Vereinigten Staaten erstmals bereit, ihre Sicherheitsgesetze an

die europäische Grundrechtstradition anzupassen. Ohne die anhaltende Vollzugspraxis hätte die Europäische Kommission in den Verhandlungen sicherlich keine so weitreichenden Erfolge gehabt.

Für eine breit angelegte Rechtsdurchsetzung, die nicht nur auf Einzelbeschwerden reagiert, hat die Datenschutzkonferenz (DSK) die Taskforce Schrems II gebildet. Der HmbBfDI leitete darin die Teilaufgabe, eine gemeinsame Vollzugsstrategie zu entwickeln und umzusetzen.

Im Rahmen der Taskforce wurde eine abgestimmte Prüfaktion durchgeführt. Zehn teilnehmende Landesdatenschutzbehörden sowie eine kirchliche Aufsicht haben im Jahr 2021 Fragebögen an verantwortliche Stellen in ihrem jeweiligen Zuständigkeitsbereich geschickt (siehe 30. TB 2021, Kap. V 2.2). Die Fragebögen zu verschiedenen Fallgruppen waren zuvor gemeinsam entwickelt worden. Im Jahr 2022 haben sich die beteiligten Häuser über den Umgang mit den eingegangenen Stellungnahmen abgestimmt. Typische Verteidigungsstrategien wurden identifiziert und Best Practices für den Umgang wurden ausgetauscht. Auf dieser Grundlage werden die Prüfungen durch die unabhängigen Aufsichtsbehörden durchgeführt. Diese bearbeiteten ihre Einzelfälle jeweils eigenständig, aber auf Grundlage harmonisierter Bewertungen.

In Hamburg wurden 23 Unternehmen angeschrieben. Ziel der Aktion war die Sensibilisierung, aber auch die Durchsetzung der Anforderungen des Europäischen Gerichtshofs (EuGH). Der HmbBfDI hat sich auf Großunternehmen und Konzerne konzentriert und dabei einen besonderen Fokus auf Versandhändler gelegt. Die Ergebnisse sind differenziert und durchaus positiver als zuvor befürchtet. Hinsichtlich der abgefragten Dienstleister wurde bei keinem der Adressaten ein Hosting im Drittstaat ermittelt. Häufig Verwendung finden jedoch Anbieter mit Geschäftssitz in den USA. Die Datenverarbeitung erfolgt jeweils im Europäischen Wirtschaftsraum, aber vielfach sind Zugriffsmöglichkeiten aus den USA heraus nicht hinreichend ausgeschlossen. Teilweise wurden uns aber auch vorbildliche Verschlüsse-

lungstechnologien präsentiert, die als wirksame technische Maßnahmen die vertraglichen Absicherungen ergänzen. Andere Drittstaaten als die USA spielen in den Antworten keine nennenswerte Rolle.

Um die Zugriffsmöglichkeiten der Konzernmütter in den USA zu unterbinden, wurde im Rahmen der Prüfung mehrfach der Umstieg auf andere Dienstleister erwirkt. In einem Fall, in dem der spezifische Softwareservice bislang nur von einem Unternehmen in den USA erbracht werden kann, hat das geprüfte Hamburger Unternehmen die Entwicklung der Dienstleistung bei einem deutschen Anbieter in Auftrag gegeben. Deutsche IT-Dienstleister wurden damit als direkte Folge der Prüfung des HmbBfDI gestärkt.

Darüber hinaus hat sich die Taskforce zudem mit inhaltlich-rechtlichen Folgen der Schrems-II-Entscheidung des EuGH auseinandergesetzt, die für die Prüfaktion von Relevanz sind. Als wesentliche, bis dato ungeklärte Rechtsfrage wurde der Anwendungsbereich der relevanten US-Sicherheitsgesetze identifiziert. Nur dann, wenn übermittelte Daten tatsächlich auch Gegenstand geheimdienstlicher Überwachung sein können, sind die engen Anforderungen aus der Schrems-II-Entscheidung zu erfüllen. Um US-amerikanische Expertise zu erlangen, hat die Taskforce ein Gutachten bei Professor Stephen I. Vladeck von der Universität Texas eingeholt. Der Experte ist zuvor als Gutachter für Facebook in den Schrems-Verfahren tätig gewesen. Die Ergebnisse zeigen, dass zahlreiche Dienstleister in den Anwendungsbereich der FISA 702 (Foreign Intelligence Surveillance Act) fallen, die davon in ihren Stellungnahmen im Rahmen der Prüfungen zuvor nicht ausgegangen waren. Die Taskforce hat das Gutachten einer eigenen Plausibilitätsbewertung unterzogen und die zitierte Literatur und Rechtsprechung nachvollzogen. Sie hat das Gutachten ferner ins Deutsche übersetzt und im Rahmen einer zusammenfassenden Bewertung die wesentlichen Erkenntnisse interpretiert.

Die Taskforce wird ihre Arbeit fortsetzen, solange die individuellen Prüfungen andauern. Sie wird dabei die Entwicklungen zum mögli-

chen Trans Atlantic Data Pricacy Framework im Blick behalten und darauf gegebenenfalls reagieren.

BERATUNGEN ÖFFENTLICHER STELLEN VI.

VI. Beratungen öffentlicher Stellen

1. Neues Krankenhaus-Informationssystem im Universitätsklinikum Hamburg-Eppendorf

Das Universitätsklinikum Hamburg-Eppendorf plant im April 2023 die Umstellung des bisherigen Arbeitsplatzsystems auf eine alternative Software. Das mit der Umsetzung beauftragte Projektteam beteiligte den HmbBfDI im Berichtszeitraum und versucht nun, das seit 2016 laufende Vorhaben auf eine akzeptable datenschutzrechtliche Grundlage zu stellen. Hierzu erfolgten im Jahr 2022 viele Austausche zu technischen und rechtlichen Fragestellungen.

Im April 2022 wurde der HmbBfDI gem. der Beteiligungsrichtlinie der FHH über die Ablösung des derzeitigen im Universitätsklinikum Hamburg-Eppendorf genutzten klinischen Arbeitsplatzsystems „Soarian" und weiterer klinischer IT-Systeme des UKE sowie seiner Tochtergesellschaften Martini-Klinik GmbH, Altonaer Kinderkrankenhaus gGmbH, Ambulanzzentrum des UKE GmbH informiert. Der HmbBfDI ist seitdem in einem sehr engen Austausch mit dem für die Umsetzung verantwortlichen Projektteam, welches sich aus UKE-internen und -externen Personen zusammensetzt und mit dem Hersteller des neuen klinischen Arbeitsplatzsystems zusammenarbeitet.

Die Beratungstätigkeit des HmbBfDI wird dabei sehr intensiv praktiziert, da aufgrund des großen Umfangs von jährlichen neuen Patientendaten – das UKE spricht von rund 500.000 Patient:innen pro Jahr – und der besonders sensiblen Gesundheitsdaten sowie aufgrund der Stellung als größter Maximalversorger innerhalb der Metropolregion Hamburgs, potentiell ein hohes datenschutzrechtliches Risiko mit der Datenverarbeitung einhergeht. Aus diesem Grunde erklärte sich der HmbBfDI bereit, in einem dreiwöchigen Turnus mit der Projektgruppe zusammenzukommen und aufgeworfene Fragestellungen und Themenkomplexe zu erörtern. Eine solche enge Beratung entspricht nicht der aufsichtsbehördlichen Regel, da hierdurch in einem hohen Maße Ressourcen an ein Projekt gebunden werden;

in Anbetracht der Bedeutung des Projektes erscheint dieser Aufwand jedoch aktuell gerechtfertigt.

Bisher erfolgte ein Austausch zu Fragen der Verantwortlichkeit des UKE sowie der Tochtergesellschaften, über das Erfordernis einer Einwilligung und daraus unter Umständen resultierende Folgen für die Zusammenführung/Trennung von Patientenstammdaten, zur Realisierung des Notfallzugriffsmanagements, dem Rollen- und Berechtigungskonzept, über eine gegebenenfalls zwischen den beteiligten Häusern zu schließende Datenschutzvereinbarung und die Datenschutzinformationen für Patient:innen sowie über besondere Verarbeitungssituationen bzw. -konstellationen (z.B. Verarbeitung von gendiagnostischen Daten, Konsil).

Eine offiziell kommunizierte Bewertung des vom UKE erwarteten Risikos für die Rechte und Freiheiten der betroffenen Patient:innen gab es bis Redaktionsschluss nicht. Ebenso erfolgte bislang noch keine finale Abstimmung zu wichtigen Themen wie u.a. der DatenschutzFolgenabschätzung und der damit verbundenen technischen und organisatorischen Maßnahmen sowie einer belastbaren Aussage zu realisierten IT-Sicherheitsmaßnahmen der künftigen Software. Der bislang mitgeteilte Zeitplan sieht vor, dass im 2. Quartal 2023 ein erster Teilstart mit dem neuen Arbeitsplatzsystem stattfinden soll, sodass das erste Halbjahr 2023 eine intensive und herausfordernde Zeit für alle Projektbeteiligten werden wird; nicht zuletzt deshalb, weil die Software während der Projektlaufzeit vom Hersteller permanent weiterentwickelt wird und auch aufgrund dieser Abhängigkeiten weitere Verzögerungen eintreten könnten. Der HmbBfDI wird sich weiter für die Gewährleistung aller Rechte der Betroffenen einsetzen, um eine sinnvolle Digitalisierung der Klinikprozesse mit dem Grundrecht auf informationelle Selbstbestimmung zu verbinden.

2. Gesundheitsforschung nach dem Hamburgischen Krankenhausgesetz

Der HmbBfDI unterstützt das UKE und den Senat bei der Schaffung von Rechtssicherheit in der Medizinforschung. Das Ziel sind gesetzlich fixier te Garantien zum Schutz der Betroffenen im Krankenhausgesetz oder einem anderen Rechtsakt.

Für die Erkenntnisgewinnung in der Medizinforschung wird eine breite Datenbasis benötigt. Sowohl die Auswertung von Patient:innendaten zu Forschungszwecken als auch die Weitergabe innerhalb eines Krankenhausverbunds oder an Forschende außerhalb ist nicht vom individuellen Behandlungsauftrag gedeckt. Ohne hinreichende Rechtsgrundlage können diese zweifellos wichtigen Aktivitäten daher nur auf Basis einer individuellen Einwilligung durchgeführt werden. Die Einwilligung ist jedoch oftmals nicht der beste Weg, weil Betroffene die Tragweite kaum einschätzen können und weil die Einwilligung noch keine Garantien zum Schutz der Gesundheitsdaten schafft.

Mit § 12 HmbKHG enthält das Hamburgische Krankenhausgesetz eine Rechtsgrundlage für die privilegierte Datenverarbeitung von Gesundheitsdaten zu Forschungszwecken. Daten im Anschluss an die Behandlung weiterzuverarbeiten und dafür zu sammeln, erlaubt die Vorschrift, wenn dies erforderlich ist und das öffentliche Interesse überwiegt. Auch die Weitergabe ist dabei unter hohen Anforderungen an die vorherige Pseudonymisierung möglich. Was der Norm jedoch fehlt, sind hinreichende Garantien im Sinne von Art. 9 Abs. 2 lit. j, 89 Abs. 1 DSGVO. Das vorrangige Europarecht erlaubt es Mitgliedstaaten inklusive der Länder, Rechtsgrundlagen zur wissenschaftlichen Datennutzung zu schaffen. Diese Vorschriften müssen jedoch – so das Unionsrecht ausdrücklich – „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte“ vorsehen. Je invasiver der Eingriff ist, desto konkreter müssen diese Maßnahmen im Ge-

setz bezeichnet sein. § 12 HmbKHG erfüllt diese Anforderung nicht. Während die Sekundärnutzung von Diagnosen und Behandlungsverläufen sehr stark in die informationelle Selbstbestimmung eingreift, enthält die landesrechtliche Ermächtigungsnorm lediglich abstrakte Garantievorgaben.

Auch das Universitätsklinikum Eppendorf sieht diese rechtliche Schutzlücke. Zur Schaffung von Klarheit und Rechtssicherheit für alle Forschenden sowie zur rechtlichen Fixierung angemessener Schutzgarantien haben das UKE und der HmbBfDI sich darauf verständigt, welche Ergänzungen das Krankenhausgesetz erhalten sollte. Mit dem Vorschlag eines § 12a und § 12b HmbKHG ist das UKE mit Unterstützung des HmbBfDI an die Sozialbehörde sowie die Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke herangetreten. Eine gemeinsame Arbeitsgruppe mit den Senatsbehörden, dem UKE und dem HmbBfDI hat in drei Terminen die legislativen Möglichkeiten erörtert.

Kernelemente der §§ 12a, 12b HmbKHG sollen demnach die Schaffung einer Treuhandstelle mit gesetzlich abgesicherter Unabhängigkeit sein. Dieser soll die Aufgabe zukommen, in einer besonders gesicherten Umgebung losgelöst vom Behandlungs- und Forschungsbereich Datenbestände zu verwalten, über Zugangsanträge von Forschenden zu entscheiden und diesen gegebenenfalls nur die wirklich benötigten, je nach Forschungsgegenstand hinreichend pseudonymisierten oder anonymisierten Daten zukommen zu lassen. Für die Durchführung der Forschung soll eine gesetzlich näher konkretisierte Forschungsplattform eingerichtet werden. Beide Stellen sollen mit neu zu schaffenden Straftatbeständen zur Verschwiegenheit verpflichtet und dem Beschlagnahmeverbot unterworfen werden.

