TÄTIGKEITSBERICHT DATENSCHUTZ 2020

Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Hamburg

29. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2020

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

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

Auflage: 800 Exemplare
Foto Titelseite: Thomas Krenz

Layout & Druck: Druckerei Siepmann GmbH, Hamburg

Dieses Druckerzeugnis ist mit dem Blauen Engel ausgezeichnet.

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

---

vorgelegt im Februar 2021
Prof. Dr. Johannes Caspar
(Redaktionsschluss: 31. Dezember 2020)

INHALTSVERZEICHNIS

Vorwort

Personenbezogene Daten das sind insbesondere Angaben, Werte, Abbildungen, Maße, Aufzeichnungen, Zahlen, Eigenschaften, alles zusammengenommen Informationen, die sich auf natürliche Personen beziehen. Dahinter stecken Menschen, persönliche Schicksale. Sie, ich, die Familie, die Kinder. Die Menschen, ihre Würde und ihr Persönlichkeitsschutz sind der Grund dafür, dass es den Datenschutz gibt. Deshalb wurden in allen Mitgliedstaaten in Europa sowie in allen Bundesländern unabhängige Stellen, die Datenschutzbehörden eingerichtet. Diese sind von staatlichen Instanzen völlig unabhängig und sollen die Menschen u.a. dabei unterstützen, ihre Rechte und Freiheiten zum Schutz ihrer Privatsphäre durchzusetzen. Dazu haben sie den Auftrag, Regierung, Verwaltung und andere öffentliche Stellen sowie all die vielen privaten Stellen zu kontrollieren, die zu völlig unterschiedlichen Zwecken personenbezogene Daten verarbeiten.

Mit diesem kleinen Exkurs möchte ich eingangs auf den zentralen Punkt aufmerksam machen, dem unsere Arbeit auch wieder im zurückliegenden Jahr gewidmet ist: Es geht beim Datenschutz um die Gewährleistung eines in der digitalen Welt zentralen Grundrechts für die Menschen. Angesichts der vielfältigen Möglichkeiten, die im Informationszeitalter mit der Verarbeitung von Daten verbunden sind, ist es wenig erstaunlich, dass die Frage nach der zulässigen Nutzung personenbezogener Daten in Gesellschaft und Staat ein nicht selten polarisierendes und umstrittenes Themenfeld darstellt.

Gerade in Pandemiezeiten wird „der Datenschutz" in der öffentlichen Wahrnehmung gern als Hindernis (miss)verstanden. Dabei wird häufig übersehen, dass das Grundrecht auf informationelle Selbstbestimmung auch unter Pandemiebedingungen keineswegs absolut gilt und erheblichen Einschränkungen unterworfen ist. Gleichzeitig ist auch in Pandemiezeiten die Privatsphäre ein Rechtsgut, das in angemessener Weise mit anderen Grundrechten und dem allgemeinen Ziel des Gesundheitsschutzes in Einklang gebracht werden muss.

Das Berichtsjahr 2020 zeigt gerade vor diesem Hintergrund: Nahezu alle gesellschaftlichen Bereiche sind von der Corona-Pandemie betroffen und werden dies wohl auch noch eine Weile bleiben. Doch Gesundheitsschutz und Datenschutz stehen nicht in einem starren Verhältnis von „Entweder-Oder" zueinander. Im Rechtsstaat geht es nicht darum, das eine Ziel dem anderen generell unterzuordnen, sondern um angemessene Lösungen anzustreben, die einen verhältnismäßigen Ausgleich kollidierender Grundrechtspositionen nach Maßgabe von Einzelabwägungen im konkreten Fall ermöglichen. Diesem Prinzip zu folgen, fällt gerade in schwierigen und herausfordernden Zeiten, die mit vielen Einschränkungen und Verlusten verbunden sind, nicht leicht. Es ist durchaus verständlich, dass der Ruf nach scheinbar einfachen Lösungen immer lauter wird, je größer die Probleme sind, die uns von unserem bisherigen Leben abgeschnitten haben. Aber es ist auch klar: Augenmaß gehört gerade in schwierigen Zeiten zur DNA des funktionierenden Rechtsstaats und der Demokratie.

Im vorliegenden Tätigkeitsbericht über das Berichtsjahr 2020 nehmen die Datenschutzaspekte rund um die Corona-Pandemie daher einen breiten Raum ein. So wurde den üblichen Hauptkapiteln wie Prüfungen, Berichte, Anordnungen/Bußgelder und Beratungen/Datenschutz-Kommunikation ein eigenes Hauptkapitel zur Pandemie vorangestellt. Die zahlreichen unterschiedlichen Einzelbeiträge in diesem neuen Hauptkapitel belegen die große Bandbreite datenschutzrechtlicher Themen, die mit der Corona-Pandemie verbunden sind.

Neben diesem unerwartet hinzugekommenen Hauptschwerpunkt der Arbeit im Jahr 2020 haben natürlich auch andere Themen weiterhin die Arbeit des HmbBfDI im Berichtsjahr bestimmt. Um aus der großen Menge nur einige wenige herauszugreifen: das von der Behörde verhängte Bußgeld gegen das Unternehmen H&M in Höhe von 35,3 Millionen Euro, die Folgen des Schrems II-Urteils des Europäischen Gerichtshofs sowie die deutlich zu Tage tretenden Probleme eines europaweit uneinheitlichen und allzu schwerfälligen Rechtsvollzugs beim grenzüberschreitenden Datenverkehr.

Der weitere Anstieg der Anzahl der eingegangenen Beschwerden von Bürgerinnen und Bürgern hat die Arbeitsbelastung beim HmbBfDI in den letzten Jahren stark ansteigen lassen. Dies kann und konnte durch die vorhandenen personellen Ressourcen des HmbBfDI nicht aufgefangen werden. Wie schon in den Vorjahren besteht bei der personellen Situation weiterhin ein deutlicher Nachbesserungsbedarf.

Zuletzt noch ein Wort in eigener Sache: Der vorliegende Tätigkeitsbericht ist der letzte, der noch vollständig in meine Amtszeit fällt. Nach insgesamt zwölf Jahren endet meine Aufgabe als Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit im Juni 2021 mit Ablauf der von der Verfassung maximal vorgesehenen zweiten Amtsperiode.

Die Digitalisierung von Gesellschaft und Staat über diesen langen Zeitraum zu begleiten war ebenso eine spannende Herausforderung wie ein steiniger Weg. Die vielen vergangenen Diskussionen und Beratungen von Menschen sowie von privaten und öffentlichen Stellen, vor allem die Interventionen für die Rechte und Freiheiten betroffener Personen sowie das Eintreten für einen transparenten Rechtsstaat haben mir vor Augen geführt: Es ist wichtig, die ungeheure Dynamik der Entwicklung digitaler Technologien bestmöglich zu nutzen, sie aber stets auch kritisch zu begleiten und nicht sich selbst zu überlassen. In Zeiten, in denen Daten und Informationen die Ressourcen für ökonomische Macht, soziale Kontrolle aber auch demokratische Teilhabe sind, lohnt sich nicht nur das kritische Nachfragen – es ist vielmehr ein Gebot zu Sicherung einer menschengerechten Zukunft.

Vor zwölf Jahren, im Jahr 2009, habe ich dieses Amt angetreten. Das war vom heutigen Stand betrachtet eine andere Welt: Barack Obama war gerade zum US- Präsidenten gewählt worden, in Hamburg regierte Ole von Beust, und die Schweinegrippe war als Pandemie ausgerufen worden. 2009 das war auch das Jahr, in dem Google seine Kamerawagen für den Dienst Street View durch deutsche

Städte und Gemeinden fahren ließen. Jede Ecke des Planeten sollte zur Kartierung gefilmt werden, woraufhin eine heftige Debatte über die Bedeutung und die Grenzen des Datenschutzes entbrannte. Seither haben sich die Anforderungen und die Sicht auf den Datenschutz tiefgreifend verändert. Vieles ist erreicht worden, es haben sich aber auch neue Fragen und Problemstellungen mit großem Eingriffspotential für die Rechte und Freiheiten ergeben. Das zentrale Ziel, einen Datenschutz zu verwirklichen, der eine Digitalisierung im Dienste der Menschen ermöglicht, ist geblieben.

Ich möchte mich an dieser Stelle ganz herzlich bei allen meinen Mitarbeiterinnen und Mitarbeitern für die großartige Zusammenarbeit und für ihre herausragenden Leistungen im Bereich des Datenschutzes und der Informationsfreiheit über all die Jahre bedanken. Es war nicht immer leicht, den vielen Aufgaben gerecht zu werden. Aber ich denke, es hat sich gelohnt.

Prof. Dr. Johannes Caspar
Februar 2021

EINLEITUNG I.

EINLEITUNG

Im Berichtsjahr 2020 hat das Corona-Virus mit seinen Auswirkungen auf Staat und Gesellschaft wesentliche Fragen und Herausforderungen auch für den Datenschutz aufgeworfen. Es zeigt sich einmal mehr: Datenschutz ist eine Querschnittsmaterie, die in alle Bereiche des täglichen Lebens eingezogen ist. Obwohl die Pandemie in erster Linie ein gesundheitspolitisches Thema darstellt, haben in den letzten Monaten die verschiedensten Maßnahmen zur Pandemiebekämpfung in unterschiedlicher Weise das informationelle Selbstbestimmungsrecht tangiert und wesentlich neue Fragestellungen in der Praxis aufgeworfen. Dies gibt Veranlassung, einen Schwerpunkt im Tätigkeitsbericht 2020 auf die Corona-Pandemie zu legen (siehe II. Corona-Pandemie).

Mit diesem Tätigkeitsbericht 2020 nimmt der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit die Gelegenheit wahr, nach 12 Jahren Amtszeit ein Resümee zu ziehen, auf Vergangenes zurückschauen, Schwerpunkte der derzeitigen Arbeit zu beschreiben und einen Ausblick in die Zukunft zu werfen. Ein wesentlicher Punkt ist die inhaltliche Auseinandersetzung mit Datenschutzproblemen in den letzten Jahren. Hier geht es um die technischen und ökonomischen Veränderungen im Zeitalter der Digitalisierung, die zunehmend große Potentiale für Eingriffe in die Rechte und Freiheiten Betroffener nach sich ziehen, aber auch Entwicklungschancen für eine moderne Gesellschaft bieten. Zudem gilt es, den Blick auf die prozeduralen Veränderungen in der täglichen Auseinandersetzung mit der Datenverarbeitung durch private und öffentliche Stellen zu richten. Die Schwierigkeiten, zu einer modernen und angemessenen Behördenausstattung zu kommen, den vielen Herausforderungen der Digitalisierung zu begegnen, das Recht der informationellen Selbstbestimmung effektiv zu schützen und bei der Beratung digitaler Anwendungen in Staat und Gesellschaft beizutragen, sind leider eine bedenkliche Konstante der letzten Jahre gewesen.