Ob eine Anpassung des HmbKHG kommen wird, ist offen. Die Sozialbehörde hat letztlich mitgeteilt, den regulativen Entwicklungen in Bund und Europa (siehe III 10.) nicht durch eine Novelle im Hamburgischen Landesrecht vorgreifen zu wollen. Das ist insofern

bedauerlich, als dass zwar in der Tat politische Bestrebungen auf den höheren Ebenen bestehen, ob, wann und mit welcher Zielrichtung sie umgesetzt werden, ist aber noch unklar. Zudem hatte die Arbeitsgruppe zuvor Signale aus dem Bundesministerium für Gesundheit erhalten, dass Inhalte der Hamburger Initiative gegebenenfalls im Rahmen des bundesweiten Gesetzgebungsprozesses Beachtung finden könnten. Die Akteure in Hamburg haben in Aussicht gestellt, ihren Austausch fortzusetzen, wenn Anfang 2023 kein Bundesgesetz in Aussicht ist oder das Bundesgesetz die hiesigen Interessen nicht vollständig abdeckt.

Parallel zu den gesetzgeberischen Bestrebungen in EU, Bund und Land unterstützt der HmbBfDI das UKE bei der Schaffung einer Alternative bzw. Übergangslösung. Die DSGVO verlangt die gesetzliche Fixierung der durch das UKE ohnehin geplanten Schutzvorkehrungen. Dass damit nicht zwingend ein Parlamentsgesetz gemeint sein muss, ist allgemein anerkannt. Gleichwohl hat das Verwaltungsgericht Hamburg in Bezug auf das Krebsregister hohe Anforderungen an die gesetzliche Bestimmung der Schutzmaßnahmen gestellt (siehe VI 3) Inwieweit andere Rechtsformen eine hinreichende Verbindlichkeit auslösen könnten, ist derzeit in gemeinsamer Klärung.

3. Hamburgisches Krebsregister

Eine Entscheidung des Verwaltungsgerichts Hamburg hat Defizite am Krebsregister aufgezeigt. Deren Beseitigung durch eine Novelle des Krebsregistergesetzes unterstützt der HmbBfDI aktiv.

Das Hamburgische Krebsregister ist ein positives Beispiel, wie Gesundheitsforschung in einem maximal sensiblen Bereich unter Wahrung der Datenschutzrechte der Patient:innen ermöglicht werden kann. Aufgabe der Einrichtung ist es, Krebserkrankungen in Bezug auf die Bevölkerung zu erfassen, also etwa Auftreten und Häufigkeit der Erkrankungen, sowie deren Verteilung nach Alter, Geschlecht

und Wohnort. Zum anderen werden behandlungsbezogene Daten von der Diagnose über einzelne Therapieschritte und die Nachsorge bis hin zu Rezidiven, Überleben und Tod erfasst. Das Hamburgische Krebsregister ist eine Abteilung der Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke. Die behandelnden Ärzt:innen sind verpflichtet, dem Hamburgischen Krebsregister bestimmte Daten zu übermitteln.

Das Krebsregistergesetz macht dabei klare Vorgaben, welche Daten einzumelden sind und unter welchen Voraussetzungen und in welchem Umfang Forschungseinrichtungen sie nutzen können. Besonders positiv ist hervorzuheben, dass jeder beim Krebsregister eingehende Antrag auf Datennutzung dem HmbBfDI zur Anhörung vorzulegen ist. Eine solche aufsichtsbehördliche Freigabe ist ungewöhnlich, in diesem hochsensiblen Bereich jedoch sinnvoll und wichtig. Die regelmäßige Zusammenarbeit mit dem Krebsregister funktioniert gut.

Die gesetzlichen Vorgaben gehen jedoch nicht weit genug. Mit seinem Urteil vom 28.07.2022 in der Rechtssache 21 K 1802/21 hat das Verwaltungsgericht Hamburg Mängel an der Bestimmtheit des Krebsregistergesetzes aufgezeigt. Die Verarbeitung von Gesundheitsdaten der klagenden Patientin hat das Gericht für unzulässig erklärt, weil die Maßnahmen zur Wahrung der Rechte und Freiheiten betroffener Personen nicht spezifisch genug im Gesetz aufgezählt sind. Nicht moniert wurde die praktische Durchführung beim Krebsregister. Das Ansinnen eines möglichst vollständigen Datenbestands für die angewandte Forschung hat das Gericht grundsätzlich gebilligt vor dem Hintergrund der ausdrücklichen Erwähnung der Krebsforschung im 157. Erwägungsgrund der DSGVO. Die beim Krebsregister etablierten Schutzmaßnahmen unter anderem in Form eines besonders geschützten Vertrauensbereichs, Einsatz von Pseudonymisierungstechniken sowie Vorgaben zur Verschwiegenheit, Datensicherheit und Übermittlung hat das Gericht nicht als unzureichend kritisiert. Die Rechtswidrigkeit führte es jedoch darauf zurück, dass diese Schutzmaßnahmen nicht konkret genug im Gesetz festgehalten sind.

Mit Art. 9 Abs. 2 lit. i und j DSGVO erlaubt der Unionsgesetzgeber den Mitgliedstaaten, eigene Rechtsgrundlagen für die medizinische Forschung zu schaffen. Er knüpft diese Gesetzgebungsbefugnis jedoch an inhaltliche Bedingungen. Eine nationale Ermächtigungsnorm erfordert demnach eine Aufzählung angemessener und spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen. Je eingriffsintensiver die Datenverarbeitung ist, desto konkreter und bereichsspezifischer müssen diese Maßnahmen im Gesetz beschrieben sein. Das Krebsregister agiert mit äußerst sensiblen Gesundheitsdaten von Betroffenen in einer persönlichen Ausnahmesituation. Diese werden ggfs. auch gegen deren Willen und als umfassendes Profil mit langer Speicherdauer erfasst. Der Eingriff in das Datenschutzrecht könnte damit kaum invasiver sein. In Anbetracht der starken gesellschaftlichen Bedeutung der Krebsforschung ist er gleichwohl verhältnismäßig, darf aber nur unter hohen Schutzvorkehrungen erfolgen. Es ist nachvollziehbar, dass das Verwaltungsgericht eine möglichst klare und verbindliche Verankerung im Gesetz dafür verlangt hat.

Der HmbBfDI sieht sich durch die Entscheidung in seiner bisherigen Beratungspraxis bestätigt. Er hat sich bereits bei Einrichtung des Registers für eine Legitimation durch ein eigenes Gesetz anstelle einer reinen Einwilligungslösung ausgesprochen. Zudem hat er sich für einen starken Datenschutz durch Verfahren und Schutzmaßnahmen stark gemacht. Wichtig waren ihm dabei insbesondere, dass nicht mit Klarnamen, sondern mit Pseudonymen agiert wird und die Schlüsselverwaltung hinter den Pseudonymen zentral, sicher und mit begrenzten Zugriffsbefugnissen verwaltet wird. Wenn die bislang primär durch interne Vorgaben eingerichteten Maßnahmen infolge der seit 2018 geltenden anspruchsvollen Öffnungsklausel in der DSGVO gesetzlich festgehalten und ggfs. ausgebaut werden, dann ist das zu begrüßen.

Im engen Austausch mit der Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke berät der HmbBfDI, wie das Krebsregistergesetz an die Anforderungen der Gerichtsentscheidung und die

Vorgaben des Datenschutzes angepasst werden kann. Der bisherige Entwurf, in den auch Hinweise des HmbBfDI einfließen, stimmt dabei positiv. Mit der Neufassung ist im Jahr 2023 zu rechnen.

4. Einsatzmöglichkeiten von ELDORADO für Daten mit hohem Schutzbedarf

Vor der Verarbeitung von Akten in ELDORADO, die einen hohen Schutz bedarf haben, sind zusätzliche technische und organisatorische Schutz maßnahmen zu treffen. Einige Maßnahmen sollen im Jahr 2023 zur Verfügung gestellt werden. Die Verantwortlichen sollten prüfen, ob mit diesen Maßnahmen ein ausreichender Schutz für ihren individuellen An wendungsfall gewährleistet werden kann.

Für jede größere Organisation stellt eine effiziente Schriftgutverwaltung eine wesentliche Voraussetzung für reibungslose Arbeitsabläufe dar. Auch hier verspricht man sich von einer Digitalisierung, die Abläufe zu vereinfachen und zu beschleunigen.

In der FHH steht mit dem Verfahren ELDORADO ein Langzeitarchivsystem und Dokumentenverwaltungsverfahren zur Verfügung, welches grundsätzlich auf die allgemeine Schriftgut- und Aktenverwaltung nach den in den jeweiligen Behörden und Ämtern geltenden Geschäfts- und Aktenordnungen ausgerichtet ist. In der Regel ist das darin enthaltene Schriftgut dem Schutzniveau „normal“ zugehörig.

Neben Sach- und Fachakten, welche einem normalem Schutzniveau zuzuordnen sind, und Schriftstücken, für die keine Schriftformerfordernis gesetzlich vorgeschrieben ist, gibt es jedoch vielfältige Aufgaben in der öffentlichen Verwaltung der Stadt, die das Führen von personenbezogenen Einzelfallakten bedingen und/oder Akten für welche besondere datenschutzrechtliche oder andere spezifische gesetzliche Anforderungen gelten und die einem hohen Schutzbe-

darf hinsichtlich der Schutzziele (Vertraulichkeit, Integrität, etc.) unterliegen. Auch hier entsteht zunehmend der Bedarf, diese aus den wuchtigen Aktenschränken in ein zeitgemäßes, elektronisches Dokumentenverwaltungssystem zu überführen. Teilweise aus Platzgründen, aber überwiegend, um auch hier die Sachbearbeitung durch bessere Aktenzugänglichkeit, weniger Medienbrüche etc. zu optimieren. Immer wieder erreichen uns Anfragen hinsichtlich der Einsatzmöglichkeiten von ELDORADO für das Führen personenbezogener Einzelfallakten und/oder Akten für die besondere datenschutzrechtliche gesetzliche Anforderungen gelten und die dadurch einem hohen Schutzniveau unterliegen.

Die Ablösung einer herkömmlichen Papieraktenverwaltung durch ein elektronisches Dokumentenverwaltungssystem stellt jedoch nicht nur hohe Anforderungen beispielsweise an die (Ausfall-) Sicherheit der Systeme und die langfristige und damit systemunabhängige Verfügbarkeit unverfälschter Daten. Mit der Digitalisierung von Akteninhalten verändern sich auch die datenschutzrechtlichen Risiken für die Betroffenen, welchen durch dem Schutzniveau entsprechende technische und organisatorische Maßnahmen begegnet werden muss.

Vor der Entscheidung, Akten in ein elektronisches Dokumentenverwaltungssystem zu überführen, muss daher eine Analyse der in den Akten enthaltenen Dokumente und personenbezogenen Inhaltsdaten hinsichtlich ihres Schutzbedarfes erfolgen. Zudem muss detailliert geprüft werden, auf welcher rechtlichen Grundlage die Verarbeitung der enthaltenen personenbezogenen Daten erfolgt, ob besondere Anforderungen gesetzlich definiert wurden und der Digitalisierung ggf. rechtliche Regelungen entgegenstehen oder sie zumindest in bestimmten Bereichen begrenzt.

Die aus der Digitalisierung der Verarbeitung resultierenden zusätzlichen Risiken für die Rechte und Freiheiten der betroffenen Personen sind daher im Vorfeld zu analysieren und zu bewerten. Dies gilt für sämtliche Verarbeitungsschritte von der Digitalisierung (Scannen)

von Dokumenten über das Speichern, die Recherche-, Zugriffs- und Bearbeitungsmöglichkeiten, Druck- und Sendefunktionen, Bildschirmfreischaltungen bis hin zur Aussonderung, Löschung und Vernichtung.

Erst wenn die spezifischen Gefährdungen erkannt und dokumentiert wurden, kann eine Prüfung erfolgen, ob ein Dokumentenverwaltungssystem für die betrachteten Dokumentenkategorien

- bereits ausreichende Schutzmaßnahmen vorhält,
- die Maßnahmen den Anforderungen entsprechend konfiguriert wurden bzw. konfiguriert werden können,
- erforderlich Maßnahmen für das Verfahren grundsätzlich entwickelt und verfügbar sind, aber noch implementiert werden müssen
- oder etwa unabdingbare Maßnahmen für das Verfahren ggf. noch nicht verfügbar sind.

Aufgrund der vielfältigen gesetzlichen Grundlagen, möglichen Dokumententypen, Interessenabwägungen etc. ist dabei eine allgemeingültige Wertung nicht pauschal möglich. Die einzelnen Bausteine des Standard-Datenschutzmodells (SDM) geben wichtige Hinweise, welche zusätzlichen Maßnahmen gerade bei einem hohen Risiko zur Gewährleistung der einzelnen Schutzziele zu treffen sind. Hier bieten auch die Technischen Richtlinien des BSI (z.B. TR-RESISCAN) den Verantwortlichen wertvolle Unterstützung.