Die letzten 12 Jahre Datenschutz in Hamburg – Rückblick, Bestandsaufnahme und Ausblick

1. Datenschutz im Spiegel der Zeit - Von Google Street View bis zur milliardenfachen Gesichtsanalyse bei Clearview und Co.

Der Umgang mit personenbezogenen Daten hat sich in den letzten Jahren stark verändert. Anfang der 2000er Jahre wäre wohl kaum jemand auf die Idee gekommen, dass die systematische Sammlung und Auswertung von Daten durch Technologiekonzerne eine neue Vorherrschaft von Unternehmen auf den Plan rufen würde, deren Fähigkeiten eine in ihren gesellschaftlichen Auswirkungen bislang unbekannte Dimension nicht-staatlicher Machtansammlung eröffnet.

1.1 Google Street View - Die Zukunft kommt mit Kamerawagen

Von diesen Entwicklungen waren wir noch recht weit entfernt, als Google ab 2007 zunächst in den USA, dann aber auch in Europa, PKWs mit Panoramakameras ausrüstete, um flächendeckend Straßenansichten aufzunehmen und diese dann im Internet zum Abruf bereitzuhalten. Es ist heute, mehr als 12 Jahre später, fast in Vergessenheit geraten, dass die damalige Kontroverse um den Datenschutz und die Privatsphäre, die sich am Abfotografieren von Häusern und Vorgärten sowie Straßenansichten entzündete, von einer massenhaften öffentlichen Kritik getragen war. Die Debatte um Google Street View in Deutschland folgte wesentlich dem Narrativ einer Invasion eines erfolgreichen außereuropäischen Digitalunternehmens in die alte Welt. Bebildern ließ sich dies durch Heerscharen von PKWs mit hohen Kameraaufbauten, die plötzlich auftauchten und in Städte und Gemeinden einfuhren, um sich ungefragt die Ansichten von Personen, PKWs, Häusern und Grundstücken nicht nur anzueignen, sondern diese auch umsonst zum Abruf für Jedermann bereitzustellen.

Die Einhaltung der nationalen Datenschutzgesetze wurde in dieser Situation nicht nur von Datenschutzbehörden angemahnt, sondern auch von vielen Menschen im Land massiv gefordert. Der Ruf nach Datenschutz gegenüber dem Street View-Projekt von Google er-

scholl gerade auch im ländlich geprägten Raum. Es meldeten sich jedoch auch andere Stimmen, die vehement für eine digitale Verbreitung der Panoramaansichten eintraten und ein Recht auf Information geltend machten. Wenn man so will, war die Auseinandersetzung um Google Street View der erste und gleichzeitig der letzte Kampf der analogen Welt mit der machtvoll heraufziehenden digitalen Moderne, die mit dem kompromisslosen flächendeckenden Einsatz von Technik gerade althergebrachte, traditionelle Werte- und Meinungsmilieus gegen sich aufbrachte.

Die Datenschutzbehörde in Hamburg, deutschlandweit zuständig für Google, nahm die Rechte Betroffener wahr, indem sie mit Google weitergehende Vorgaben für den Schutz der Privatsphäre vereinbarte als das Unternehmen global einzulösen bereit war. Es entstand ein weitgehendes Widerspruchsrecht aller in den 20 größten deutschen Städten lebenden Menschen, auf die sich Google am Ende mit dem Dienst Street View in Deutschland beschränkte. Dieses ermöglichte ihnen, über die automatisierte Verpixelung von Gesichtern und Kfz-Kennzeichen hinaus - vor dem Start von Google Street View - der Veröffentlichung ihres Wohnhauses zu widersprechen und eine Unkenntlichmachung von Google zu verlangen.

Dass für Google das Projekt Street View dennoch zum Image-GAU geworden ist, hatte der Tech-Konzern selbst zu vertreten: Als auf Nachfrage der Aufsichtsbehörden herauskam, dass die von Google eingesetzten PKW bei ihrer Befahrung gleichzeitig die Inhalte offener, nicht verschlüsselter WLANs auf einer mitgeführten Festplatte speicherten, führte dies zu einem Sturm der Entrüstung und immensen Vertrauensverlusten. Zahlreiche aufsichtsbehördliche und staatsanwaltschaftliche Ermittlungsverfahren wurden dadurch weltweit ausgelöst. Am Ende stand in Deutschland ein Bußgeld in Höhe von ca. 150.000 Euro. Diese Strafzahlung wäre heute zweifellos höher ausgefallen. Das damals geltende Bundesdatenschutzgesetz sah für Fahrlässigkeits- bzw. Vorsatztaten Bußgelder nur bis zu 150.000 Euro bzw. 300.000 Euro vor. Die Idee einer einheitlichen europäischen Datenschutzgesetzgebung, bei der die Bußgeldhöhe

bis zu 4% des jährlichen Umsatzes eines Unternehmens weltweit beträgt, wurde durch derartige Fallgestaltungen wesentlich bestärkt.

1.2 Neue Zäsuren für den Schutz der Privatsphäre

Die datenschutzrechtlichen Gefährdungen haben sich seit der Zeit von Google Street View stark verändert und erhöht. Zwei Zäsuren sind hier zu nennen: Die Snowden-Enthüllungen über die Massenüberwachung durch US- und andere befreundete Nachrichtendienste 2013 stellte das bei vielen Menschen vorherrschende Grundvertrauen in demokratische Rechtsstaaten in Frage. Mit einem Mal wurde sichtbar, dass auch die Dienste befreundeter Staaten den gesamten Bereich der globalen Kommunikation systematisch ausforschen und ohne transparente Kontrolle massenhaft Daten horten. Hatte sich die Jahre zuvor die Kritik von Datenschützern ganz wesentlich auf die globalen Tech-Konzerne fokussiert, so wurde mit Edward Snowden schlagartig klar, dass die Privatsphäre ebenso von staatlicher Seite bedroht wird. Überwachungsprogramme wie PRISM machten klar, dass die NSA nicht nur auf die eigenen Überwachungsstrukturen beschränkt ist, sondern sich aus dem nahezu unerschöpflichen Datenbestand von globalen Diensteanbietern wie Google und Facebook bedienen können. Dass diese Unternehmen für ihre Dienstleistungen auch noch staatlich entschädigt wurden, dokumentiert, wie effizient das Netz der geheimdienstlichen Überwachung aufgebaut ist.

Eine weitere Zäsur stellt der Facebook-Cambridge-Analytica-Skandal im Jahr 2018 dar. Dieser machte der Öffentlichkeit mit einem Mal klar: Personenbezogene Daten eröffnen ein Instrument zur Profilerstellung, das Manipulation und Kontrolle nicht nur im Bereich des individuellen Konsums, sondern auch zur Einflussnahme auf den Wählerwillen ermöglicht und damit auf den Kernbereich demokratischer Prozesse durchschlägt. So hatte das Unternehmen Cambridge Analytica massenhaft Daten von Facebook-Nutzern ausgewertet, um gezielt Wähler im US-Wahlkampf zu beeinflussen. Die Folgen der Datenmacht sind nicht mehr nur auf die Privatsphäre des Einzelnen bezogen, dessen Profil eine personalisierte Form der Werbung

ermöglicht und den Datenverarbeitern große Gewinne beschert. Das Geschäftsmodell des Microtargeting hat das System demokratischer Willensbildung selbst zum Ziel und die politischen Parteien zu Kunden von sozialen Netzwerken und Datenanalysten gemacht.

Was die Verfasser unseres Grundgesetzes wohl zu den Aktivitäten von Parteien auf sozialen Medien wie Facebook und der im Hintergrund erfolgenden Profilbildung von Bürgerinnen und Bürgern gesagt hätten (hierzu der Bericht, mit dem Facebook Aktivitäten zu Wahlwerbung bzw. Werbung zu politischen und gesellschaftlich relevanten Themen und die Ausgaben hierzu transparenter machen will: https://www.facebook.com/ads/library/report/)? Mit Art. 21 Grundgesetz, der bestimmt, dass die Parteien bei der politischen Willensbildung des Volkes mitwirken, war die herkömmliche Form der politischen Werbung über Rundfunk und Plakatwände abgedeckt. Dass der Rückgriff auf systematische Datenauswertung und manipulative Techniken der Willensbeeinflussung durch kommerzielle Anbieter am Ende demokratische Wahlentscheidungen zumindest mit beeinflussen, wäre damals sicherlich nicht nur aus technischen Gründen völlig undenkbar gewesen. Es ist unbestritten, dass Parteien politische Diskurse anstoßen müssen und damit auch breiter Plattformen für Information und gesellschaftliche Kommunikation bedürfen. Solange diese Praxis ein Geschäftsmodell stärkt, das im Hintergrund auf Profilbildung und Microtargeting beruht, wenig transparent und kaum kontrollierbar ist, bleibt zu befürchten, dass die politische Willensbildung und die demokratische Diskussionskultur in einen gefährlichen Sog und Abhängigkeit von Manipulation und Verzerrungen geraten.

1.3 Automatisierte Gesichtserkennung auf dem Vormarsch

Eine der größten Gefahren für die Privatsphäre geht derzeit vom Einsatz der automatisierten Gesichtserkennung aus: Der Aufbau von biometrischen Gesichtsdatenbanken, die eine Zuordnung von Gesichtern zu einzelnen Personen ermöglicht, ist bereits vollzogen. Das gilt vor allem für China, das die Gesichtserkennung wie kein anderer Staat zur umfassenden Überwachung der Bevölkerung großflächig

einsetzt. Aber auch private Anbieter in den USA und aus Europa bieten global die Möglichkeit, über Gesichter nach der Identität von Personen zu suchen.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat bereits im Jahr 2011 (siehe 23. TB 2010/2011 IV 3.3) die Einführung einer automatisierten Gesichtserkennung durch Facebook in Europa ohne die Einwilligung der Nutzer überprüft und ein Verwaltungsverfahren dagegen eingeleitet. Damals ging es noch um die eher harmlos wirkende Funktion, das Heraussuchen und Markieren von Personen auf Fotos zu erleichtern. Allerdings setzt dies voraus, dass eine Datenbank erstellt wird, in der die Bilder möglichst vieler Nutzerinnen und Nutzer des Dienstes biometrisch verarbeitet und individuellen Gesichts-IDs zugeordnet werden. Die zudem schwer zugängliche Möglichkeit des Opt-Out, mit dem ein Widerspruch gegen diese Verarbeitung des eigenen Bildes eingelegt werden konnte, ersetzt keine Einwilligung. Die Funktion war daher datenschutzwidrig. Facebook stoppte in der Folge den Einsatz der Gesichtserkennungsfunktion in Europa und nahm den Betrieb dann erst wieder nach Geltung der Datenschutzgrundverordnung (DSGVO) in Betrieb, allerdings auf Basis einer Einwilligungslösung.