In der folgenden Auflistung ist beispielhaft eine Auswahl an Aspekten genannt, die bei einer Prüfung der datenschutzkonformen Nutzung von ELDORADO zu bewerten sind.

- **Digitalisierung**
  Grundsätzlich werden sensible, personenbezogene Daten in Fachverfahren verarbeitet, welche so gestaltet sind, dass nur die für die Aufgabenerfüllung erforderlichen personenbezogenen Daten (abgestimmte Datenfelder) entsprechend der einschlägigen rechtlichen Grundlage nach vordefinierten Regeln verarbei-

tet werden. Für die Verarbeitung von personenbezogenen Daten in und aus Papierakten galten datenschutzrechtliche Sonderregelungen, welche insbesondere in den eingeschränkten Möglichkeiten der Datenzugänglichkeit und Datenauswertung der konventionellen Papieraktenverwaltung begründet waren (sog. Aktenprivileg).

Werden Akten und Schriftstücke durch Scannen für die elektronische Aktenführung digitalisiert, wird damit der gesamte Inhalt der Schriftstücke verarbeitet und einer weiteren digitalen Verarbeitung zugänglich gemacht. Es erfolgt dabei i.d.R. keine Differenzierung zwischen Daten, die für die der Datenerhebung zugrunde liegende Aufgabe erforderlich sind und ggf. darüber hinaus gehende Daten und Informationen. Aufgrund dieser mit diversen Auswertungsmöglichkeiten verbundenen Verarbeitung sämtlicher Daten kann das Aktenprivileg hier i.d.R. keine Anwendung finden. Die rechtliche Zulässigkeit dieser Verarbeitung (Art. 5 und 6 DSGVO) ist durch die Verantwortlichen zu prüfen. Sofern vor der Digitalisierung Schwärzungen erfolgen müssen, ist der genaue Prozess festzulegen.

- **Auswertungsmöglichkeiten**
  Der Zugriff auf die Inhalte in Papierakten ist grundsätzlich nur über vordefinierte Ordnungskriterien (Aktenplan, Aktenverzeichnis, Aktentitel, Stichwortverzeichnis) möglich, wobei die Struktur der Aktenpläne und -verzeichnisse und Akten in der Regel sach- und aufgabenbezogen ist. Da eine Auswertung nach anderen Kriterien grundsätzlich nicht möglich bzw. mit erheblichem Aufwand verbunden ist, ist eine zweckgebundene Verarbeitung personenbezogener Inhaltsdaten letztlich systembedingt gewährleistet.

  Der Zugriff auf die Inhalte in digitalen Akten ist ebenso über vordefinierte Ordnungskriterien (Aktenplan, Aktenverzeichnis, Aktentitel, Stichwortverzeichnis, Metadaten) möglich. Daneben verfügen die Systeme meist über darüberhinausgehende Such-

funktionen. Diese erleichtern zwar das Auffinden von Unterlagen, insbesondere aber die beliebte Volltextrecherche ist bei personenbezogenen Inhaltsdaten datenschutzrechtlich problematisch. Durch diese Funktion werden (ggf. akten- oder systemübergreifend) freie Zugriffs- und Auswertungsmöglichkeiten nach unbestimmten und zweckfremden Zusammenhängen möglich, welche nicht aufgabenbezogen eingrenzbar sind. Der Verantwortliche muss daher prüfen, ob diese Recherchefunktionen oder auch sonstige Funktionen im System vorhanden und bspw. durch Trennungsebenen und/oder restriktive Rechtevergaben zu unterbinden sind und diese Maßnahme umsetzen.

ELDORADO verfügt standardmäßig über eine aktenübergreifende Volltextrecherche. Es besteht jedoch die Möglichkeit, Akten und auch Aktenpläne von der Indexierung und so von der Volltextrecherche auszunehmen. Die Indexierung kann pro Akte eingestellt werden. Es kann festgelegt werden, ob Inhalt und Metadaten, nur die Metadaten und keine Inhalte durchsuchbar sein sollen oder keine Indexierung erfolgt. Unabhängig von der Indexierungseinstellung kann die tatsächliche Nutzbarkeit der Volltextrecherche zusätzlich auch benutzerindividuell eingestellt oder verweigert werden.

- **Zugriffsrechte**
  Mit der Übertragung von Zugriffsrechten wird dem Nutzer eines elektronischen Dokumentenverwaltungssystems ein permanenter, schneller und selbständiger Aktenzugriff ermöglicht. Die im herkömmlichen Verfahren zumeist gegebene Zutrittskontrolle beim Einzelzugriff durch eine weitere Person (Vier-Augen-Prinzip) entfällt. Es gibt in der Regel keine Einzelanforderungen bei der Registratur, keine Kontrolle durch den sachlich zuständigen Sachbearbeiter, denn es besteht keine Notwendigkeit, die Akte physisch zu entnehmen oder zu transportieren.

  Im Hinblick auf personenbezogene Inhalte elektronischer „Akten" sind daher an die Datenspeicherung und das Zugriffsmanage-

ment (Zugriffshierarchie, Rechtematrix) besondere Anforderungen zu stellen. Die Aufgabenverteilung aller Beteiligten muss vor der Einführung des Systems klar definiert und gegeneinander abgrenzt werden. Die für die Daten verantwortliche Stelle muss die zugriffsberechtigten Personen (Sachbearbeiter, Vorgesetzte, Registratur, Administratoren, Vertreter etc.) für die elektronischen „Akten" ermitteln, festlegen und dokumentieren. Dabei sind gesetzlich vorgeschriebene Verarbeitungs-, Übermittlungs- und Zugriffsbeschränkungen ebenso zu beachten wie das Zweckbindungsgebot und Geheimhaltungsvorschriften. Die individuellen, aufgabenbezogen festzulegenden Zugriffsprofile müssen revisionssicher dokumentiert und bei organisatorischen Veränderungen zeitnah angepasst werden.

Neben der Festlegung des regelmäßig zugriffsberechtigten Personenkreises müssen Regelungen getroffen werden, wie Einsichtsrechte und die bisherige Bereitstellung/Übersendung von Akten (beispielsweise für am Verfahren Beteiligte, parlamentarische Untersuchungsausschüsse, Kontrollinstanzen, Gerichte oder auch eine Aktenabgabe wegen Zuständigkeitswechsels) künftig organisiert und Lösch-, Aussonderungs- und/oder Anonymisierungspflichten technisch und organisatorisch umgesetzt werden sollen.

Der Zugriffsschutz muss auch im Rahmen der Such-/Recherchefunktionen gewährleisten, dass die jeweiligen Nutzer in Trefferlisten nur die Akten und Dokumente angezeigt bekommen und einsehen können, für die sie für ihre Aufgabenwahrnehmung berechtigt worden sind.

Im ELDORADO-Verfahren können Zugriffsrecht/-beschränkungen bis auf Aktenebene umgesetzt werden. Die Nutzenden können nur die Akten sehen und deren Inhalt aufrufen, für welche sie berechtigt wurden. Der Zugriffsschutz wird auch bei Recherche umgesetzt. Die Trefferlisten enthalten nur Dokumente aus Akten, für die eine Zugriffsberechtigung besteht.

Da die Benutzerverwaltung ELDORADO intern erfolgt, soll der damit verbundene Aufwand künftig durch Verbindung und Synchronisation mit den Activ Directory-Strukturen vereinfacht werden.

Der Verantwortliche muss prüfen, ob damit die erforderlichen Zugriffsbeschränkungen umsetzbar sind, und Regelungen treffen, wie Einsichtsrechte und die bisherige Bereitstellung/Übersendung von Akten umgesetzt werden kann. Daneben ist zu prüfen, ob ggf. besondere Schutzmaßnahmen wie z.B. eine Zwei-Faktor-Authentisierung notwendig sind. Dies ist bislang nicht vorgesehen und kann – je nach Ausgestaltung der weiteren Schutzmaßnahmen – auch dazu führen, dass für die Umsetzung der Maßnahmen eine individuelle Instanz von ELDORADO aufgesetzt werden muss.

- **Schwärzung**
  Es muss geprüft werden, ob eine Schwärzung vor der Digitalisierung und Speicherung von Daten erforderlich ist. Ebenso kann es notwendig sein, einzelne Inhalte von bereits in Akten befindlichen Dokumenten nachträglich und dauerhaft zu entfernen (Anonymisierungspflichten). Der Verantwortliche muss prüfen, ob entsprechende Funktionen benötigt werden und umsetzbar sind sowie entsprechende Verfahren festschreiben.

  In ELDORADO ist eine Schwärzung von Inhalten derzeit noch nicht möglich. Eine entsprechende Funktionalität befindet sich in einer frühen konzeptionellen Phase.

- **Aussonderung, Löschung und Vernichtung**
  Die Archivgesetze schreiben die Aussonderung und Anbietungsverpflichtung fest. Der Prozess der Abgabe von Unterlagen an das Staatsarchiv umfasst auch das anschließende Löschen aller Übernahmen und zu vernichtenden Unterlagen (die das Staatsarchiv nicht übernehmen möchte).

Das Aussonderungsverfahren, die Anbietung der Akten an das Staatsarchiv und die tatsächliche Abgabe, der Datentransfer, müssen umgesetzt und festgeschrieben werden, da es aufgrund der Anbietungsverpflichtung Voraussetzung für eine Löschung von Akten darstellt. Das Löschen und Vernichten der Daten muss entsprechend der rechtlichen Vorgaben und Fristen datenschutzgerecht (physisches Löschen) umgesetzt werden.

Für ELDORADO befindet sich der Prozess der Abgabe von Unterlagen an das Staatsarchiv gemäß hamburgischem Archivgesetz in der Entwicklung und Umsetzung und soll pilotiert werden.

In ELDORADO konnte bislang nur logisch gelöscht werden, ein Zugriff auf das Dokument war über die Akte damit nicht mehr möglich. Im Jahr 2023 soll auch das physikalische Löschen (mittels Vier-Augen-Prinzip) bereitgestellt werden.

- **Protokollierung**
  In Abhängigkeit von der Sensibilität der Inhaltsdaten kann die Protokollierung auch lesender Zugriffe erforderlich sein.

  Die Protokollierung lesender Zugriffe ist im ELDORADO-Verfahren derzeit weder vorgesehen noch umgesetzt.

ELDORADO bietet bereits einige Schutzmaßnahmen, welche in den Standardverfahren auf ein normales Schutzniveau ausgerichtet sind, jedoch grundsätzlich eine Anpassung im Sinne einer restriktiveren Konzeption und Einstellung zulassen.

Daneben gibt es einige Entwicklungen, welche demnächst verfügbar sein sollen.

In der Regel wird das eingesetzte Standardverfahren ELDORADO zurzeit ohne eine Schärfung der vorhandenen und ohne die oben genannten zusätzlichen technischen und organisatorischen Maßnahmen nicht das Schutzniveau erfüllen, was für die Führung von

personenbezogenen Einzelakten mit einem hohen Schutzbedarf erforderlich ist. Insofern rät der HmbBfDI allen Dienststellen der FHH, genau zu überprüfen, ob die Anforderungen erfüllt werden können und nötigenfalls entsprechend weitergehende Maßnahmen zu ergreifen und die Wirksamkeit der getroffenen Maßnahmen vor der Produktivsetzung zu testen. Hier steht der HmbBfDI für Beratungsanfragen weiterhin zur Verfügung.

5. Digitale Personalakte

Der HmbBfDI hat die Einführung der digitalen Personalakte auch in diesem Berichtszeitraum begleitet und stand dem Zentrum für Personaldienste weiterhin beratend zur Seite.

Im letzten Tätigkeitsbericht hat der HmbBfDI ausführlich über die geplante Einführung der digitalen Personalakte (DigiPA) berichtet (vgl. 30. TB, 6.2.). Auch innerhalb dieses Berichtszeitraums erfolgte eine Begleitung, Beratung und Sensibilisierung durch den HmbBfDI. Bereits frühzeitig entwickelte sich eine enge und vertrauensvolle Zusammenarbeit auf Augenhöhe. Ebenfalls kann durch die frühzeitige Einbindung des HmbBfDI und Berücksichtigung des Datenschutzes (kostspieligen) Korrekturmaßnahmen vorgebeugt werden.

Im Fokus der diesjährigen Beratung standen u.a. das Berechtigungs- und Rollenkonzept sowie die Möglichkeit der Löschung von nicht erforderlichen Daten in der digitalen Personalakte.

Da die Einsichtnahme in Personalakten nur für bestimmte Personengruppen und nur unter bestimmten Voraussetzungen zulässig ist, ist hier das Berechtigungs- und Rollenkonzept und dessen Umsetzung von maßgeblicher Bedeutung. Dieses wurde für die DigiPA so konzipiert, dass die Rechte grundsätzlich den Zugriffrechten des Fachverfahrens KoPers (Kooperatives Personalmanagement, vgl. u.a. 28. TB. II 7) folgen. Besteht in KoPers Zugriff auf einen Personalfall zu

einem Beschäftigungsverhältnis, so wird grundsätzlich der Zugriff auf die DigiPA und ihren Teilakten im Rahmen der Zweckbindung ermöglicht. Können Personalfälle oder weitere Beschäftigungsverhältnisse in KoPers hingegen nicht eingesehen werden, so wird der Zugriff auf die DigiPA versagt.