Zwischenzeitlich hielt die Technologie der automatisierten Gesichtserkennung Einzug auch in die Strafverfolgung der Freien und Hansestadt Hamburg: Die Polizei Hamburg hatte im Zuge der Ermittlungen der Ausschreitungen anlässlich des G20-Gipfels in Hamburg im Jahr 2017 eine Datenbank aufgesetzt, die Bilder von Personen enthielt, die sich auf Demonstrationen, als bloße Passanten auf den Straßen oder im Bereich öffentlicher Verkehrsmittel aufhielten. Sämtliche aus unterschiedlichen Quellen zusammengetragene Bilder wurden mit Hilfe einer Gesichtserkennungssoftware ausgewertet. Dieser Referenzdatenbestand wurde sodann mit Fotos von Straftätern abgeglichen (dazu siehe 26. TB 2016/2017 II 2). Die Anordnung des HmbBfDI, die biometrische Referenzdatenbank zu löschen – nicht jedoch die Dateien zu begangenen Straftaten und Tatverdächtigen – wurde vom VG Hamburg aufgehoben. Leider ist über die Zulassung

der Berufung durch das OVG bis heute nicht entschieden worden. Solange eine Entscheidung zum Einsatz einer derartig invasiven Technologie auf der Basis einer Generalklausel im Bundesdatenschutzgesetz nicht ergangen ist, gibt es keine rechtliche Klarheit darüber, ob derartige Bildauswertungen zu Strafverfolgungszwecke zulässig sind und künftig ohne eine spezialgesetzliche Regelung zum Schutz der Rechte und Freiheiten Betroffener erfolgen dürfen.

Das Auswerten von Fotos aus sozialen Netzwerken und anderen Diensten, aber auch aus Datenbeständen der Videoüberwachung oder privaten Aufnahmen, ermöglicht es, die Anonymität von Personen in allen denkbaren Situationen aufzubrechen. Ob Videos von Versammlungen oder Ansammlungen, vor und in religiösen Begegnungsstätten oder ganz einfach beim Einkauf im Supermarkt – künftig können abgebildete Personen mit Hilfe von Gesichtserkennungssoftware sowohl in Echtzeit als auch nachträglich selbst in großen Menschenmengen identifiziert werden.

Eine wichtige Aufgabe der Aufsichtsbehörden im Bereich des Datenschutzes war und ist es daher, den erheblichen Gefahren für die Privatsphäre entgegenzuwirken, die von einem umfassenden und unregulierten Einsatz von Gesichtserkennungssoftware und dem Aufbau von entsprechenden Referenzdatenbeständen ausgehen. Unternehmen, die durch sog. Scraping, d.h. durch das Durchsuchen von Webseiten, öffentlich zugängliche Bilddateien extrahieren und damit riesige biometrische Datenbanken füllen, die dann nach einzelnen Bilddaten durchsucht werden können, müssen darauf überprüft werden, ob sie die Anforderungen des Art. 9 Abs. 2 DSGVO betreffend die Verarbeitung besonderer Kategorien von Daten erfüllen, unter die biometrische Gesichtsmodelle fallen.

Das Geschäftsmodell, das zahlenden Kunden ermöglicht, binnen Sekunden jederzeit von jedem Ort aus Gesichter von Personen zu identifizieren und zuzuordnen, ist derzeit auf dem Vormarsch. Ein Unternehmen, das seine Dienste insbesondere Sicherheitsbehörden in den USA anbietet und über eine Datenbank mit Milliarden von Gesichtern

verfügen soll, ist das US-Unternehmen Clearview. Aufgrund einer Beschwerde hat der HmbBfDI ein Verwaltungsverfahren gegen das Unternehmen eingeleitet und prüft die rechtliche Zulässigkeit der Speicherung und biometrischen Verarbeitung in diesem Zusammenhang.

Ein anderes Unternehmen, das einen ähnlichen Dienst für die breite Öffentlichkeit als Suchmaschine für Gesichter anbietet, ist das ursprünglich in Polen ansässige Unternehmen PimEyes, das unter dem Firmennamen „Face Recognition Solutions Ltd." seit kurzem auf den Seychellen registriert ist. Auch gegenüber diesem Unternehmen ist in Hamburg eine Beschwerde anhängig. Derzeit prüft die polnische Datenschutzaufsichtsbehörde, ob sich das Unternehmen immer noch innerhalb ihres Zuständigkeitsbereichs befindet.

In beiden Fällen geht es nicht nur um die Frage der zulässigen Verarbeitung von biometrischen Daten, sondern auch um die Anwendbarkeit der DSGVO, da in beiden Fällen die Unternehmen offenbar außerhalb der EU sitzen. Ein Firmensitz in Europa ist wichtig für die Zuordnung einer federführenden Aufsichtsbehörde: Er ist jedoch nicht erforderlich, um aufsichtsbehördliche Maßnahmen auszulösen. Für die Anwendbarkeit der DSGVO reicht es aus, dass ein außerhalb der EU niedergelassener Verantwortlicher Dienste gegenüber betroffenen Personen in der EU anbietet (zum Verfahren gegenüber Clearview siehe noch unter V 3). Insoweit sind dann alle Aufsichtsbehörden der Mitgliedstaaten zuständig.

Wichtig ist, derartige Angebote mit biometrischer Datenverarbeitung an der EU-Datenschutzgrundverordnung zu messen. Unklarheiten der Anwendbarkeit der DSGVO sowie der Zuständigkeiten der Aufsichtsbehörden dürfen am Ende kein rechtliches Vakuum schaffen, in dem Geschäftsmodelle von Firmen die Rechte betroffener Personen an ihren biometrischen Daten unterlaufen.

1.4 Datenschutz zwischen gestern und heute

Der Vergleich zwischen 2009 und der Gegenwart lässt erkennen,

dass vieles, worüber damals diskutiert und gestritten wurde, heute mit Blick auf die tatsächlichen Risiken für das informationelle Selbstbestimmungsrecht in einem weit weniger grellen Licht erscheint. Der Blick zurück macht schnell klar, wie sehr die digital-technologische Entwicklung und die Ökonomisierung personenbezogener Daten den Begriff der Privatsphäre verändert und das Recht auf informationelle Selbstbestimmung zurückgedrängt haben. Die erheblichen Auswirkungen von digitalen Technologien auf die Privatsphäre sind Themen, die bei weitem nicht mehr so elektrisieren wie noch zu Zeiten von Google Street View. Dafür verantwortlich sind eine schleichende Anpassung an die technischen Vorgaben und der damit verbundene Gewöhnungseffekt. Digitale Entwicklungen vollziehen sich in einem schrittweisen Prozess. Die Privatsphäre ist dabei kein statischer Rechtsbegriff, sondern in hohem Maß dem gesellschaftlichen Wandel unterworfen. In einer Zeit der massiven technologischen Innovationen, die die gesamte Kommunikationskultur verändern, wird das Bewusstsein einer eigenen Privatsphäre durch die Öffentlichkeit des Privaten und durch die massenhafte Verbreitung und den Austausch von personenbezogenen Daten relativiert. Dabei ist die Bedeutung der Privatsphäre gerade vor dem Hintergrund der jederzeitigen Abrufbarkeit persönlicher Daten aus sozialen Netzwerken und über Suchmaschinen immer wertvoller geworden. Was privat ist und bleiben soll und was nicht, verändert sich zusehends. Die Veröffentlichung des Bildes des eigenen Hauses im Netz wird deshalb anders beurteilt als vor 10 Jahren. Dieser Effekt macht aber den Datenschutz nicht obsolet. Im Gegenteil: Jeder Einzelne braucht ein Konzept des eigenen Datenmanagements, gerade um in der digitalen Welt die Grenzen zu ziehen, die nötig sind, um die eigene Person zu schützen.

Es ist deshalb zu begrüßen, dass die DSGVO die Aufsichtsbehörden nicht nur ermächtigt, gegen Datenschutzverstöße vorzugehen, sondern auch die Kompetenz enthält, die Öffentlichkeit über die besonderen Risiken der Digitalisierung und deren Gefahren für die Privatsphäre fortlaufend zu informieren (Art. 58 Abs. 3 lit b DSGVO).

2. Die Vollzugsprobleme des Datenschutzes auf EU-Ebene - Implodiert die DSGVO aufgrund der fehlenden Rechtsdurchsetzung bei der grenzüberschreitenden Datenverarbeitung?

Die DSGVO hat eine völlig neue Architektur des Zusammenwirkens von Aufsichtsbehörden eingeführt, die den Rechtsvollzug massiv erschwert. Während gewöhnlich die Rechtsanwendung eine monokratische Aufgabe einer hierarchisch organisierten Behörde ist, beruht das Modell des Vollzugs in der DSGVO bei grenzüberschreitender Datenverarbeitung auf einem filigranen Geflecht kooperativer Absprachen sowie Informationsverpflichtungen mit dem Ziel, einen Konsens zu erreichen (Art. 60 Abs. 1 S. 1 DSGVO). Im Falle, dass in dem kooperativen Verwaltungsverfahren ein solcher Konsens verfehlt wird, erfolgt eine Übertragung der Letztentscheidung auf den Europäischen Datenschutzausschuss (EDSA), dem höchsten EU-Organ für den Datenschutz, bestehend aus allen mitgliedstaatlichen Aufsichtsbehörden. Hier gilt dann das Mehrheitsvotum. Leider hat der EDSA seit seinem Bestehen erst eine Entscheidung im Streitbeilegungsverfahren getroffen. Hierin hat er eine restriktive Haltung gegenüber seinen eigenen Befugnissen eingenommen, Beschlüsse einzelner Aufsichtsbehörden zu überprüfen und zu korrigieren (dazu siehe III 6).

Das Konsens- und Diversitätsmodell im Rechtsvollzug, bei dem grundsätzlich jeder für jedes Verfahren eine Mitzuständigkeit hat und alle konkreten Fälle ein Nadelöhr gemeinsamer Befassung durchlaufen müssen, wirkt auf den ersten Blick sympathisch und demokratisch fundiert. Tatsächlich wirft es massive Schwierigkeiten auf, die einen effektiven und harmonisierten Vollzug erschweren und eine einheitliche Durchsetzung des Datenschutzrechts zugunsten der Rechte und Freiheiten Betroffener in Europa behindert. Unterschiedliche nationale Verfahrensregelungen verstärken diesen Effekt. Bislang wurden die globalen Tech-Unternehmen trotz zahlreicher datenschutzrechtlicher Beschwerden und schwerwiegender Vorkommnisse so gut wie nicht sanktioniert. Mittels der DSGVO erhobene Bußgelder betrafen in der Masse rein nationale Verfahren, bei denen keine grenzüberschreiten-

de Datenverarbeitung erfolgte und eine Zusammenarbeit auf europäischer Ebene nicht ausgelöst wurde. Die Anzahl und Höhe der bei der grenzüberschreitenden Datenverarbeitung erhobenen Bußgelder ist unproportional gering, verglichen mit den im Bereich der nationalen Verarbeitung erhobenen Bußgeldern. Rechtsverbindliche Anordnungen in diesen Verfahren sind äußerst selten. Das Verfahren des One-Stop-Shop, wonach für jedes Unternehmen grundsätzlich die Aufsichtsbehörde am Ort der Hauptniederlassung in der EU federführend zuständig ist, führt zu einer Konzentration verantwortlicher Stellen auf einige wenige Mitgliedstaaten und schwächt nicht nur den Datenschutz, sondern erweist sich als Einfallstor für Wettbewerbsverzerrungen auf dem digitalen Binnenmarkt.