Neben dauerhaft notwendigen Zugriffsberechtigungen gibt es jedoch Aufgaben/Funktionen, für die lediglich ein temporärer Zugriff auf relevante Teilakten einzelner Personalakten erforderlich ist (z.B. Beamten- und Zusatzversorgung, Nachversicherung, Ernennungsreferat).

Hier hat das Projekt eine datenschutzgerechte Lösung konzipiert. Es wurde eigens ein Modul entwickelt und implementiert, über das der jeweils zuständige Personalsachbearbeiter die grundsätzlich zur Einsichtnahme berechtigten Personen (mit entsprechend hinterlegtem Profil) auswählen und für ihre Aufgabe und für den erforderlichen Zeitraum die temporäre Zugriffserteilung auslösen kann.

Eine Herausforderung stellte ebenfalls die rückstandslose Löschung von Unterlagen aus der Personalakte dar. Grundsätzlich haben Arbeitgeber:innen laufend zu überprüfen, ob die Daten aus der Personalakte weiterhin aufbewahrt werden dürfen. Falsche Angaben sind zu berichtigen oder zu löschen. Zu löschen sind personenbezogene Daten in Personalakten insbesondere dann, wenn das berechtigte Interesse der Arbeitgeber:innen an einem dauernden Verbleib weggefallen ist und der weitere Verbleib in der Personalakte Gefahren für die berufliche Entwicklung für Arbeitnehmer:innen begründet. Dies gilt nicht nur für Unterlagen in Papierform, sondern auch in Bezug auf elektronische Unterlagen. Hierbei ist eine zeitgerechte und rückstandslose Löschung zu gewährleisten. Bereits im Vorjahr hatte der HmbBfDI darauf hingewiesen, dass ein rückstandsloses Löschen in der elektronischen Aktenführung für die Sach- und Fachaktenführung der FHH (ELDORADO) nicht möglich war. Bei einem Löschvorgang wurden die Einträge der Daten vom Datenverzeichnis entfernt und ein Zugriff auf die gelöschten Daten war nicht mehr möglich

(sog. logisches Löschen). Faktisch waren die Daten aber noch in ELDORADO gespeichert. Dieser Umstand ist auch mit DSGVO, HmbDSG und HmbBG unvereinbar.

Der HmbBfDI ließ sich versichern, dass die FHH mit Hochdruck an einer Lösung arbeite um zeitnah das physikalische Löschen einzuführen (siehe auch VI 4).

Im September 2022 wurde die digitale Personalakte im Bezirksamt Nord als Pilotprojekt eingeführt. Geplant ist, die digitale Personalakte flächendeckend in der gesamten FHH auszurollen. Der HmbBfDI wird hierüber weiterhin berichten.

6. Childhood-Haus Hamburg

Das Hamburger Childhood-Haus wurde mittlerweile offiziell eröffnet. Am Ende des Berichtszeitraums wurde die aktive Arbeit aufgenommen. Das Kompetenzzentrum für Kinderschutz am UKE erhält somit eine zentrale Anlaufstelle für Kinder und Jugendliche, die körperliche, sexuali sierte oder emotionale Gewalt oder Vernachlässigung erfahren haben. Der HmbBfDI hat sich bei der technischen Realisierung der genutzten Systeme eingebracht.

Während der HmbBfDI über den Jahreswechsel 2021/22 beratend mit dem Childhood-Haus befasst war, wurde die Beteiligung im Berichtszeitraum von Seiten der Projektbeteiligten nicht mehr intensiv nachgefragt. Die Rahmenbedingungen des Projekts wurden zu Beginn des Jahres 2022 vereinbart und mit der Umsetzung durch Verantwortliche und Dienstleister begonnen. Der HmbBfDI wurde daraufhin punktuell in einzelne Fragestellungen eingebunden.

In Fällen, in denen ein Ermittlungsverfahren, ein Strafverfahren oder ein familiengerichtliches Verfahren läuft, können Befragungen durch die Polizei oder die Justiz im Childhood-Haus in kindgerech-

ter Umgebung durchgeführt werden. Die Aussagen der Betroffenen können mithilfe von Audio- und Videotechnik aufgenommen werden und so eine spätere Aussage vor Gericht ersetzen. Dadurch werden sich wiederholende, belastende oder an verschiedenen Orten stattfindende Befragungen vermieden. Hierbei ist es dem HmbBfDI wichtig gewesen, dass die dafür genutzten Systeme ausreichend abgesichert sind und Zugriffe auf angefertigte Audio- und Videodateien protokolliert werden. Hierdurch wird ein belastbarer Betrieb der Systeme gewährleistet, da die genaue Nutzung sowie Datenzugriffe jederzeit nachvollzogen werden können. Ebenfalls hervorzuheben sind technische Änderungen, die ein Einhalten einer stadtweit gültigen Passwortrichtlinie erzwingen, sowie die Übertragung der Videoaufzeichnung über das Netzwerk ermöglichen, sodass der fehleranfällige Einsatz von externen Datenträgern nicht mehr erforderlich ist.

Zum Ende des Jahres 2022 sollte mit der Erstellung einer umfänglichen datenschutzrechtlichen Dokumentation begonnen und diese dem HmbBfDI zur Verfügung gestellt werden, um auf dieser Basis das gesamte Verfahren beurteilen zu können. Ebenfalls sollten zum Ende des Berichtszeitraums Abnahmetests erfolgen, die dem HmbBfDI allerdings zum Zeitpunkt des Redaktionsschlusse nicht vorgelegt worden sind.

Zudem beschäftigte sich der HmbBfDI generell mit dem Thema der Childhood-Häuser, da sich fast im gesamten Bundesgebiet aktuell Projekte auf den Weg machen bzw. gemacht haben, ähnliche Voraussetzungen für Kinder und Jugendliche zu schaffen. Aus diesem Grund stimmt sich der HmbBfDI auch mit anderen Aufsichtsbehörden in Deutschland ab, um eine einheitliche Aufsichtspraxis bei diesen sehr sinnvollen Initiativen zu gewährleisten.

7. Digitalisierung Parkraumkontrolle

Der Landesbetrieb Verkehr (LBV) ist im Berichtsjahr mit Überlegungen zur Digitalisierung der Parkraumkontrolle an den Hamburgischen Be auftragten für Datenschutz und Informationsfreiheit (HmbBfDI) her angetreten. Der HmbBfDI wird das Thema auch zukünftig konstruktiv begleiten.

Im März 2022 hat der LBV dem HmbBfDI erstmalig das Projekt „Digitalisierung Parkraumkontrolle – DigiParK" vorgestellt. Weil Bewohnerparkgebiete ausgeweitet werden und der für Parkraumkontrollen zuständige LBV das Problem sieht, den auch daraus resultierenden Mehraufwand bei der Kontrolle des ruhenden Verkehrs personell abdecken zu können, wird über eine Digitalisierung der Parkraumüberwachung nachgedacht. Das heißt, dass die Mitarbeiter des LBV nicht mehr händisch kontrollieren würden, ob z.B. ein gültiger Bewohnerparkausweis oder ein Parkschein sichtbar in einem Kfz ausgelegt ist. Vielmehr würde das durch ein Erfassen des Kennzeichens des parkenden Kfz, z.B. durch ein Scan-Fahrzeug, und durch den automatisierten Abgleich mit einer Datenbank der Kfz-Kennzeichen parkberechtigter Personen ersetzt.

Das setzt zunächst voraus, dass ein Abgleich mit in Datenbanken verarbeiteten Kennzeichen parkberechtigter Personen möglich und zulässig ist. Für den Bereich des Bewohnerparkens, das der Bundesgesetzgeber in § 45 Absatz 1b Satz 1 Nr. 2a Straßenverkehrsordnung (StVO) für städtische Quartiere mit erheblichem Parkraummangel vorsieht, wird das Kennzeichen der berechtigten Personen in Hamburg bereits in einer Datenbank verarbeitet, auf die bei der Kontrolle von Parkberechtigungen allerdings regelmäßig nicht zugegriffen wird. Gleiches gilt für Ausnahmegenehmigungen nach § 46 StVO. Anders verhält es sich in Bezug auf das sog. Kurzzeitparken nach § 13 StVO. Diese Norm sieht neben der Nutzung elektronischer Einrichtungen oder Vorrichtungen zur Überwachung der

Parkzeit die Parkuhr, den Parkscheinautomat und die Parkscheibe vor – analoge Methoden der Parkraumbewirtschaftung, die regelmäßig ohne Verarbeitung des Kennzeichens oder anderer personenbezogener Daten auskommen. Eine abschließende Datenbank mit den Kennzeichen von Kurzzeitparkenden existiert deshalb in Hamburg nicht. Aus diesen Gegebenheiten resultieren zahlreiche, auch datenschutzrechtliche Fragen rund um das Führen von und den Abgleich mit Datenbanken mit Kennzeichen parkberechtigter Fahrzeuge und/oder Personen im Rahmen der Parkraumkontrolle.

Außerdem ist momentan nicht geklärt, ob und in welchem Umfang Kennzeichen parkender Kfz zum Zweck des Abgleichs mit solchen Datenbanken, z.B. durch Scan-Fahrzeuge, erfasst werden dürfen. Ausdrücklich geregelt ist eine solche Kennzeichenerfassung zum Zweck der Parkraumkontrolle bisher nicht. Eine gesetzliche Grundlage für die Kennzeichenerfassung, die den verfassungsrechtlichen Anforderungen genügt, verlangt aber das Bundesverfassungsgericht (BVerfG) in einem Beschluss vom 18. Dezember 2018 (1 BvR 142/15). Das BVerfG hat sich in den vergangenen Jahren in mehreren Entscheidungen mit der Frage nach der Zulässigkeit polizeilicher Kontrollen mittels Kennzeichenerfassung befasst und in dem zuvor genannten Fall der automatisierten Kennzeichenkontrolle in Bayern bei Überschreiten der Landesgrenze zu Österreich einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung angenommen – auch im Fall sog. „Nichttreffer“, also bei Kennzeichen, die nach Abgleich als unproblematisch erkannt und gelöscht wurden. Dass bei der datenschutzrechtlichen Beurteilung darüber hinaus die konkreten Umstände des Einzelfalls, insbesondere die Art und Weise der Verarbeitung von Kennzeichen – also etwaige technische und organisatorische Maßnahmen – eine Rolle spielen, lässt eine Entscheidung des Bundesverwaltungsgerichts (BVerwG) aus dem Jahr 2020 erkennen (BVerwG, Beschluss vom 31. Juli 2020 – 3 B 4/20). Das BVerwG hatte einen Fall der Kennzeichenerfassung im Zusammenhang mit dem Pilotbetrieb einer abschnittsbezogenen Geschwindigkeitskontrolle zu beurteilen. Auch diese Rechtsprechung wird bei der weiteren Ausgestaltung des Projekts DigiParK zu berücksichtigen sein.

Der HmbBfDI wird die Überlegungen zur Digitalisierung der Parkraumkontrolle in der FHH weiterhin beratend begleiten. Besondere Bedeutung wird bei der weiteren Realisierung der Frage zukommen, ob auf Bundesebene eine Rechtsgrundlage für die angedachte Datenverarbeitung im Zusammenhang mit einer digitalisierten Parkraumkontrolle geschaffen wird. Anfang 2023 stehen weitere Gespräche zwischen dem LBV und dem HmbBfDI zum aktuellen Stand des Projekts an.

8. eTicket hvv

Die vorgesehene Umstellung des bisherigen hvv-ProfiTickets auf eine digitale Wallet-Lösung sowie auf einen direkten Ausgabeprozess der Fahrkarten durch die S-Bahn Hamburg setzt unter anderem die Übermittlungen von Beschäftigtendaten an das Unternehmen voraus. Der HmbBfDI hat erreicht, dass der Umfang der zu übermittelnden Daten wesentlich reduziert wurde und nun auf einer informierten Einwilligung der Nutzenden basiert.

Die FHH bietet Ihren Beschäftigten die Möglichkeit, eine Netzkarte im Rahmen des hvv-Großkundenabonnements vom Vertragspartner S-Bahn Hamburg (SBHH) zu erwerben. Das „ProfiTicket“ wird den teilnehmenden Beschäftigten bislang jeweils zum 1. Dezember jeden Jahres als Papierticket über die jeweiligen Personalabteilungen gegen Empfangsbescheinigung ausgehändigt und über die Bezügeabrechnung abgerechnet.

Das Projekt „eTicket hvv“ des Zentrums für Personaldienste (ZPD) informierte den HmbBfDI im Rahmen der gem. „Beteiligungsrichtlinie der FHH“ vorgesehenen Beteiligung des HmbBfDI bereits im Mai 2021, dass diese Papierticket-Lösung bis Dezember 2022 durch eine digitale Lösung ersetzt werden soll. Vorgesehen war zu diesem Zeitpunkt die Ablösung durch ein elektronisches Ticket (Fahrkarte in Form einer Scheckkarte mit Lichtbild; ähnlich zur bereits erhältlichen

elektronischen Kundenkarte, der hvv Card). Der HmbBfDI befasste sich mit der datenschutzgerechten Ausgestaltung dieses Verfahrens bis ihn im Sommer 2022 die Information erreichte, dass das hvv ProfiTicket nicht mehr als eTicket, sondern nunmehr als digitales Ticket auf dem Smartphone in der hvv-App angeboten werden soll. Auch mit dieser Variante hat der HmbBfDI sich daraufhin datenschutzrechtlich befasst, bis er abermals im November 2022 darüber informiert wurde, dass die App-Variante zugunsten einer sog. Wallet-Lösung im Smartphone verworfen wurde, der Lösung, mit der auch das Deutschlandticket im kommenden Jahr abgebildet werden soll.

Für Mitarbeitende ohne Smartphones mit den Betriebssystemen iOS oder Android bzw. jene, welche ihr Smartphone nicht für diese Zwecke nutzen wollen, soll eine Alternative – als Übergangslösung weiterhin das hvv ProfiTicket in der bisherigen Papierform – verfügbar bleiben.

Alle drei vorgenannten Lösungen haben gemein, dass eine alternative Lösung (s.o.) bereitgestellt wird – aber auch, dass mit ihnen ein geänderter Ausgabeprozess der Tickets etabliert werden soll. Das Ticket soll den Beschäftigten künftig direkt von der S-Bahn Hamburg übersandt und die Personalabteilungen dadurch von der jährlichen Fahrkartenausgabe entlastet werden. Hierfür benötigt das Unternehmen die Anschrift der Beschäftigten. Die bisherige Zustimmungserklärung der Betroffenen zur Datenübermittlung personenbezogener Daten an den hvv bzw. die SBHH umfasste jedoch lediglich Namen, Kartennummer, Ausgabedatum und Tarifmerkmale.

Für die Umsetzung des neuen Verfahrens war zunächst eine umfangreichere Datenübermittlung von Beschäftigtendaten aus dem Personalverfahren KoPers an die SBHH vorgesehen. In diesem initial geplanten Umfang war die Datenübermittlung jedoch nicht von der bisherigen Zustimmungserklärung der Bestandskunden abgedeckt und die Erforderlichkeit für die Vertragsabwicklung nicht für alle Daten ersichtlich.

In sehr konstruktiven Gesprächen mit dem Projekt hat sich der HmbBfDI nicht nur dafür eingesetzt, den Datenumfang auf das erforderliche Maß zu reduzieren und insbesondere Daten wie die Personalnummer oder Angaben zur konkreten Beschäftigtenstelle von der Übermittlung auszuschließen. Zudem wurde deutlich gemacht, dass eine Widerspruchslösung hinsichtlich der Datenübermittlung an die SBHH nicht für ausreichend erachtet wird, eine informierte Einwilligung zu ersetzen.

Die datenschutzrechtlichen Bedenken wurden weitestgehend aufgegriffen. Der Datenumfang, welcher aus KoPers an die SBHH zur Abwicklung übermittelt werden soll, wurde erheblich reduziert und umfasst nun weder die konkrete Beschäftigungsstelle noch die Personalnummer. Die betroffenen Beschäftigten wurden zudem über die geplante Datenübermittlung vorab per E-Mail informiert, so dass ihnen die Möglichkeit zur Entscheidung für/gegen die jeweilige Lösung erhalten blieb.

Mit der Wallet-Lösung konnte sich der HmbBfDI aufgrund der kurzfristigen Entscheidung noch nicht abschließend befassen. Er wird sich aber auch bei dieser Lösung für eine datenschutzgerechte Umsetzung einsetzen.

9. Intelligente Verkehrssysteme

Wenn Hamburg zukünftig zur bundesweit ersten Metropol-Modellregion Mobilität gemacht wird und in der Stadt digitale und autonome Verkehrsformen im Realbetrieb erprobt werden sollen, müssen Datenschutz und Datensicherheit dabei weiterhin Berücksichtigung finden. Das gilt für den öffentlichen Personennahverkehr ebenso wie für den Individual- und den Güterverkehr. Der HmbBfDI steht insoweit als Ansprechpartner zur Verfügung.

Mit der Strategie zur Weiterentwicklung und Umsetzung von Maßnahmen Intelligenter Transportsysteme (ITS) hat der Hamburger

Senat im Jahr 2016 den Grundstein gelegt für die Ausrichtung der Stadt im Verkehrsbereich. Im Zuge des ITS-Weltkongresses, dessen Gastgeber Hamburg im Jahr 2021 war, sind zahlreiche Projekte zur Umsetzung dieser Strategie realisiert bzw. angestoßen worden. Zu einzelnen dieser Projekte hatte sich der HmbBfDI im Vorfeld des Kongresses mit den Projektverantwortlichen ausgetauscht und war in beratender Funktion tätig geworden (vgl. 30. TB, Kapitel 6.6). Dieser Austausch ist im Berichtszeitraum fortgeführt worden und sollte auch weiterhin fortgeführt werden.

1. Hamburg Electric Autonomous Transportation (HEAT)
Aus dem Projekt HEAT, dem automatisiert fahrenden Kleinbus in der Hafencity, wurde seitens der Hamburger Hochbahn AG grundsätzlich ein positives Fazit gezogen. Das Projekt habe gezeigt, dass autonome Shuttle den Nahverkehr ergänzen können und von den Nutzerinnen und Nutzern durchaus akzeptiert werden. Seitdem wird an einer Umsetzung gearbeitet, die verlässlich und leistungsfähig im Regelbetrieb eingesetzt werden kann. Der HmbBfDI geht davon aus, dass er erneut beteiligt wird, wenn und soweit bei dieser Umsetzung die Verarbeitung personenbezogener Daten im Raum steht.

2. Check-in/Be-out – Funktion hvv Any in der hvv switch-App
Was das Projekt Check-in/Be-out der Hamburger Hochbahn AG anbelangt, die Ermittlung des günstigsten Tarifs für in Anspruch genommene Beförderungsleistungen, so war geplant, nach Abschluss der Ausrüstung der Infrastruktur mit Bluetooth-Beacons (Sender, die auf Bluetooth Low Energy (BLE) oder auch Bluetooth Smart Technologie basieren und durch mitgeführte Smartphones empfangen werden) die Nutzung für alle Fahrgäste im hvv-Netz im Frühjahr 2022 zu ermöglichen. Die Einführung des 9-Euro-Tickets im Sommer 2022 hat jedoch zu nicht unerheblichen Verzögerungen geführt. Zum Zeitpunkt des Redaktionsschlusses für diesen Tätigkeitsbericht war hvv Any noch nicht für den Wirkbetrieb freigeschaltet. Wann das im Jahr 2023 genau der Fall sein wird, stand auch mit Blick auf die geplante Einführung des Deutschlandtickets noch nicht fest. Zu Fragen der Transparenz sowie der Informa-

tionspflichten steht der HmbBfDI weiterhin mit der Hamburger Hochbahn AG im Austausch.

3. Smarte Liefer- und Ladezonen

In Phase 2 des Projekts Smarte Liefer- und Ladezonen (SmaLa) für Paketdienstleister, Kuriere oder Lieferanten war darüber nachgedacht worden, absenkbare Poller mit Kameraausstattung zum Einsatz zu bringen. Weil dabei voraussichtlich auch Kennzeichen unbeteiligter Kfz erfasst worden wären, hatte der HmbBfDI angeregt, andere Möglichkeiten der Umsetzung einer Nutzungskontrolle in Erwägung zu ziehen. Im Berichtszeitraum ist die kamerabasierte Lösung verworfen worden, auch weil technische Erwägungen dagegensprachen. Die künftigen Planungen sollen auf Konzepte ohne Kameraeinsatz ausgerichtet sein. Der HmbBfDI steht für den weiteren Austausch zur konkreten Ausgestaltung zur Verfügung, wenn doch eine Lösung gewählt werden sollte, bei der personenbezogene Daten verarbeitet werden.

4. Teststrecke für Automatisiertes und Vernetztes Fahren

Die bestehende Teststrecke für Automatisiertes und Vernetztes Fahren (TAVF-HH) soll weiterhin genutzt werden, wenn Hamburg in den kommenden Jahren in einem von der EU bezuschussten Pilotprojekt autonome Lkw-Transportfahrten von der Autobahn zum Terminalgelände des Hamburger Hafens erprobt (s. https://tavf.hamburg). Der HmbBfDI erwartet, dass er – wie in der Vergangenheit (vgl. vgl. 30. TB, Kapitel 6.6.4) – beteiligt wird, wenn es in diesem Zusammenhang zu einer Verarbeitung personenbezogener Daten kommt.

5. Verkehrsmengenerfassung

Im Nachgang zum ITS-Weltkongress sind im ersten Quartal 2022 die Gespräche über die automatisierte Verkehrsmengenerfassung inklusive Reisezeitermittlung fortgesetzt worden. Dabei standen nach wie vor insbesondere die Fragen nach der Geeignetheit sowie nach einer Rechtsgrundlage für die Verarbeitung von WiFi-Signalen der von Verkehrsteilnehmern mitgeführten Smartphones zum Zweck der Reisezeitermittlung im Raum. Letztendlich ist es nicht zu einer

Fortführung des Projekts Reisezeitermittlung in der angedachten Form gekommen.

6. PrioBike-HH

Auch bei den Themen Radverkehr und Digitalisierung des Radverkehrs möchte Hamburg eine Vorreiterrolle einnehmen. So hat der Landesbetrieb Straßen, Brücken und Gewässer (LSBG) dem HmbBfDI das Projekt PrioBike-HH vorgestellt, das aus verschiedenen Maßnahmen besteht – inklusive der Entwicklung einer Radverkehrsinformations-App gemeinsam mit der Technischen Universität Dresden. Mit der App sollen den Radfahrenden Routen- sowie Geschwindigkeitsempfehlungen gegeben werden, bei deren Einhaltung sie bei Grün am nächsten lichtsignalanlagengesteuerten Knotenpunkt ankommen und somit ohne Warten weiterfahren können.

Zu diesem Zweck werden vor Fahrtbeginn Start- und Endpunkt der geplanten Route sowie der genutzte Fahrradtyp erfragt, um daraus eine Route zu berechnen. Mit der Einwilligung der Nutzer:innen werden bei aktiver App während der Fahrt die GPS-Positionsdaten, die aktuelle Geschwindigkeit und die Fahrtrichtung erfasst. Wird das Smartphone am Fahrradlenker im Sichtbereich montiert, werden Hinweise zu Ampeln, Fahrroute und empfohlener Geschwindigkeit angezeigt. Für die Verwendung ist kein Nutzerkonto erforderlich. Jede Fahrt wird bei Nutzung der App mit einer neuen, zufälligen Session-ID verknüpft, die am Ende der Nutzung vom verwendeten Endgerät gelöscht wird. Die im Zusammenhang mit der Ermittlung von Geschwindigkeits- oder Routenempfehlungen erhobenen Positionen der App-Nutzenden werden durch mehrere Maßnahmen mit einer Unschärfe versehen, um die Personenbeziehbarkeit der verarbeiteten Informationen zu reduzieren. Hierzu zählt das Verwerfen von Start- und Endpunkt der Fahrtroute in einem Radius von 100 Metern. In dem Fall, dass eine Position sich über einen Zeitraum von fünf Minuten nicht verändert, wird die Aufzeichnung gestoppt.

Der HmbBfDI begrüßt den datensparsamen Ansatz der PrioBike-HH App. Zu den weiteren Maßnahmen, die in PrioBike-HH über die App

hinaus umgesetzt werden sollen, hat der LSBG angekündigt, dem HmbBfDI datenschutzrechtliche Bewertungen in separaten Dokumenten zukommen zu lassen.

10. Microsoft 365 an beruflichen Schulen

Der HmbBfDI wurde durch das Hamburger Institut für berufliche Bildung (HIBB) an der geplanten Einführung von Microsoft 365 beteiligt und konnte im Rahmen dieses Prozesses weitgehende Kritikpunkte einbringen. Diese werden mittlerweile in mehreren Punkten durch die DSK geteilt. Im Ergebnis ist ein datenschutzkonformer Einsatz auf der Grundlage der eingereichten Unterlagen zurzeit nicht möglich.

Im datenschutzrechtlichen Tätigkeitsbericht für das Jahr 2021 wurde bereits unter der Überschrift „Schule in Zeiten von Corona" von der durch das HIBB geplanten Einführung von Microsoft 365 berichtet. Während es zum damaligen Zeitpunkt noch an einer förmlichen Beteiligung des HmbBfDI an diesem Projekt fehlte, wurde dies korrigiert und der Beteiligungsprozess mit dem HmbBfDI zu Beginn des Jahres 2022 gestartet. Im Rahmen der Beteiligung kam es zu verschiedenen Gesprächen und der Vorlage von Unterlagen und Dokumentationen.

Eine Datenschutz-Folgenabschätzung im Sinne von Art. 35 DSGVO wurde bisher nicht vorgelegt. Auch konnte eine vollständige Übersicht der bei Microsoft 365 für den Administrator möglichen Voreinstellungen nicht beigebracht werden. Dies aber ist für die Frage der Einflussmöglichkeiten des HIBB als verantwortliche Stelle auf Art und Umfang der zu verarbeitenden und an Microsoft und seine Unterauftragsverarbeiter weiterzugebenden personenbezogenen Daten von Schüler:innen und Lehrer:innen vor dem Hintergrund des Datenminimierungsgrundsatzes und der technischen Sicherheit der Verarbeitung relevant.