Trotz einer umfassenden Evaluation der Regelungen der DSGVO durch den EDSA und die EU-Kommission sind Empfehlungen und Anregungen, mit denen die Schwächen des derzeitigen Vollzugsverfahrens ausgeräumt werden könnten, bislang nicht geltend gemacht worden. Die Grundannahme, die DSGVO werde zu einer besseren Regulierung gerade jener globalen Datenverarbeiter führen, deren Geschäftszweck es ist, Daten zu sammeln und auszuwerten, wird zunehmend enttäuscht. Zentrale Fragestellungen, die durch Beschwerden an die Aufsichtsbehörden herangetragen werden, bleiben jahrelang offen. Wird hier auch weiterhin nichts unternommen, werden kleinere gesetzliche Korrekturen an der Verfahrensausgestaltung der DSGVO nicht mehr ausreichend sein. Stattdessen müssten tiefe Eingriffe in die DSGVO diskutiert werden – etwa eine Verlagerung der Aufsicht großer Unternehmen auf eine dafür zu schaffende pan-europäische Aufsichtsbehörde.

3. Der lokale Blick: Die angemessene Ausstattung der Aufsichtsbehörde – Ein wiederkehrendes Grundproblem in Zeiten steigender Aufgabenverantwortung

3.1 Die gegenwärtige Entwicklung

In den letzten Jahren haben sich im Rahmen der Haushaltsverhandlungen immer wieder unterschiedliche Einschätzungen über die an-

gemessene Ausstattung zur Erfüllung der Aufgaben der Behörde des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ergeben. Der HmbBfDI hat im Zuge der Einführung der DSGVO weitergehende Bedarfe angemeldet, die jedoch im Haushaltsverfahren erheblich gekürzt wurden. Ein Gegensteuern durch die befristete Einstellung von Personal war in den letzten Jahren ein Mittel, um den qualitativen sowie quantitativen Anstieg der Aufgaben kurzzeitig zu kompensieren. Dies ist gegenwärtig nicht mehr ausreichend.

Bereits im letzten Tätigkeitsbericht für das Jahr 2019 wurde auf Folgendes hingewiesen: „Trotz einer zwischenzeitlich erfolgten Verstärkung des Personals … stellt sich die Frage nach der mittelfristigen Handlungsfähigkeit der Behörde.“, 28. TB 2019 I 1). Die Situation hat sich innerhalb eines Jahres weiter zugespitzt. Immer mehr Menschen fordern ihre Rechte oder eine Beratung ein. Dies ist durchaus positiv, zeigt sich darin doch eine Sensibilisierung für die Privatheit. Gleichzeitig führt es zu einem bedenklichen Bearbeitungsstau, der bedrohlich anwächst. Die Forderung nach einer auch nur temporären weiteren Verstärkung, um den Rückstau abzuarbeiten, wurde bislang nicht erfüllt.

Die Situation der Aufsichtsbehörde im Berichtszeitraum war insoweit geprägt von einem nicht abbrechenden Eingaben- und Beschwerdeaufkommen, einem erheblichen Anstieg von OWi-Verfahren (siehe VII 1.3) sowie insbesondere von einem Großverfahren, das zu der Verhängung eines Bußgeldes in Höhe von 35,3 Millionen Euro führte. Neu auftretende pandemiebedingte Fragestellungen in ganz unterschiedlichen Bereichen des Datenschutzes haben mit dazu geführt, dass die Bilanz bei der Beschwerdeabarbeitung am Ende des Jahres sich nicht so gut wie erhofft entwickelt hat. Auch die pandemiebedingte Verlagerung in das Home Office hatte sicherlich ihren Anteil daran. Hierauf wurde mit einer erneuten Veränderung der Organisation der Behörde reagiert. Künftig soll durch Zentrierung auf weniger Fachreferate und deren Untergliederung in Fachbereiche sowie durch die Schaffung von Zuständigkeiten für Altfälle eine effizientere und zeitgemäßere Struktur entstehen. Eine Differenzierung

zwischen Datenschutz im öffentlichen und privaten Bereich, die bereits durch die DSGVO verabschiedet wurde, erfolgt künftig nicht mehr. Stattdessen werden inhaltliche Kompetenzen zusammengelegt, die einen stärkeren Bezug zueinander haben.

3.2 Die Wirtschaftlichkeit der Behörde im Rückblick

Auch wenn mit öffentlichen Geldern finanzierte Behörden keine Profit-Center sind, gehört zu der Zehnjahresbilanz ein haushalterischer Rückblick. Es mag insoweit durchaus überraschen, dass während immer wieder Debatten um die angemessene Ausstattung geführt wurden, die Behörde im Durchschnitt der letzten Dekade ihren eigenen Haushalt nicht nur vollständig selbst tragen konnte, sondern darüber hinaus in den Haushalt der FHH eingezahlt hat. So ergibt sich aufgrund der Einnahmen aus Bußgeldern und Gebühren im Schnitt in den letzten 10 Jahren von 2010 bis 2020 und insbesondere durch den Einmaleffekt des 35,3 Millionen Euro hohen Bußgelds aus dem aktuellen Berichtsjahr ein Überschuss des HmbBfDI in Höhe von rund 1,4 Millionen Euro jährlich nach Abzug aller Personal- und Sachkosten. Obwohl die Erzielung von Erlösen nicht dem Aufgabenbereich einer unabhängigen Stelle für den Datenschutz entspricht, ist die Tätigkeit der Aufsichtsbehörde unter dem Strich der letzten Jahre dennoch durchaus auch ökonomisch erfolgreich gewesen.

3.3 Neue Vorschläge zur Stärkung der Stellung des HmbBfDI

Datenschutz und Informationsfreiheit sind zentrale Grundpfeiler einer digitalen Demokratie und des Rechtsstaats. Als staatliche Institution ist der HmbBfDI wie jede andere unabhängige Aufsichtsbehörde eine Einrichtung, die dem Schutz der Rechte und Freiheiten von Bürgerinnen und Bürgern verpflichtet ist. Dieses Leitbild der DSGVO macht künftig weitere Anstrengungen nötig, um die Belange des Datenschutzes, aber auch der Informationsfreiheit, zu stärken.

Für eine effektive Struktur erscheint es sinnvoll, die Anbindung an

den Unterausschuss für Datenschutz und Informationsfreiheit in der Bürgerschaft zu lockern. Die Verhandlungen zentraler Themen der Rechtsstaatlichkeit und der Digitalisierung in einem Unterausschuss hat sich in den letzten Jahren nicht immer bewährt. Unterausschüsse der Bürgerschaft sind durch ihre Abhängigkeit von dem Fachausschuss nur bedingt in der Lage, eigenständig eine Agenda zu verfolgen. Sie werden von den Fachausschüssen eingesetzt und erhalten von diesen ihre Aufträge. Bereits die Verweisung des alljährlichen Tätigkeitsberichts von der Bürgerschaft in den Justizausschuss und von dort in den Unterausschuss Datenschutz und Informationsfreiheit ist bürokratisch und zeitraubend. Aktuelle Themen, die einer zügigen Beratung bedürfen, lassen sich so nur schwer aufgreifen. Zudem werden die Bereiche Datenschutz und Informationsfreiheit durch die Delegierung in den Unterausschuss verfahrenstechnisch in eine zweite Reihe geleitet, wo sie dann einem parlamentarischen Diskurs unterzogen werden, der häufig wenig öffentlichkeitswirksam wird und an dem in der Regel eher eine kleine Anzahl Abgeordnete teilnehmen. Es könnte sinnvoll sein, aktuelle Fragestellungen künftig im Hauptausschuss ohne Zeitverzögerung zu diskutieren. Im Gegenzug sollte gerade auch eine stärkere inhaltliche Schwerpunktsetzung erfolgen, so dass Themen mit größerer Detailtiefe und weniger tagesaktueller Ausrichtung auch weiterhin im Unterausschuss behandelt werden.

Ein weiterer wichtiger Aspekt betrifft die Stellung des HmbBfDI im Rahmen des Haushaltsverfahrens. Die besondere Bedeutung als Kontrollinstanz der senatsunabhängigen und senatsabhängigen Behörden lässt es sinnvoll erscheinen, hier künftig eine Verfahrensgestaltung zu verankern, die eine objektivierbare Ermittlung des personellen und sächlichen Haushaltsbedarfs ermöglicht. Die bisherige Praxis ist davon geprägt, dass die erforderlichen Mittel für eine angemessene Ausstattung, die durch den HmbBfDI angemeldet wurden, im Haushaltsverfahren nur unzureichend Anerkennung gefunden haben.

Künftig könnte diese Debatte stärker versachlicht werden, indem ein Gremium oder eine Kommission durch die Bürgerschaft eingesetzt

wird und einen Bericht über den Stand der Ausstattung bzw. eine konkrete Bedarfsanalyse erstellt. Damit wäre eine Grundlage für die Haushaltsverhandlungen geschaffen, auf deren Basis eine transparente Diskussion über die Angemessenheit der angemeldeten Bedarfe erfolgen kann. Dieses Gremium kann aus Sachverständigen, durchaus auch aus Abgeordneten zusammengesetzt sein. Wichtig ist, dass die Mitglieder eines derartigen Gremiums sich vor Abfassung ihres Berichts mit den Arbeits- und Organisationsabläufen der Datenschutzaufsichtsbehörde vertraut gemacht haben.

Ein solches Gremium würde dem rechtlichen Hintergrund Rechnung tragen, dass es bei der angemessenen Ausstattung nicht um eine Wohltat durch den Haushaltsgesetzgeber geht, sondern um ein organschaftliches Recht, das unmittelbar mit der völligen Unabhängigkeit der Aufsichtsbehörde verknüpft ist. Dieses Recht ist sowohl auf Ebene des Primärrechts der EU als auch auf Ebene der Landesverfassung verankert. Hierzu enthält Art. 52 Abs. 4 DSGVO folgende Aussage: „Jeder Mitgliedstaat stellt sicher, dass jede Aufsichtsbehörde mit den personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen ausgestattet wird, die sie benötigt, um ihre Aufgaben und Befugnisse auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Ausschuss effektiv wahrnehmen zu können."