Der HmbBfDI konnte allerdings Einsicht in verschiedene Dokumente, wie u.a. die mit Microsoft zu schließenden Lizenzvereinbarungen, den Auftragsverarbeitungsvertrag in Form des von Microsoft zur Verfügung gestellten Data Protection Addendum (DPA) 09/21, eine Übersicht der durch das HIBB vorgenommen Konfigurationen und eine Schwellenwertanalyse nehmen, die dann Gegenstand der vorgenommenen Prüfung waren.

Im Ergebnis stellte der HmbBfDI fest, dass ein datenschutzrechtlich zulässiger Einsatz von Microsoft 365 in der vom HIBB vorgesehen Version und Konfiguration nicht ohne Weiteres möglich ist. Entgegen der vom HIBB vorgelegten Schwellenwertanalyse wurde vom HmbBfDI die Erstellung einer Datenschutz-Folgenabschätzung für notwendig erachtet, da von der Verarbeitung insbesondere auch minderjährige Schüler:innen betroffen sein würden und die beim Betrieb von Microsoft 365 bzw. der in diesem Softwarepaket enthaltenen unterschiedlichen Einzelanwendungen auftretenden Datenflüsse sich als sehr unübersichtlich darstellten. Gleichzeitig war das HIBB bemüht, Verarbeitungsrisiken zu minimieren, indem beispielsweise bestimmte Verwaltungsprozesse aus dem Anwendungsbereich von Microsoft 365 herausgenommen (z.B. die Verwaltung von Krankmeldungen) wurden.

Weiteren Kritikpunkten des HmbBfDI konnte indes nicht abgeholfen werden. Insbesondere blieben bis zum Abschluss des Beteiligungsprozesses Bedenken bezüglich des Vorliegens einer Rechtsgrundlage und Bedenken hinsichtlich der Erfüllung der Vorgaben aus Art. 28 DSGVO gemessen an den mangelhafte DPAs von Microsoft.

Die tatbestandlichen Voraussetzungen der vom HIBB angeführten gesetzlichen Verarbeitungsgrundlage aus den §§ 98b und c Hamburgisches Schulgesetz (HmbSG) wurden als nicht erfüllt angesehen. Dabei ist zu berücksichtigen, dass diese schulrechtlichen Vorschriften den Betrieb von pädagogischen Netzwerken und Lernportalen, wozu Microsoft 365 hier aufgrund der Begründung des HIBB zu zählen war, durch Stellen außerhalb des öffentlichen Berei-

ches nur in Ausnahmefällen und unter bestimmten Voraussetzungen zulassen. Diese Voraussetzungen waren aus Sicht des HmbBfDI nicht gegeben, weil es an der notwendigen Erforderlichkeit fehlte. Allen beruflichen Schulen steht bereits die vom Bildungsträger zur Verfügung gestellte Lernplattform „Lernen Hamburg“ zur Nutzung zur Verfügung, die auch Textverarbeitungsmöglichkeiten, einen Messenger und ein Videokonferenztool bietet. Es wurde im Rahmen des Beteiligungsprozesses nicht differenziert vorgetragen, welche pädagogischen Zielsetzungen mit dem Lernmanagementsystem „Lernen Hamburg“ im Einzelnen nicht erreicht werden können und blieb bei allgemeinen Hinweisen auf den Verbreitungsgrad von Microsoft 365.

Auch sieht § 98b Absatz 2 HmbSG bei einem Betrieb eines Systems durch Stellen außerhalb des öffentlichen Bereiches lediglich eine Weitergabe von anonymen Daten vor. Die beim Betrieb von Microsoft 365 anfallende Weitergabe von pseudonymen Daten wäre nur unter der Voraussetzung zulässig, dass Microsoft vertraglich verpflichtet wird, die erhaltenen Daten nicht zu wirtschaftlichen Zwecken zu nutzen. Ein derartiger Verzicht war dem vorgelegten DPA 09/21 allerdings nicht hinreichend bestimmt zu entnehmen, im Gegenteil behält sich Microsoft vor, Daten für „geschäftliche Zwecke“ zu nutzen, ohne dies genauer zu spezifizieren. Letztlich könnte das HIBB als verantwortliche Stelle nicht transparent belegen, welche Daten der betroffenen Hamburger Schüler:innen und Lehrer:innen vom Auftragsverarbeiter Microsoft zu welchen Zwecken verarbeitet werden.

Sowohl der vorgenannte also auch weitere Kritikpunkte an dem DPA von Microsoft waren schließlich Gegenstand des Beschlusses der Datenschutzkonferenz vom 24.11.2022 (https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf). Der hierin enthaltene Abschlussbericht fasst im Einzelnen die Ergebnisse aus dem mit Vertretern von Microsoft geführten Gespräch zu den vertraglichen Voraussetzungen einer Auftragsverarbeitung unter Berücksichtigung von Nachbesserungen durch Microsoft bewertend zusammen.

Die dortigen Feststellungen im Hinblick auf die fehlende Transparenz bzgl. der Verarbeitung der im Rahmen des Auftragsverhältnis empfangenen personenbezogenen Daten zu eigenen Geschäftsinteressen, das Fehlen einer umfassenden und widerspruchsfreien Regelung zur Sicherstellung der Weisungsbindung und der weisungsgerechten Löschung sowie der weiterhin mangelhaften Einbindung von Unterauftragsverarbeitern, die nicht den Vorgaben aus Art. 28 DSGVO entsprechen, waren auch im Beteiligungsverfahren gegenüber dem HIBB für die abschließende, kritische Stellungnahme entscheidend. Gleiches gilt für die Bedenken, dass verantwortliche Stellen mit dem DPA von Microsoft ihrer Rechenschaftspflicht nach Art. 5 Absatz 2 DSGVO nachkommen können.

Es wird sich zeigen, wie das HIBB mit der Empfehlung des HmbBfDI, von einer flächendeckenden Einführung von Microsoft 365 an den beruflichen Schulen in Hamburg vorerst Abstand zu nehmen, umgeht und ob Microsoft angesichts der deutlichen Kritik der DSK an seinen Geschäftsbedingungen und vertraglichen Grundlagen zur Auftragsverarbeitung diese nachbessern wird.

11. Umsetzung des Onlinezuganggesetzes – EfA- und Online-Dienste in der FHH

Das Onlinezugangsgesetz (OZG) regelt, dass Verwaltungsleistungen in Deutschland elektronisch angeboten werden müssen. Die Umsetzungsfrist ist eigentlich zum 01.01.2023 abgelaufen. Trotzdem sind zahlreiche Dienste bisher nicht so einsatzbereit, wie es das Gesetz vorsieht. Die Stadt Hamburg hat die ihr zugewiesenen Dienste fristgerecht entwickelt. Zudem wurde eine Lösung für die problematische Frage der datenschutzrechtlichen Verantwortlichkeit entwickelt. Das erforderliche Vertrauensniveau muss für 18 der 21 Onlinedienste, die die Senatskanzlei im Themenfeld „Unternehmensführung und entwicklung" seit 2022 betreibt, noch festgelegt werden.

Bei der Umsetzung des OZG haben sich Bund und Länder auf ein arbeitsteiliges Vorgehen geeinigt, das Einer-für-Alle-Prinzip (EfA). Demnach muss nicht jedes Bundesland für jede Verwaltungsleistung selbstständig einen Onlinedienst) entwickeln. Stattdessen wurde der Gesamtkatalog aller 575 zu digitalisierenden Leistungen in 14 Themenfelder aufgeteilt. Nach Entwicklung stehen diese Dienste allen Ländern und dem Bund zur Verfügung. Diese Art der Verwaltungskooperation ist neuartig. Bei Durchführung eines Verwaltungsverfahrens können somit mehrere Stellen beteiligt sein: eine, die ein Bürgerkonto verwaltet, eine, die das Frontend des Onlinedienstes bereitstellt und eine, die aufgrund ihrer Zuständigkeit das Verfahren durchführt. Natürlich bedeutet dies auch datenschutzrechtliche Herausforderungen, da ein Verfahren, welches nach alter Verwaltungstradition in einer Hand lag, nunmehr durch mehrere Hände gehen muss. Die Aufsichtsbehörden von Bund und Ländern arbeiten aus diesem Grund ebenfalls daran, die Dienste datenschutzrechtlich zu begleiten.

Eine besondere rechtliche Herausforderung war die Klärung der datenschutzrechtlichen Verantwortlichkeit für die bei der Durchführung des Verwaltungsverfahrens beteiligten Stellen. Hoheitsträger

mit klar abgrenzbaren Zuständigkeiten sollten möglichst nicht in hoheitliche Bereiche anderer Stellen eingreifen. Der Gesetzgeber hat diese Notwendigkeit gesehen und wird sie in einer Novelle des OZG (genannt „OZG 2.0“) adressieren. Ein entsprechender Entwurf ist bereits online verfügbar. Ein zukünftiger § 8 Abs. 4 OZG wird vorsehen, dass eine getrennte Verantwortlichkeit vorliegt. Eine eng begrenzte Ausnahme, die in Art. 4 Nr. 7 zweiter Halbsatz DSGVO bereits grundsätzlich vorgesehen ist. Eine klare gesetzgeberische Regelung ist begrüßenswert. In Hamburg wurde entsprechend mit der zugehörigen Datenschutzerklärung zu den Onlinediensten reagiert und eine Regelung getroffen, die auf die zu erwartende Gesetzesänderung eingeht.

Die FHH ist für die Entwicklung und den Betrieb der Onlinedienste im Themenfeld „Unternehmensführung & -entwicklung“ zuständig. Die Senatskanzlei als verantwortliche Stelle hat dem HmbBfDI auf Nachfrage zu 21 Onlinediensten kurz vor Redaktionsschluss die datenschutzrechtlichen Unterlagen zur Verfügung gestellt. Insgesamt liegen die Verfahrensbeschreibungen von 18 Onlinediensten vor. Positiv ist auch, dass für immerhin 17 Onlinedienste eine Datenschutzerklärung erstellt wurde. Die Senatskanzlei hat angekündigt, noch weitere Dokumente zu den Onlinediensten bereitzustellen. Nach den Unterlagen sind die Dienste, mit denen die für eine Verwaltungsleistung erforderlichen Daten erhoben und an das zuständige Verwaltungsverfahren übermittelt werden, im Zeitraum von Juni bis November 2022 gestartet worden. Für 11 Dienste ist ein Nutzerkonto für Organisationen erforderlich, 3 Dienste können mit einem Organisationskonto oder einem Konto für Bürger:innen genutzt werden und für 7 Dienste ist keine Registrierung erforderlich.

In einigen der beschriebenen Dienste werden auch Gesundheitsdaten oder andere sensible personenbezogenen Daten verarbeitet. Für jeden Onlinedienst muss die verantwortliche Stelle nach den EU Durchführungsbestimmungen der eIDAS-Verordnung 2015-1502, mit welchem Vertrauensniveau auf einen Dienst zugegriffen werden kann, damit sich die Nutzer:innen mit ausreichender Sicherheit

identifizieren und bei einer erneuten. Die Dokumentation zur Feststellung des erforderlichen Vertrauensniveaus lag jedoch nur für 3 Onlinedienste vor. Für diese ist das Vertrauensniveau „Niedrig“ festgeschrieben. Dieses Niveau wird jedoch ohne eine Registrierung, die bei diesen Diensten nicht erforderlich ist und auch beim einfachen Bürgerkonto nicht erreicht. Eine Identifizierung findet in diesen Fällen nicht statt. Ohne eine Identifizierung der Nutzer:innen beim Registrieren bzw. bei einer Beantragung einer Verwaltungsleistung lässt sich jedoch keine durchgehende Ende-zu-Ende-Digitalisierung erreichen. Auch ist eine ausreichend sichere Authentisierung der Nutzer:innen erforderlich, wenn Daten aus einem Onlinedienst abgerufen werden können und eine Rückfrage oder die Bescheidzustellung über ein Nutzerkonto erfolgt.

Eine Nutzung von hamburgischen Onlinediensten, für die ein Organisationskonto erforderlich ist, kann nur erfolgen, wenn die Organisation ein solches Konto in Hamburg angelegt hat. Die Nutzung mit einem Organisationskonto, das in einem anderen Bundesland oder beim Bund registriert ist, ist nicht möglich. Für eine spätere bundesweite Nutzung hat der IT-Planungsrat beschlossen, dass nur das Organisationskonto des Bundes eine Nutzung aller bundesweit angebotenen Onlinedienste ermöglichen wird. Die Vorbereitungen für die dafür erforderlichen Anpassungen laufen.

Der HmbBfDI wird in 2023 an die Senatskanzlei herantreten, um die offenen Fragen zur Umsetzung des OZG und zu den Onlinediensten schnellstmöglich zu klären und die noch fehlenden Unterlagen zu erhalten.

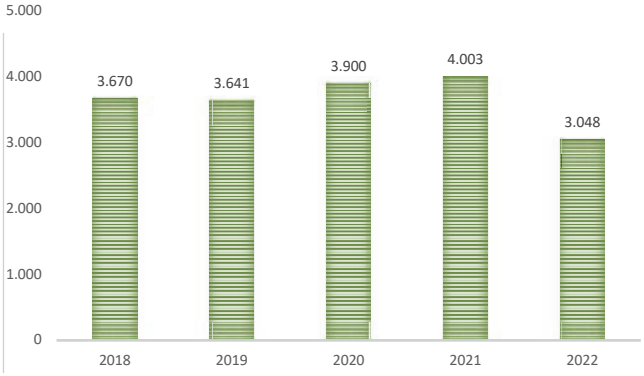
INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT VII.