Datenschutzaufsichtsbehörden haben eine Gewährleistungsverantwortung zum Schutz von Rechten und Freiheiten Betroffener. Sie müssen daher so aufgestellt sein, dass sie der Nachfrage durch rechtssuchende oder einfach nur ratsuchende Personen nachkommen und ihre zahlreichen weiteren Aufgaben (Vgl. Art. 57 Abs. 1 lit a - lit v DSGVO) erfüllen können. Die Mitgliedstaaten haben ihrerseits eine Gewährsleistungsverantwortung gegenüber den Aufsichtsbehörden und müssen sicherstellen, dass diese mit den personellen, technischen und finanziellen Ressourcen ausgestattet sind, die sie benötigen, um ihre Aufgaben und Befugnisse wirksam zu erfüllen. Wo dies nicht möglich ist, gilt es die hierfür erforderliche Unterstützung zu gewähren.

Um diese Gewährleistungsverantwortung sachgerecht wahrzunehmen sollte eine entsprechende Verfahrensgestaltung die Unabhängigkeit des HmbBfDI künftig absichern.

4. Zur Zukunft des Datenschutzes

Datenschutz ist nicht Zweck an sich, sondern setzt Menschen mit Rechten und Freiheiten voraus. Die Unabhängigkeit von Aufsichtsbehörden hat dabei eine streng dienende Funktion. Aufsichtsbehörden haben insbesondere die Aufgabe, verantwortliche Stellen unabhängig zu kontrollieren. Dazu zählen nicht nur private Unternehmen, sondern auch alle öffentlichen Stellen, von der Regierung bis zur Verwaltungsbehörde, in denen Daten verarbeitet werden. Eine unabhängige Aufsichtsbehörde sollte daher stets bereit sein, die Rechte und Freiheiten Betroffener auch dann durchzusetzen, wenn dies im Einzelfall beschwerlich ist und Widerstände zu überwinden sind. Gleichzeitig werden die Aufsichtsbehörden nur erfolgreich sein, wenn sie sich als Teil digitaler Strategien und des Wandels verstehen und diesen Wandel offen mitgestalten. Bürokratische Prozesse, langsame Entscheidungswege und fehlende Bereitschaft zum Dialog sind hier nicht nur auf der Seite der Aufsichtsbehörden, sondern auch auf Seiten der öffentlichen und privaten Stellen, die den Datenschutz umsetzen, zu vermeiden.

4.1 Die Aufsicht in Mehrbehördensystemen – Keine Zentralisierung der Datenschutzaufsicht auf Bundesebene!

Datenschutz darf sich nicht in bürokratischen Verfahren verlieren. Besondere Gefahren erwachsen den Datenschutzbehörden hierbei in einem föderalen Gefüge, in dem sich die aufsichtsbehördlichen Kompetenzen in einzelne sachliche und örtliche Zuständigkeiten aufsplitten. Das gilt in besonderer Weise für die Aufsichtsbehörden in Deutschland, die sich nicht nur untereinander beim Vollzug auf nationaler Ebene, sondern auch bei der Abstimmung auf europäischer Ebene im Kreis von 27 mitgliedstaatlichen Aufsichtsbehörden

miteinander verständigen müssen.

Daten sind ein überaus bewegliches Gut. Landesgrenzen, aber auch die Grenzen der Mitgliedstaaten der EU halten den Fluss der Daten nicht auf. Die Rechte Betroffener sollten daher ebenfalls nicht von Grenzen abhängig sein. Es ist ein wichtiges Legitimationskriterium für die Arbeit der Aufsichtsbehörden, dass sie einen einheitlichen Vollzug des Datenschutzrechts in ihren Zuständigkeitsbereichen herstellen: Das geht nur, wenn es gelingt, übergreifende Standards bei der Rechtsauslegung und -anwendung zu formulieren und diese einheitlich zu vollziehen. Unterschiedliche Standards führen zu einer Zersplitterung des Rechts und haben erhebliche Wettbewerbsverzerrungen zur Folge.

Hier liegen auf Ebene der EU wesentlich größere Probleme, die u.a. aus dem bürokratischen aufsichtsbehördlichen Verfahren resultieren, als im nationalen Bereich (siehe dazu oben unter I 2). Die Debatte, die derzeit um eine Zentralisierung der Datenschutzaufsicht in Deutschland verläuft und eine Zentrierung der Vollzugskompetenzen auf die Bundesebene verfolgt, hat insoweit einen falschen Fokus. Diese Debatte ist ein Wiedergänger und war schon früher aufgekommen, um sich dann sehr schnell in Luft aufzulösen. Das Thema ist unter verschiedenen Aspekten problematisch: Es ist in Deutschland ein verfassungsrechtlicher Grundsatz, dass die Länder für den Vollzug der Gesetze zuständig sind. Die nicht immer einheitliche Auslegung und Anwendung des Rechts ist bis zu einem bestimmten Punkt dem Föderalismus immanent. Die nationalen Behörden haben in der Konferenz der Unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in der Vergangenheit gemeinsame Standards und Leitlinien festgelegt und bis auf wenige Ausnahmen eine einheitliche, gemeinsame Linie verfolgt. Die Abstimmung wesentlicher Rechtsfragen in der Datenschutzkonferenz, in der alle Landesbeauftragten und der Bundesbeauftragte vertreten sind, ermöglicht eine harmonisierte Anwendung des Rechts und dient der Herstellung und Wahrung einer einheitlichen Linie im Vollzug. Wer dies ändern will, trägt zunächst einmal die

Argumentationslast und sollte Beispiele anführen, inwieweit die Praxis hier nicht funktioniert.

Im nationalen Bereich verbietet sich eine Zentralisierung der Datenschutzaufsicht in einer Bundesbehörde neben dem verfassungsrechtlichen Argument auch unter dem Aspekt der mangelnden Bürgernähe. Auch kann diese nicht im Interesse der regionalen Wirtschaft liegen, die den direkten Draht zu der Datenschutzbehörde vor Ort verlieren würde.

Bei näherer Betrachtung zeigt sich: Das Problem liegt nicht im Bereich des nationalen Vollzugs, sondern auf EU-Ebene. Hier gibt es sehr unterschiedliche Standards sowie einen Vollzugsstau gerade gegenüber globalen Tech-Unternehmen mit Sitz in einigen wenigen EU-Mitgliedstaaten. Vor allem funktioniert das aufsichtsbehördliche Verfahren der DSGVO nicht, das einen bürokratischen und schwerfälligen Vollzug vorsieht und in der gegenwärtigen Praxis zum Forum-Shopping der Unternehmen einlädt, die naturgemäß an einer strengen Aufsichtsbehörde nicht interessiert sind. Auf europäischer Ebene besteht daher massiver Handlungsbedarf. Das Thema Datenschutz darf in Europa nicht auf eine Standortfrage reduziert werden und einzelnen Unternehmen Vorteile verschaffen, weil sie ihre Hauptniederlassungen in einem bestimmten Mitgliedstaat genommen haben.

4.2 Die Unabhängigkeit ist zu wahren!

Die Zukunft des Datenschutzes hängt ganz wesentlich von der Unabhängigkeit der Stellen ab, die die Einhaltung der Datenschutzregeln überwachen und kontrollieren sollen. Die völlige Unabhängigkeit der Aufsichtsbehörden wird im EU-Primärrecht und Sekundärrecht seit vielen Jahren garantiert. Das bedeutet nicht, dass eine politische Einflussnahme auf Entscheidungen der unabhängigen Stellen praktisch kein Thema ist. Es gibt viele Verbindungslinien und Schnittstellen zwischen Datenschutzaufsicht und politischer Gestaltung. Dies beginnt - auch ohne dass eine Rechts- und Fachaufsicht sowie eine Dienstaufsicht über die unabhängige Stelle besteht - bei der trans-

parenten Auswahl der Behördenleiterin bzw. des Behördenleiters (Art. 53 Abs. 1 DSGVO) und endet bei der Frage der Ausstattung in personeller wie technischer Sicht. Gerade Mängel in der Ausstattung können sehr schnell die Unabhängigkeit beeinträchtigen. Dies ist der Fall, wenn personelle oder finanzielle Defizite auf die Entscheidungen der unabhängigen Stelle durchschlagen.

Über den Haushalt der unabhängigen Stellen entscheidet die kontrollierte Stelle selbst durch das durch die Verfassung vorgegebene Haushaltsverfahren. Das ist mit Blick auf die Regierung bei der Aufstellung des Haushaltsplans der Fall, aber auch bei der Entscheidung des Haushaltsgesetzgebers über den Haushalt selbst. Auch wenn die Kontrolle von parlamentarischen Kerntätigkeiten in der Vergangenheit nicht zu den Aufgaben der Datenschutzaufsicht in Bund und Ländern gehört, steht doch zumindest die Parlamentsverwaltung unter deren Kontrolle. Jüngst hat der EuGH überdies die Geltung der Regelungen der DSGVO auch auf die Kerntätigkeit der Parlamente (insbesondere den Petitionsausschuss) ausgedehnt (EuGH C-272/19).

Um die Unabhängigkeit der Kontrollstellen zu wahren, sollte das Verfahren zu deren finanzieller und personeller Ausstattung ein Höchstmaß an Objektivierbarkeit und Transparenz aufweisen. Entscheidungen über den Haushalt der unabhängigen Stelle sollten daher durch die Entscheidung eines unabhängigen Gremiums vorbereitet und an der tatsächlichen Bedarfssituation ausgerichtet sein (s.o.). Dies sichert die Neutralität des Entscheidungsfindungsprozesses und ermöglicht eine sachgerechte Aufgabenerfüllung der unabhängigen Stellen.

4.3 Aufsichtsbehörden als Partner, nicht als Gegner von Innovationsoffenheit und digitalem Aufbruch wahrnehmen!

Vor dem Hintergrund der Erfahrung der letzten Jahr und insbesondere des vorliegenden Berichtszeitraum in 2020 muss hervorgehoben werden: Digitaler Aufbruch, Innovationsoffenheit und die Schaffung einer modernen digitalen Infrastruktur sind zentrale Ziele und in einem Europa der Grundrechtecharta und der Datenschutz-

grundverordnung nicht gegen, sondern nur mit dem Datenschutz umzusetzen. Das funktioniert nicht ohne eine Kultur der Kommunikation und Kooperation. Ob nun beim Einsatz bei der Einführung von Videokommunikationsmitteln in Schulen und in Universitäten oder bei der Formulierung von Regelungen zur Rückverfolgbarkeit von Infektionsketten: Die Datenschutzbehörden sind immer auch Partner öffentlicher Stellen und sollten früh genug von diesen einbezogen werden. Dies ist im zurückliegenden Berichtsjahr leider nicht immer erfolgt.

Im Berichtszeitraum erreichte den HmbBfDI ein Brief von einer zentralen Stelle des Senats, in dem ihm empfohlen wurde, sich darauf zu beschränken, die Verwaltung zu kontrollieren, denn er sei nicht der IT-Berater des Senats. Dies zeigt eine Grundhaltung, die es zu überwinden gilt. Die Beratungsaufgabe ist eine zentrale Funktion von Datenschutzbehörden. Sie sind im Boot, wenn es darum geht, Herausforderungen der Digitalisierung in menschengerechter und souveräner Weise anzugehen. Die Tätigkeit von Aufsichtsbehörden auf Kontroll- und Sanktionsfunktionen zu beschränken, mag einem weit verbreiteten Vorurteil entsprechen. Ein zukunftsfähiges Konzept ist es nicht, Aufsichtsbehörden in das Bremserhäuschen zu setzen und sie bei Strategiediskussionen und Planungen außen vor zu lassen. Politisch und ökonomisch führt dies in eine Sackgasse, denn zukunftsfähige Entwicklungen kommen ohne die Berücksichtigung des Rechts auf Privatsphäre, informationelle Selbstbestimmung, die Vertraulichkeit und Integrität informationstechnischer Systeme nicht aus. Privacy by Design und Privacy by Default sind bereits heute integrative Bestandteile einer digitalen Innovation, die den Fortschritt nicht als Selbstzweck, sondern im Dienste der Menschen begreift. Offene Kommunikation und Kooperation und der klare Wille, moderne und gut ausgestattete Behörden für den Datenschutz für die Umsetzung dieser Aufgaben zu schaffen, sind hierfür Voraussetzung. Dies sollte künftig selbstverständlich sein.

CORONA-PANDEMIE II.

1. Corona-Eindämmungsverordnung

Die HmbSARS-CoV-2-Eindämmungsverordnung hat im Jahr 2020 nicht nur das öffentliche Leben in Hamburg bestimmt, sondern auch zahlreiche Grundrechtseingriffe, auch in das informationelle Selbstbestimmungsrecht, ermöglicht. Der HmbBfDI hat Hilfestellungen bei der Auslegung geleistet und auf Anpassungen hingewirkt.

Zur Eindämmung der Neuinfektionen mit dem Coronavirus hat der Hamburger Senat am 2. April 2020 die HmbSARS-CoV-2-EindämmungsVO erlassen. Darin wurden weitreichende Kontaktbeschränkungen, Gewerbeschließungen und Veranstaltungsverbote eingeführt. Im Laufe des Jahres wurde die Verordnung 23 Mal an die veränderte Pandemielage und an Bund-Länder-Absprachen angepasst. Dabei wurden unter anderem auch Ermächtigungen und Verpflichtungen zu datenschutzrelevanten Eingriffen eingefügt. Dies betrifft vor allem die verpflichtende Erfassung der Kontaktdaten von Gästen in Restaurants, Friseursalons sowie weiteren Einrichtungen und Veranstaltungen. Auch andere Regelungen, etwa zur Glaubhaftmachung der Befreiung von der Pflicht zum Tragen eines Mund-Nasen-Schutzes, haben Datenschutzbezug.

Die Verordnung basiert auf §§ 28, 32 Satz 1 und 2 des Infektionsschutzgesetzes (IfSG). Aufgrund ihrer weitreichenden Grundrechtseingriffe hat der HmbBfDI sich dafür ausgesprochen, die wesentlichen Befugnisse durch ein Parlamentsgesetz zu regeln. Die dem zugrundeliegenden, auch von vielen Akteuren geäußerten verfassungsrechtlichen Bedenken wurden mit der Schaffung des § 28a IfSG am 18. November 2020 aufgegriffen, sodass die besonders invasive Kontaktdatenerfassung nun auf einer dem Parlamentsvorbehalt genügende Grundlage steht.

Die sich stetig verändernde Verordnung hat zu zahlreichen Nachfragen bei Unternehmerinnen und Unternehmern sowie Betroffenen

geführt, welche Anforderungen an Datenerhebungen und -verwendungen zu stellen sind. Dieser Verunsicherung ist der HmbBfDI neben Einzelberatungen auch mit Hilfestellungen wie dem fortlaufend angepassten Internetratgeber „Datenschutz in Zeiten von Covid-19" gerecht geworden.

Weder beim erstmaligen Erlass noch bei den Neufassungen der CoV-2-EindämmungsVO hat der Senat den HmbBfDI beteiligt. Dies ist nicht nur vor dem Hintergrund zu bedauern, dass die Gewährung der Gelegenheit zur Stellungnahme in der Beteiligungsrichtlinie des Senates vorgesehen ist. Auch um seine Expertise und die Erfahrung mit Beratungsfällen in die Fortentwicklung der Verordnung einfließen zu lassen, hat der HmbBfDI wiederholt darum gebeten, bei weiteren Änderungen konsultiert zu werden.

Immerhin hat der Senat doch mehrfach Änderungen vorgenommen, nachdem der HmbBfDI in seinem öffentlichen Beratungsangebot auf Unklarheiten im Verordnungstext hingewiesen hatte. So ist beispielsweise aufgefallen, dass mit der Fassung vom 13. Mai 2020 zunächst die Erfassung von „Kontaktdaten" in bestimmten Einrichtungen zwar verpflichtend war, dieser Begriff aber nicht definiert war. Dies führte bei Betroffenen und Verantwortlichen aufgrund der Vielzahl denkbarer Kommunikationsmedien zu großen Unsicherheiten. Nach dem Hinweis des HmbBfDI, dass ohne konkrete Begriffsbestimmung ein Wahlrecht der Gäste besteht, welche Daten sie offenbaren möchten, hat der Senat mit der Novelle vom 30. Juni 2020 bestimmt, dass Name, Postanschrift und eine Telefonnummer anzugeben sind. Ein weiteres Beispiel ist eine bis zum 30. Juni 2020 in der Verordnung enthaltene missverständliche Bestimmung, die teilweise als Anforderung an Gastwirtinnen und -wirte verstanden wurde, zu überprüfen, ob Gäste an einem Tisch demselben Haushalt angehören würden. Nach dem Hinweis des HmbBfDI auf diese seiner Ansicht nach falsche Interpretation, wurde die Klausel bei der nächsten Überarbeitung aus der Verordnung gestrichen. Auch erfolgte eine Klarstellung der Prüfungspflicht der zur Erhebung der Kontaktdaten verpflichteten Stellen sowie der Rechtsfolgen bei nicht oder nicht ordnungsgemäßer Angabe.

Es steht außer Frage, dass das pandemische Geschehen schnelle Reaktionen erfordert. Dies allein erklärt nicht, die fehlende Bereitschaft zur Kommunikation. Die ausgelösten Unklarheiten bei der Umsetzung der Regelungen im Bereich der Gastronomie hätten durch eine Beteiligung der Datenschutzbehörde im Vorfeld sicherlich verhindert werden können.

2. Prüfung der Kontaktdatenerfassung in Gaststätten

Gaststättenbetriebe müssen die Datenschutzvorschriften umsetzen und alle nötigen technischen oder organisatorischen Maßnahmen ergreifen, um die Kontaktdaten der Kundinnen und Kunden, die zur Nachverfolgung von Infektionsketten erhoben werden, zu schützen. Die sichere Verwahrung der Kontaktdaten vor Ort erwies sich in der Praxis mitentscheidend für die Akzeptanz der Erfüllung der bestehenden Angabepflichten durch die Betroffenen.

Zahlreiche Gaststättenbetriebe und Betroffen haben sich im Berichtszeitraum an den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) gewandt, weil eine große Unsicherheit herrschte, wie die Kontaktdatenverarbeitung nach der Hamburgischen SARS-CoV-2-Eindämmungsverordnung umzusetzen ist. Betroffene berichteten zudem über die teilweise verbreitete Praxis, offene Listen im Eingangsbereich auszulegen. Dies ist insofern datenschutzrechtlich problematisch, da die Kontaktdaten dadurch für alle nachfolgenden Gäste unbefugt offengelegt werden.

Hintergrund für die Kontaktdatenerhebung in Gaststätten ist die seit dem 13.5.2020 bestehende Verpflichtung der Betriebsinhaber in verschiedenen Branchen, die Namen und Kontaktdaten aller Gäste zu erfassen. Dies folgt aus der HmbSARS-CoV-2-Eindämmungs-

VO und betrifft auch den Bereich der Gaststätten. Es besteht somit eine Verpflichtung und damit gemäß Art. 6 Abs. 1 lit. c DSGVO auch die Berechtigung, Kontaktdaten und Zeitpunkt des Aufenthalts schriftlich zu dokumentieren und vier Wochen lang aufzubewahren. Zu den Kontaktdaten gehört auch der Name. Hinsichtlich der weiteren Kontaktdaten hat die Verordnung zunächst keine Vorgabe gemacht, sodass es nach Auffassung des HmbBfDI den Besuchern freistand, sich z.B. für Postanschrift, Telefonnummer oder E-Mail-Adresse zu entscheiden. Wurden mehr als diese Daten abgefragt, lag offensichtlich ein Verstoß gegen den Grundsatz der Datenminimierung und folglich ein Verstoß gegen die DSGVO durch die Gaststättenbetriebe vor, da diese verantwortlich waren für die Kontaktdatenerhebung.

Erst zum 30.06.2020 wurde die Regelung zur Kontaktdatenerhebung konkretisiert und dahingehend erweitert, dass die Kontaktdaten konkret definiert wurden als Name, Wohnanschrift und einer Telefonnummer. Nachdem der HmbBfDI den Gesetzgeber von Anfang an darauf hingewiesen hat, dass auch offene Listen nicht akzeptabel sind, hat der Senat erfreulicherweise auch einen entsprechenden Hinweis in die HmbSARS-CoV-2-EindämmungsVO aufgenommen. Dort heißt es nun, dass zu gewährleisten ist, dass unbefugte Dritte keine Kenntnis von den Daten erlangen. Die Regelung hat bis heute seine Gültigkeit behalten.

Der HmbBfDI hat die zahlreichen Beschwerden und Beratungsanfragen zum Anlass genommen, im Juni stichprobenartig 100 Gewerbe- und Gaststättenbetriebe hinsichtlich der Umsetzung der Kontaktdatenerhebung zu kontrollieren. Dabei lag der Schwerpunkt auf der Beratung und Sensibilisierung der Wirtschaft vor Ort bei der Umsetzung der Kontaktdatenverarbeitung nach den Regeln der DSGVO. Sanktionen waren in diesem Schritte noch nicht zu befürchten.