VII. Informationen zur Behördentätigkeit

1. Statistische Informationen (Zahlen und Fakten)

Im Jahr 2022 sind beim HmbBfDI insgesamt 3.048 Eingänge verzeichnet worden. Erstmals seit vielen Jahren ist damit ein Rückgang an Eingängen festzustellen. Dies scheint eine bundesweite Entwicklung zu ein, wie eine erste Umfrage bei den deutschen Datenschutzaufsichtsbehörden ergab.

Schriftliche Eingänge beim HmbBfDI 2018 – 2022 (gesamt)



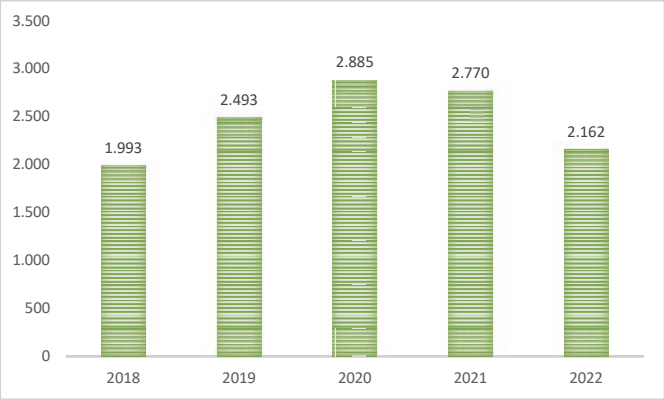
Die Gründe sind nach einer ersten Analyse nicht eindeutig erkennbar. Plausibel scheint, dass die Jahre 2018 und 2019 besondere Jahre waren, weil ab Mai 2018 die DSGVO umgesetzt wurde, und in den Jahren 2020 und 2021 aufgrund der Pandemie Spitzenwerte erreicht wurden. Hingegen dominierten 2022 andere Themen die Öffentlichkeit. Der Anstieg telefonischer Beratungen mag eingabenreduzierend gewirkt haben. Zudem gab es in einigen Bereichen konkrete Verbesserungen, die objektiv Beschwerdeanlässe reduzierten.

Wir werden aber diese Entwicklung noch tiefer analysieren müssen und die weitere Entwicklung beobachten.

1.1 Beschwerden und Beratungen

Datenschutzrechtliche Beschwerden sind schriftliche Eingänge, mit denen Betroffene sich an den HmbBfDI wenden, wenn sie meinen, dass ihre Rechte verletzt wurden (Art. 77 DSGVO). 2022 haben den HmbBfDI 2.162 datenschutzrechtliche Beschwerden erreicht. Das sind 593 weniger Beschwerden als im Vorjahr, und etwas mehr als 2018, dem ersten DSGVO-Jahr.

Datenschutzrechtliche Beschwerden 2018 – 2022



Beratungen werden beim HmbBfDI schriftlich und telefonisch durchgeführt. Dabei hat sich der HmbBfDI 2022 auf die gesetzlichen Aufgaben der Beratung von betroffenen Büger:innen (Art. 57 Abs. 1 lit. e DSGVO) und von Behörden (Art. 57 Abs. 1 lit.c DSGVO) konzentriert. Die Zahl der schriftlichen Beratungen von Unternehmen hat sich im Vergleich zum Vorjahr (171) fast halbiert.

Schriftliche Beratungen 2022

Betroffene	Unternehmen	Behörden	gesamt
254	98	9	361

Die Zahl der schriftlichen Beratungen ist im Vergleich zu 2021, in dem 537 schriftliche Beratungen registriert wurden, ebenfalls stark gesunken.

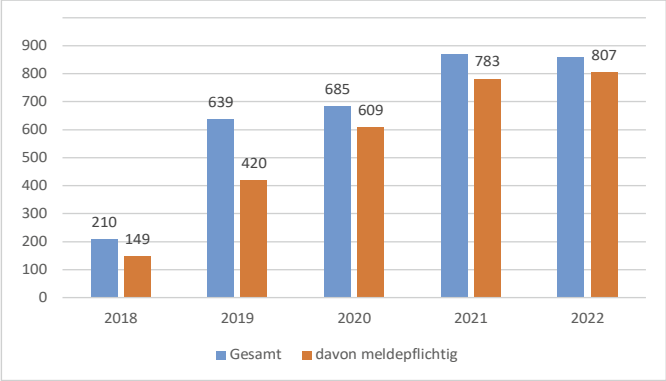
Dagegen ist jedoch die Anzahl der telefonischen Beratungen deutlich von 642 im Jahre 2021 auf 1.432 im Berichtszeitraum gestiegen, wobei hier, zur Vereinfachung der statistischen Erhebung, nicht mehr nach der Stelle, die beraten wurde, differenziert wird. Der Trend zu mehr Beratung, der sich schon in den Vorjahren abzeichnete, scheint sich also zu bestätigen. Dabei ist die Annahme naheliegend, dass es einen Zusammenhang zwischen mehr Beratung und weniger Beschwerden gibt, dies kann zum jetzigen Zeitpunkt aber noch nicht belegt werden. Hier muss, wie bereits in den Vorjahren, weiter beobachtet und Zahlenmaterial gesammelt werden.

1.2. Meldepflicht nach Art. 33 DSGVO

Die beim HmbBfDI als „Data Breaches" bezeichneten Verletzungen des Schutzes personenbezogener Daten sind der zuständigen Aufsichtsbehörde von der verantwortlichen Stelle unverzüglich (möglichst binnen 72 Stunden nach Bekanntwerden) zu melden, vorausgesetzt es besteht voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen.

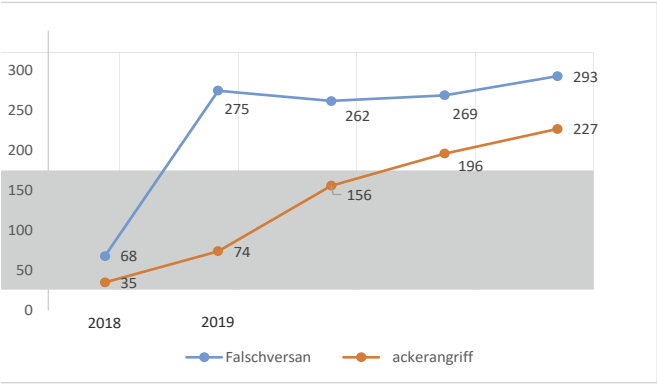
Im Berichtszeitraum haben den HmbBfDI wieder 859 solcher Meldungen erreicht, womit das hohe Niveau des Vorjahres (871) nicht ganz erreicht wurde. Auffällig ist aber, dass im Gegensatz zum Vorjahr nur 52 der gemeldeten Fälle als nicht meldepflichtig eingestuft wurden (2021: 88), sodass 2022 mit 807 Fälle die bisher höchste Anzahl von meldepflichtigen „Data Breaches" beim HmbBfDI gemeldet wurde.

Meldungen nach Art. 33 DSGVO seit 2018



Wie bereits in den Vorjahren sind der Falschversand (293) und der Hackerangriff (227) die am Häufigsten gemeldeten Gründe für die Verletzung des Schutzes personenbezogener Daten. Während der Falschversand sich aber seit Einführung der DSGVO mit leichten Abweichungen auf einem hohen Niveau einzupendeln scheint, steigert sich die Zahl der gemeldeten Hackerangriffe von Jahr zu Jahr:

Meldungen von Falschversand und Hackerangriffe 2018



Diese Entwicklung hatten wir an dieser Stelle schon 2020 vermutet (156 - 29. TB VII 1.2) und diese Vermutung scheint sich zu bestätigen.

1.3 Bußgelder und Anweisungen (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 2022 folgende Maßnahmen ergriffen:

Maßnahme	Rechtsgrundlage	Anzahl 2022
Warnungen	Art. 58 Abs. 2 lit. a	
Verwarnungen	Art. 58 Abs. 2 lit. b	10
Anweisungen und Anordnungen	Art 58. Abs. 2 lit. c – g und j	1
Geldbußen	Art. 58 Abs. 2 lit. i	15
Widerruf von Zertifizierungen	Art. 58 Abs. 2 lit. h	

1.4 Europäische Verfahren

Wenn von einem Sachverhalt Bürger:innen mehrerer europäischer Staaten betroffen sind, wird dieser Sachverhalt in das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission eingegeben. Federführend ist dann die Aufsichtsbehörde, in deren Zuständigkeitsbereich die verantwortliche Stelle ihre europäische Hauptniederlassung hat, alle anderen Aufsichtsbehörden können sich im Verfahren als betroffen melden.

Wie schon im Vorjahr war der HmbBfDI 2022 an 13 europäischen Verfahren beteiligt:

Europäisches Verfahren	Anzahl 2022
Verfahren mit Betroffenheit (concerned)	0
Verfahren mit Federführung (lead)	

1.5 Stellungnahmen in Gesetzgebungsverfahren

Im Jahr 2022 wurde der HmbBfDI auf Grundlage der ‚Richtlinie zur Beteiligung der/des HmbBfDI' in 94 Fällen an der Abstimmung von Senatsdrucksachen-Entwürfen beteiligt und konnte zu den datenschutzrechtlichen Fragen Stellung nehmen. Das waren 19 Vorgänge mehr als im Vorjahr, wie schon 2021 waren 44 dieser Vorgänge tatsächliche Beteiligungen in Gesetzgebungs- und Rechtsetzungsvorhaben (einschl. dem Abschluss von Staatsverträgen). Die weiteren Stellungnahmen erfolgten zu Berichterstattungen des Senats an die Bürgerschaft oder zu hamburgweiten Strategien und Vorhaben.

2. Presse- und Öffentlichkeitsarbeit

Im Berichtsjahr 2022 erreichten den HmbBfDI ca. 100 Presseanfragen. Wichtigste Themenbereiche waren hierbei Datenschutzfragen rund um Facebook, den Einsatz von Cookie-Bannern, Vorratsdatenspeicherung sowie Datenschutzfragen im Kontext der Corona-Pandemie.

Auffällig waren zahlreiche Presseanfragen zu europäischen Datenschutzthemen. Hier ist zunächst das Bußgeld gegen Instagram bzw. den Meta-Konzern in Höhe von 425 Millionen Euro zu nennen. Ebenso zogen die Vorgänge rund um die Twitter-Übernahme und die Folgen für den One-Stop-Shop-Status des Unternehmens großes mediales Interesse auf sich. Des Weiteren standen die Regelungen bezüglich der Cookie Banner von Google im Fokus. Ein wichtiger Komplex mit großer internationaler Bedeutung war schließlich die Diskussion um das EU-US Data Privacy Framework bzw. die Executive Order des US-Präsidenten, die eine Nachfolgelösung für den Privacy Shield im transatlantischen Datenverkehr herstellen sollen.

Auch im Berichtsjahr 2022 war erneut Corona bzw. das Auslaufen einiger Regelungen des Infektionsschutzes zum 30. April ein wichtiger medialer Themenbereich. Die Verarbeitung von Daten in der Luca App und in der CovPass-App oder auch die Frage eines zentra-

len Impfregisters standen hierbei im Vordergrund. Auch die mit einer Pressemitteilung begleitete Anregung des HmbBfDI, die im Zuge der Corona Hotspot-Regelung erhobenen und nun nicht mehr benötigten Daten zu löschen, stieß auf mediales Interesse.

Ein ebenfalls mit einer Pressemitteilung unterstützter wichtiger Komplex im Berichtsjahr war der Zensus 2022, die alle 10 Jahre stattfindende europaweite „Volkszählung". Hier galt es, die Bürger:innen über das Verfahren zu informieren und aufzuklären, u.a. mit einem speziellen FAQ-Bereich auf der Website des HmbBfDI. Der Zensus 2022 war auch in den Medien ein entsprechend viel beachtetes Thema.

Mit Blick auf speziell hamburgische Themen, die für Presseanfragen sorgten, lassen sich die Entwicklungen und Planungen rund um den Komplex Smart City sowie die Einführung digitaler Lösungen im Hamburger Nahverkehr anführen. Aufgrund der angespannten Lage am Wohnungsmarkt in der Hansestadt ist auch hier ein datenschutzrechtliches Thema mehr und mehr medial in den Fokus geraten: die unrechtmäßige Praxis der Anforderung von Schufa-Auskünften bereits bei der Wohnungssuche.

Auch nach über vier Jahren DSGVO erreichten den HmbBfDI im Berichtsjahr mehrere statistische Anfragen zur Zahl der eingegangenen Beschwerden, der Data Breaches und der verhängten Sanktionen.

Nimmt man die großen Internet-Konzerne Meta/Facebook, Google und Twitter in den Blick, so lässt sich sagen, dass sie fast ein Fünftel aller Anfragen des Berichtsjahres 2022 ausmachen. Von den Konzernen liegt Google (9%) vor Facebook (5%) und Twitter (5%). Bei Letzterem sorgten die Umwälzungen seit der Übernahme des Unternehmens im November 2022 für ein kurzfristiges Anfragen-Hoch.