Bei der stichprobenartigen Prüfung stellte der HmbBfDI fest, dass 33 % der geprüften Betriebe für die Kontaktdatenverarbeitung Lis-

ten verwendeten, die offen herumlagen und für jedermann zugänglich waren (z.B. Listen, die offen auf dem Tresen, auf den Tischen oder aber am Eingang ausgelegt waren).

Die Beschwerdelage ist im weiteren Verlauf unverändert hoch geblieben. Auch die Presse berichtete, dass weiterhin viele Gaststättenbetriebe von der Praxis nicht abgewichen sind, offen ausliegende Listen für die Kontaktdatenverarbeitung zu verwenden.

Unsere daraufhin durchgeführte Nachkontrolle hat erwiesen, dass in einigen Gaststätten eine Umsetzung der Vorgaben entgegen unserer Anordnung nicht erfolgt ist, so dass eine Verhängung von weitergehenden Maßnahmen zur Durchsetzung der Datenschutzvorgaben angezeigt war. In drei Fällen wurden schließlich Bußgelder in Höhe von 50 bis 100 Euro verhängt.

Weitere Bußgeldverfahren wurden gegen Einzelpersonen und Unternehmen eröffnet, die Kontaktdaten zu persönlichen oder werblichen Zwecken missbraucht haben.

3. Prüfung Bezirksamt: Datenbeschlagnahme und Abgleich Melderegister

Die Durchsetzung von Vorschriften der HmbSARS-CoV-2-Eindämmungsverordnung durch die Gesundheitsämter hat zahlreiche datenschutzrechtliche Fragestellungen aufgeworfen. Natürlich muss der Staat bei Erlass einschneidender Regelungen sicherstellen, dass diese auch befolgt werden. Doch der Rechtsstaat bewährt sich auch und gerade in der Krise – daher muss die Durchsetzung der Regelungen in außergewöhnlichen Situationen den rechtsstaatlichen Vorgaben folgen.

Der HmbBfDI erfuhr aus der Presse, dass das Bezirksamt Mitte am

Wochenende des 19./20. September 2020 auf St. Pauli in verschiedenen Lokalitäten Kontaktdatenlisten beschlagnahmt und diese im Anschluss mit dem Melderegister abgeglichen hatte. Diese Berichterstattung nahm der HmbBfDI zum Anlass, den Sachverhalt im Rahmen eines eigenen Prüfungsverfahrens zu untersuchen.

Es wurde dabei festgestellt, dass die genannten Maßnahmen dem Zweck dienten, die Einhaltung von Vorgaben der HmbSARS-CoV-2-Eindämmungsverordnung zu überprüfen. Speziell der Melderegisterabgleich sollte darüber hinaus allgemeine Erkenntnisse liefern, ob die Vorgaben der Verordnung durch die Bürgerinnen und Bürger eingehalten werden oder ob flächendeckend fiktive, unrichtige oder unvollständige Daten angegeben wurden. Hierfür wurde geprüft, wie oft die gemachten Angaben mit den im Melderegister hinterlegten Anschriften übereinstimmen. Die so generierten Ergebnisse wurden nur statistisch und nicht personengenau gespeichert. Die Kontaktdatenlisten selbst wurden nach wenigen Tagen an die Betreiber der Lokalitäten zurückgegeben.

Die rechtliche Überprüfung dieses Sachverhaltes hat ergeben, dass der durch das Bezirksamt Mitte vorgenommene Abgleich der Kontaktdaten Betroffener mit dem Melderegister rechtswidrig war. Der Eingriff beruhte weder auf dem Verdacht eines Infektionsgeschehens, noch stand er im Zusammenhang mit Bußgeldverfahren, die aufgrund von Verstößen gegen die Eindämmungsverordnung durchgeführt wurden. Zum damaligen Zeitpunkt sah die Eindämmungsverordnung für Betroffene bei Verstößen, ihre Daten anzugeben, keine Bußgeldbewehrung vor. Maßnahmen gegen Betreiber von Gaststätten, die einen Abgleich der Kontaktdaten mit dem Melderegister gerechtfertigt hätten, bestanden mangels einer Pflicht zur Überprüfung der inhaltlichen Richtigkeit der Daten nicht. Ein Abgleich mit dem Melderegister war für den Nachweis fehlender bzw. offenkundig fehlerhafter Angabe der Kontaktdaten weder geeignet noch erforderlich.

Diese Kritik hat der Verordnungsgeber zum Anlass genommen, Anfang Oktober klarere Regelungen zu erlassen, wozu genau Gastro-

nomen verpflichtet sind und unter welchen Voraussetzungen die zuständige Behörde sich Kontaktdaten der Besucher herausgeben lassen darf. Aus diesem Grunde hat der HmbBfDI davon abgesehen, förmliche Maßnahmen wie etwa eine Verwarnung in Bezug auf diese Datenverarbeitung zu treffen.

4. Prüfung einer Weisung der Sozialbehörde zur Übermittlung von Kontaktdaten infizierter Schülerinnen und Schüler von den Gesundheitsämtern an die BSB

In der Bekämpfung des Pandemiegeschehens bestand großes Konfliktpotential bezüglich verschiedener Bereiche des Schulwesens. Insbesondere die Übermittlung von Daten positiv getesteter Schülerinnen und Schüler von den Gesundheitsämtern an die Behörde für Schule und Berufsbildung (BSB) warf komplexe datenschutzrechtliche Fragen auf.

Der HmbBfDI ist am 05.10.2020 darüber informiert worden, dass die Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration sowie die Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke alle Gesundheitsämter der Freien und Hansestadt Hamburg am 06.10.2020 förmlich angewiesen haben, nach § 6 Abs. 1 Satz 1 Nummer 1 Buchstabe t des Infektionsschutzgesetzes neben den Schulen auch regelhaft der Behörde für Schule und Berufsbildung Daten über Namen, Geburtsdatum und die Wohnanschrift von positiv getesteten Schülerinnern und Schülern zu übermitteln. Im Kern ging es dabei um die Rechtmäßigkeit einer derartigen Datenübermittlung und darum, ob sich die Mitarbeiter des Gesundheitsamtes rechtswidrig verhalten oder gar nach § 203 StGB strafbar machen würden, wenn sie personenbezogene Gesundheitsdaten nicht nur regelhaft an die betroffenen Schulen, sondern auch an die BSB übermittelten.

Zur datenschutzrechtlichen Prüfung dieses Sachverhaltes hat der HmbBfDI ein Prüfverfahren eingeleitet. In dessen Rahmen wurde die Übermittlung von Daten über Namen, Geburtsdatum und die Wohnanschrift von positiv getesteten Schülerinnern und Schülern von den Gesundheitsämtern an die Behörde für Schule und Berufsbildung als dem Grunde nach rechtmäßig befunden.

Die Rechtmäßigkeit der Verarbeitung dieser Daten durch die BSB ergab sich aus Art. 6 Absatz 1 lit. e DSGVO i.V.m. § 98 HmbSG. Die Verarbeitung der Klarnamen infizierter Schülerinnen und Schüler war nämlich zur Erfüllung der der BSB nach § 23 HambSARS-CoV-2-EindämmungsVO zugewiesenen Aufgaben erforderlich. Diese Vorschrift weist der BSB und den Schulen gemeinsam Aufgaben des Infektionsschutzes zu. Diese Aufgaben wurden durch die BSB durch die Erstellung von Musterhygieneplänen nach § 23 Absatz 1 HambSARS-CoV-2-EindämmungsVO umgesetzt. Die Schulen setzten diese Musterhygienepläne als Einrichtungen gemäß § 33 Infektionsschutzgesetz (IfSG) durch konkrete Hygienepläne um. Der Inhalt der Hygienepläne orientierte sich dabei an den Vorgaben zur Gestaltung des Unterrichtsbetriebs nach § 23 Absatz 2 HambSARS-CoV-2- EindämmungsVO, wonach z.B. sicherzustellen war, dass Schülerinnen und Schüler, für die eine behördliche Quarantäne angeordnet ist, die Schule nicht betreten (§ 23 Absatz 2 Nr.2 letzter Halbsatz HambSARS-CoV-2-EindämmungsVO). Um diese Aufgabe zu erfüllen, bedurfte es der Kenntnis der Klarnamen der betroffenen Schülerinnen und Schüler. Die grundsätzliche Entscheidung über die Notwendigkeit der Erhebung dieser Daten trafen dabei die BSB im Rahmen des Aufstellens von Hygienevorgaben und die betroffene Schule im Rahmen der konkreten Umsetzung dieser Vorgaben. Die Kenntnis der Klarnamen war dabei für die betroffene Schule zur Erfüllung der Verpflichtung aus § 23 Absatz 2 HambSARS-CoV-2-EindämmungsVO notwendig, um z.B. konkrete Hausverbote gegen die betroffenen Schülerinnen und Schüler auszusprechen. Auch wenn die BSB im Rahmen des § 23 Absatz 1 HambSARS-CoV-2-EindämmungsVO vorwiegend allgemeine Vorgaben durch Musterpläne gibt, so kommt ihr als Schulaufsicht die Überwachungsfunktion hinsichtlich der Einhaltung der Verpflichtung

aus § 23 Absatz 2 HambSARS-CoV-2-EindämmungsVO zu, sodass auch für die BSB die Kenntnis der Klarnamen zu diesem Zweck notwendig ist. Im Einzelfall hat die BSB als Schulaufsicht die Pflicht zu überprüfen, ob die Schule Hausverbote ausgesprochen hat und insofern Pflichten des Infektionsschutzes erfüllt hat.

Vor diesem Hintergrund war die Datenübermittlung dem Grunde nach nicht zu beanstanden. Die betroffenen Behörden wurden jedoch noch einmal auf die Erfüllung der datenschutzrechtlichen Nebenpflichten, insb. der Informationspflichten und der erforderlichen Datensicherheitsmaßnahmen, aufmerksam gemacht.

5. Videokonferenzsysteme im Schulunterricht

Die pandemiebedingte Schließung der Hamburger Schulen im Frühjahr des Jahres 2020 brachte den Einsatz von Videokonferenzsystemen und anderen digitalen Diensten zur Durchführung von Distanzunterricht mit sich, deren datenschutzkonformer Einsatz die Schulen vor Herausforderungen stellte. Datenschutzrechtliche Belange blieben zunächst oft unberücksichtigt, was jedoch aufgrund der besonderen Problematik nur Beratungen durch die Aufsichtsbehörde nach sich zog.

Während der coronabedingten Schließungen der Schulen im Frühjahr des Jahres 2020 sahen sich die Behörde für Schule und Berufsbildung (BSB) und die Hamburger Schulen vor der Aufgabe einen digitalen Distanzunterricht zu organisieren, ohne bereits eine digitale Strategie oder ein entsprechendes Konzept erarbeitet zu haben. In der Folge entwickelten zumeist die Schule eigenständige Lösungen und setzten dabei auf ganz verschiedene Lösungen und Produkte ohne datenschutzrechtliche Fragstellungen hinreichend zu berücksichtigen, was für zahlreiche Eingaben und Beschwerden beim Ham-

burgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) sorgte.