Wie im Vorjahr kann man hinsichtlich der Herkunft der anfragenden Medien sagen, dass über die Hälfte der Anfragen von überregionalen deutschen Medien stammen. Anfragen ausländischer Medien und regional hamburgisch-norddeutscher Medien sind im Vergleich zum

Jahr 2021 auf etwa gleichem Niveau geblieben, wie die nachstehende Tabelle zeigt:

Presseanfragen…	2021	2022
regionaler Medien:	28%	26%
überregionaler Medien:	48%	53%
ausländischer Medien:	24%	21%

Tabelle: Presseanfragen beim HmbBfDI 2021 und 2022

Neben dem vorliegenden Tätigkeitsbericht Datenschutz 2022 gab es im Berichtsjahr keine weiteren Veröffentlichungen im Printbereich. Das Internet-Angebot des HmbBfDI wird stets aktuell weiterentwickelt. Im Berichtszeitraum 2022 hat der HmbBfDI insgesamt neun Pressemitteilungen veröffentlicht.

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

3. Datenschutzkompetenzförderung durch den HmbBfDI

Wie in den Vorjahren hat der HmbBfDI auch im Berichtsjahr 2022 Workshops zum Thema informationelle Selbstbestimmung veranstaltet. Außerdem hat er an der Jugendwebsite youngdata.de mitgewirkt. In den Startlöchern steht ein mit EU-Fördergeldern ausgestattetes Projekt zur Unterstützung von Eltern im Bereich Datenschutz.

In einer Studie des Digital Autonomy Hub gaben über 70% der Menschen an, besorgt zu sein, dass digitale Geräte und Anwendungen

Daten über sie sammeln (Quelle: „Mensch und Technik in Interaktion – Wie gelingt individuelle digitale Souveränität?“ des Digital Autonomy Hub). Dass sich so viele Menschen um ihre persönlichen Daten sorgen zeigt, dass ihnen Informationen fehlen und sie so ihr Recht auf informationelle Selbstbestimmung nicht angemessen wahrnehmen können. Der HmbBfDI hat sich bereits seit mehreren Jahren dieses Problems angenommen. Auch in 2022 hat er daher für verschiedenen Zielgruppen Workshops zum Thema informationelle Selbstbestimmung durchgeführt. Unter anderem veranstaltete der HmbBfDI gemeinsam mit den Bücherhallen Billstedt einen Workshop zum Thema „Sicher surfen im Netz“ für Senior:innen. Außerdem beteiligte sich der HmbBfDI am Girls’day, dem bundesweiten Berufsorientierungstag für Mädchen ab der 5. Klasse. Neben allgemeinen Informationen zum Datenschutz wurden den 30 Teilnehmerinnen unter dem Motto „Datenschutz ist langweilig? Von wegen!“ die Berufsbilder Juristin und Informatikerin vorgestellt. Zudem nahm der HmbBfDI am Young Economic Summit teil, einem Schulwettbewerb der ZBW – Leibniz-Informationszentrum Wirtschaft und der Joachim Herz Stiftung unter der Schirmherrschaft des Bundesministeriums für Wirtschaft und Klimaschutz. Schüler:innen des Gymnasiums Martineum Halberstadt stellten ihre Idee “INSIGHT – Transparency. Privacy. Insight.” vor, die gemeinsam mit der ESMT Berlin entwickelt wurde. Das Projekt verfolgt das Ziel, auf die Herausforderungen der heutigen Datenökonomie hinzuweisen. Der HmbBfDI wurde als Sprecher eingeladen und diskutierte vor dem jungen, internationalen Publikum die Idee der Schüler:innen. Das Projekt überzeugte am Ende so sehr, dass die Schüler:innen des Gymnasiums Martineum Halberstadt den ersten Platz des Schulwettbewerbs belegten. Ein Beweis dafür, dass jungen Menschen der Datenschutz sehr wichtig ist!

Außerdem engagierte sich der HmbBfDI auch in 2022 maßgeblich an der Überarbeitung der Jugendwebsite Youngdata.de der unabhängigen Datenschutz Aufsichtsbehörden des Bundes und der Länder, dem neuen Jugendportal zum Thema Datenschutz und Informationsfreiheit. Ziel der Website ist es, die Öffentlichkeit – hier mit beson-

derem Fokus auf Kinder und Jugendliche – für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung von Daten zu sensibilisieren und sie darüber aufzuklären (Artikel 57 Abs. 1 (b) DSGVO). In 2022 wurde auf Basis wissenschaftlicher Ergebnisse in einem Projektworkshop die zukünftige Struktur der Seite erarbeitet. Anschließend wurde das Ausschreibungsverfahren zur technischen Neugestaltung der Website eröffnet und durchgeführt. Seit dem Sommer 2022 wird an der technischen Umsetzung der neuen Website und der inhaltlichen Überarbeitung der Texte gearbeitet. Im kommenden Jahr wird die Website der Öffentlichkeit zur Verfügung stehen.

In den letzten Jahren fiel immer wieder auf, wie groß der Informationsbedarf zum Thema informationelle Selbstbestimmung und der Wunsch nach Unterstützung bei Eltern ist. Viele Eltern fühlen sich überfordert, wenn sie über mögliche Risiken, die mit ihrer digitalen Mediennutzung verbunden sind, konfrontiert werden (vgl. Kutscher & Bouillon, 2018; Manske & Knobloch, 2017). Eine möglicherweise daraus resultierende Resignation deutet sich in der Studie „Kindheit, Internet, Medien (KIM)“ an, einer jährlichen Basiserhebung zur Mediennutzung der 6- bis 13-Jährigen durch den Medienpädagogischen Forschungsverbund Südwest (mpfs 2020). Der Studie zu Folge nutzen über 70% der teilnehmenden Eltern weder technische Hilfsmittel noch Sicherheits- oder Privatsphäre-Einstellungen auf den Geräten der Kinder (KIM 2020). Außerdem geben 55% der Eltern an, dass sie „nichts zu verbergen“ haben und sich daher nicht um eine mangelnde Sicherheit und Privatsphäre im Netz sorgen (KIM 2020).

Da es sich beim Thema Datenschutz um ein vielschichtiges und komplexes Thema handelt, müssen die Informationen zielgruppengerecht und verständlich aufgearbeitet werden. Leider gibt es derzeit nur wenige Angebote, die Eltern nutzen können, um sich zum Thema Datenschutz zu informieren. Sucht man nach mehrsprachigen Informationsmaterialien zum Datenschutz, wird das Angebot noch rarer.

Das möchte der HmbBfDI gemeinsam mit Partnern ändern: Im Tätigkeitsbericht 2021 wurde bereits berichtet, dass sich die Datenschutzbehörden von Hamburg und Mecklenburg-Vorpommern mit dem Hamburger Bürger:innensender und Ausbildungskanal TIDE zusammengeschlossen haben 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 haben. In 2022 wurde bekannt, dass die EU-Kommission das Projekt D.E.A.P. ausgewählt hat und mit einer Summe von 633.605 € fördern wird. Eine solche Projektförderung für Datenschutzaufsichtsbehörden ist in Deutschland bisher einmalig!

Das auf zwei Jahre angelegte Projekt D.E.A.P. wird nun den Datenschutz für Eltern erlebbar und verständlich machen. Neben diversen barrierearmen (Online-)Workshops wird es in den kommenden zwei Jahren verschiedene Präsenzangebote geben, in denen sich Eltern niedrigschwellig rund um das Thema informationelle Selbstbestimmung informieren können. Außerdem werden mehrsprachige Bildungsmaterialien (z.B. Videos, Podcasts, Broschüren) entwickelt und frei zur Verfügung gestellt.

4. Aufgabenverteilung (Stand: 1.1.2023)

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:	Frau Vukšić
Pressereferent, Internetangebot des HmbBfDI	Martin Schemm
Pressereferentin, Datenschutzkompetenzförderung und Medienbildung, Öffentlichkeitsarbeit	Alina Feustel
EU-Projekt D.E.A.P.	Lydia Roth
Presse, Öffentlichkeitsarbeit und Medienbildung	Gregor-Wielan, Sidney
Verwaltungsleitung, BfH und Unternehmerpflichten, Personal- und Organisationsleitung, Auskünfte nach HmbTG und Art. 15 DSGVO	Arne Gerhards
Haushaltsleitung, Haushaltsplanung und –bewirtschaftung, Kennzahlen u. VZÄ-Controlling, Berichtswesen, DRiVe (Chief), Gebühren- und Beschaffung	Robert Flechsig
IT-Leitung und -Steuerung, Akkreditierung und Zertifizierung, IMI-Koordination	Herr Schneider
Kennzahlenerhebung, Gebührensachbearbeitung (einschl. Bußgelder), Beschaffung, Gebäude- und Raumangelegenheiten, Aus- und Fortbildung	Rolf Nentwig
Geschäftsstelle	Heidi Niemann
Registratur	Frau Vukšić
Registratur, Auskünfte nach DSGVO	Ipek Sari

Grundsatzfragen DSGVO, BDSG, HmbDSG, HmbTG, VIG und HmbUIG — Dr. Christoph Schnabel

Grundsatzfragen HmbVwVfG, VwGO, VwZG, Arbeitsrecht, öff. Dienstrecht, allg. zivil- und strafrechtliche Fragen der Dienststelle, Themenübergreifende Einzelfallbearbeitung (Front Office), Sanktions- und Abhilfebescheide — Richard Heyer

Grundsatzfragen Sanktionen und Aktenführung, Themenübergreifende Einzelfallbearbeitung (Front Office), Sanktions- und Abhilfebescheide — Cornelia Goecke

Grundsatzfragen Art. 58 DSGVO (Befugnisse der Datenschutzaufsichtsbehörde) und Art. 32 f. DSGVO, Themenübergreifende Einzelfallbearbeitung (Front Office), Sanktions- und Abhilfebescheide — N.N.

Polizei und weitere Sicherheitsbehörden, Verfassungsschutz, Staatsanwaltschaften und Gerichte (einschl. Sachverständige, Dolmetscher u. Gerichtsvollzieher), Strafvollzug — Anna-Lena Greve

Pass-, Ausweis- und Meldewesen, Personenstands- und Archivwesen, Statistik, Zensus, Mikrozensus — Uta Kranold

Polizei und Verfassungsschutz, Feuerwehr, Ausländerwesen, Waffen- und Hafensicherheitsrecht, Friedhöfe — Dirk Pohl-Schönmehl

Informationsfreiheit (HmbTG, UIG, VIG), presserechtliche Auskunftsansprüche — Swantje Wallbraun

Stellvertretender Hamburgischer Datenschutzbeauftragter, Akkreditierung und Zertifizierung	Ulrich Kühn
Akkreditierung und Zertifizierung, Presse und Rundfunk, ePrivacy, Telekommunikation, Tracking und Cookies, Kultur	Katja Weber
TTDSG, Strategie und Planung	Wolfram Felber
Werbung und Adresshandel	Joelle Kremser
Tracking und Cookies	Amina Merkel
Bildung (Schulen und Hochschulen), Werbung und Adresshandel (nur Versandhandel), Forschung (soweit nicht Gesundheit oder Verkehr), Geodaten	Alexander Schiermann
E-Mail- und Spieleanbieter, Cloud-Dienste (rechtlich), Apps, E-Government, Bewertungsportale	Felix Wagner
Akkreditierung und Zertifizierung, Grundsatzfragen des Kapitel VII der DSGVO, Koordination der europäischen Verfahren der Behörde sowie Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII der DSGVO	Frau Jacobson
Entwicklung von Prüftools, technisch-organisatorische Beratung und Prüfung verantwortlicher Stellen, technische Unterstützung bei der Fall- und Sachbearbeitung	N.N.
Suchmaschinen (insb. Google, NorthData), Bewertungsportale	Dr. Jutta Hazay
Soziale Netzwerke (insb. Facebook, XING und Twitter), Datingportale	Simone Hoffmann

Soziale Netzwerke, Altfallbearbeitung (Facebook, Instagram), IMI, Data-Breach-Meldungen	Viviane Messan-Lawson
Soziale Netzwerke, Altfallbearbeitung (Facebook, Instagram), IMI, Data-Breach-Meldungen	Anna-Mareike Werth
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, Rechtsanwälte und Notare, Versicherungswirtschaft, Sicherheitsdienste, Beschäftigtendatenschutz	Pieter Jauernig

Finanz- und Steuerwesen, Steuerberater, Wirtschaftsprüfer, Sport, Vereine und Stiftungen	Heike Wolters
Stationärer Handel, Videoüberwachung nicht-öffentlicher Stellen	Bianka Albers-Rosemann
Verkehr, Smart City, Gastronomie	Pauline Mattern
Versandhandel, Inkasso, Auskunfteien, Markt- und Meinungsforschung, Kirchen	Eggert Thode
Gesundheit	Sabine Siekmann
Soziales, Gesundheit, Versorger (Strom, Gas, Abfall)	Sebastian Reich
Themenübergreifende Sachbearbeitung	Laura Bruhn
Themenübergreifende Sachbearbeitung	Christopher Schack

STICHWORTVERZEICHNIS

A

B

C

D

E

F

G

H

W

Y

Z

Auflage: 500 Exemplare
Layout: Gebr. Klingenberg & Rompel in Hamburg GmbH
Foto Titelseite: www.mediaserver.hamburg.de
(U-Bahn-Station Hafencity Universität)
Druck: Bonifatius 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