Die Beschwerden, die den Einsatz ganz unterschiedlicher Videokonferenzsysteme und digitaler Lernmittel zum Gegenstand hatten, wurden durch den HmbBfDI in einem intensiven Kontakt mit dem behördlichen Datenschutzbeauftragten der BSB verfolgt. Der HmbBfDI verfolgte aufgrund der pandemiebedingten Ausnahmesituation eine kooperative Lösung und hat der BSB und dem Senator für Schule und Berufsbildung verschiedene Kooperationsangebote unterbreitet, um bei dem Aufbau eines behördlichen Angebotes eines Videokonferenzsystems, bzw. einer entsprechenden Lernplattform für die Durchführung eines Distanzunterrichts in datenschutzrechtlicher Hinsicht Hilfestellungen zu leisten. Während auf der Arbeitsebene im Rahmen der Beschwerdebearbeitung eine intensive Zusammenarbeit folgte, blieben die konkreten Kooperationsangebote auf höherer Ebene leider unbeantwortet. Dennoch trat die BSB in der zweiten Dezemberhälfte in eine grundsätzliche Planung einheitlicher Vorschriften für einen digitalen Schulunterricht ein und beteiligte den HmbBfDI.

Der Aufbau eines behördlichen Angebotes eines Videokonferenzsystems bzw. einer digitalen Lernplattform ist in Hamburg nicht zuletzt bereits vor dem Hintergrund der Datenschutzvorschriften des hamburgischen Schulrechtes geboten. Nach der Vorschrift des § 98 b Hamburgisches Schulgesetz (HmbSG) ist nur die zuständige Behörde befugt, elektronische Lernportale und pädagogische Netzwerke zu betreiben und im Unterricht einzusetzen um den Schülerinnen und Schüler mediale Kompetenzen zu vermitteln. Nach § 98 Absatz 2 HmbSG darf sich die zuständige Behörde nur in Ausnahmefällen dafür anderer Stellen außerhalb des öffentlichen Bereichs bedienen und deren digitale Lernangebote und Lerninhalte in die schulisch betriebenen Netzwerke einbinden. In diesem Fall ist aber für eine besondere Sicherung der Daten der Schülerinnen und Schüler zu sorgen. Zudem dürfen die Daten der Schülerinnen und Schüler nur anonymisiert, aggregiert oder pseudonymisiert genutzt werden.

Die Voraussetzungen konnten in den beim HmbBfDI anhängigen Beschwerdefällen nicht erfüllt werden, so dass die für den Einsatz von Videokonferenzsystemen und anderen digitalen Lernmitteln notwenigen Verarbeitung der personenbezogenen Daten der Schülerinnen und Schüler nicht auf die insoweit bereichsspezifische und damit abschließende Regelung des § 98 b HmbSG als Rechtsgrundlage in Verbindung mit § 6 Abs. 1 S. 1 lit. e Datenschutz-Grundverordnung gestützt werden konnte.

In der Folge wurde durch den Datenschutzbeauftragten der BSB durch Beratung der Schulen dafür gesorgt, dass eine Verarbeitung personenbezogener Daten der Schülerinnen und Schüler beim Einsatz von Videokonferenzsystemen oder anderen digitalen Lernmitteln, die nicht die Voraussetzung des § 98b HmbSG erfüllten, nur bei Einwilligung durch die Schülerinnen und Schüler, bzw. durch deren Eltern stattfand und somit auf die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. a DSGVO gestützt werden konnte. Das machte eine vorherige Information über Art und Umfang der Datenverarbeitung notwendig. Im schulischen Bereich war in diesem Zusammenhang darauf zu achten, dass die Einwilligung tatsächlich freiwillig erteilt werden konnte, so dass dafür insbesondere vergleichbare und angemessene Unterrichtsmittel als Alternative zum Unterricht über einen digitalen Dienst zur Verfügung zu stellen waren.

Zu den datenschutzrechtlichen Rahmenbedingungen, die beim Einsatz von Videokonferenzsystemen zu beachten sind, wird zudem auf die von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) am 23.10.2020 veröffentlichte Orientierungshilfe (OH) zum Einsatz von Videokonferenzsystemen, die darin auch für den schulischen Bereich abstrakt die rechtlichen Anforderungen an den Aufbau, Betrieb und Wartung von Videokonferenzsysteme definiert, verwiesen (siehe dazu unter II 10).

Der Einsatz von Videokonferenzsystemen durch kommerzielle Anbieter, die häufig in intransparenter Weise die bei der Nutzung anfallenden Daten von betroffenen Schülerinnen und Schülern, aber

auch von Lehrerinnen und Lehrern für eigener Zwecke verarbeiten, erschwert die in informierter Weise abzugebenden Einwilligung als Rechtsgrundlage in der Praxis. Hinzu kommt, dass im schulischen Verhältnis die Freiwilligkeit beim Einsatz von Videokonferenzsystemen grundsätzlich in Frage steht: Gerade in einer Situation der Schulschließung ist der Druck auf alle Beteiligten hoch, sich alternativer Kommunikationskanäle zu bedienen und deren Einsatz vor Ort zuzustimmen. Insoweit bleibt nur wenig Raum für Einwilligungslösungen, die es ermöglichen, den Anforderungen des § 98 b SchulG zu entgehen.

Es ist zu begrüßen, dass die Schulbehörde diesen Bedenken Rechnung tragend eine umfassende und einheitliche Regelung für den digitalen Unterricht flächendeckend für alle Hamburger Schulen anstrebt. Dabei soll eine § 98 SchulG ausgerichtete Regelung das Live-Streaming von Schulunterricht aus besonderem Anlass zukünftig ermöglichen, so dass der damit verbundene Eingriff in die Privatsphäre Betroffener auf eine klare parlamentsgesetzliche Regelung gestellt wird.

Der HmbBfDI tritt für eine nachhaltige Verankerung des Schutzes der informationellen Selbstbestimmung aller am digitalen Lernen Beteiligten ein und berät die Beteiligten auf der Suche nach einer modernen die Privatsphäre der Betroffenen angemessen berücksichtigenden Lösung.

6. Prüfung IFB und Nect-App

Die erste Welle der Covid-19-Pandemie hat nicht nur das Gesundheitssystem, sondern auch viele Wirtschaftszweige unter enormen Druck gesetzt. Die Regierungen versprachen daher die schnelle und unbürokratische Auszahlung von Soforthilfen. Deren Umsetzung hat allerdings diverse datenschutzrechtliche Schwachstellen aufgeworfen.

Wie auch andere Bundesländer ist Hamburg in das Visier von Betrügern geraten, die fehlende Datensicherheitsmaßnahmen auszunutzen versuchten, indem sie mit gefälschten oder abgegriffenen Daten Zahlungen beantragten. Damit gab es auch hier Bedarf zur Nachjustierung.

Die Auszahlung von Soforthilfen wurde in der Freien und Hansestadt Hamburg durch die Investitions- und Förderbank Hamburg (IFB) übernommen. Nach Aufdeckung von Phishing-Angriffen begann die IFB, zur Identifizierung von Antragstellern eine von der Nect GmbH zur Verfügung gestellte App einzusetzen, die den Identifizierungsprozess übernehmen sollte. Die Nect GmbH verarbeitete hierdurch Daten von Antragstellern, wofür sie sich maßgeblich auf Einwilligungen als Rechtsgrundlage stützte.

Die App realisierte eine weitgehend automatisierte Prüfung der Identität und Authentizität der Antragsteller. Sie ersetzte damit den Einsatz von Mitarbeitern, die im Online-Verfahren z. B. mittels eines Videotelefonats durch Vorzeigen eines Ausweisdokuments die korrekte Identität von Antragstellern erkennen mussten. Der App musste das Ausweisdokument dagegen mittels der Handy-Kamera vorgelegt werden. Zudem wurde durch das Nachsprechen eines von der App vorgegebenen kurzen Texts sichergestellt, dass es sich um eine echte Person handelt. Im Rahmen der App wurden biometrische Daten verarbeitet, um die angestrebte Echtheitsprüfung durchführen zu können, was auf die entsprechende Einwilligung der Antragsteller gestützt wurde.

Der HmbBfDI erfuhr durch diverse Beschwerden von diesem Sachverhalt und leitete eine Prüfung ein. Da die Verarbeitung personenbezogener Daten im Zuge der Authentifizierung durch die App auf Grundlage einer Einwilligung erfolgte, war fraglich, ob diese tatsächlich freiwillig hatte erteilt werden können. So konnten die Antragsteller ohne Authentifizierung durch die Nect GmbH nicht in den Genuss von den versprochenen Soforthilfen kommen. Zur Herstellung einer entsprechenden Freiwilligkeit der Einwilligung war es

daher erforderlich, dass Alternativen zu dem von der Nect GmbH betriebenen Authentifizierungsverfahren hergestellt wurden.

Mit diesen Bedenken wandte sich der HmbBfDI an den Anbieter der App und an die IFB. Der Anbieter wurde zur Beantwortung eines Katalogs an Fragen aufgefordert, woraus sich hinsichtlich der formalen Anforderungen wie Zweckbindung, Speicherfristen und Datenschutz-Folgenabschätzung keine Mängel erkennen ließen. Hinsichtlich der grundsätzlichen Frage einer einschlägigen Rechtsgrundlage griff die IFB die Bedenken des HmbBfDI auf und nahm die Anfrage zum Anlass, die Freiwilligkeit dadurch herzustellen, dass andere Alternativen eingerichtet wurden, sich als Antragsteller zu identifizieren. Hierbei griff sie auf das etablierte PostIdent-Verfahren zurück. Dessen Einrichtung ermöglichte es schlussendlich allen Personen, für die die Nutzung der Nect-App aus verschiedenen Gründen nicht in Betracht kam, ebenfalls Soforthilfen zu beantragen. Mit diesem erfreulichen Ergebnis konnte der Vorgang hier geschlossen werden.

7. Corona Warn App

Mit der Entwicklung der Corona Warn App ist die Bundesregierung neu Wege gegangen, sowohl bei ihrem offenen Entwicklungsmodell als auch ihrer datenschutzfreundlichen Funktionsweise. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat ihr Entstehen kritisch begleitet.

Auf der Suche nach einem gesellschaftlichen Umgang mit der aufkommenden Covid-19-Pandemie zu Beginn des Jahres wurde unter anderem eine Reihe technischer Lösungen zur Nachverfolgung von Infektionsketten und Vermeidung weiterer Infektionen durch bereits infizierte Personen diskutiert.

Unter den ersten Ideen befanden sich einige aus Datenschutzperspektive problematische Ansätze. Darunter insbesondere solche, die

auf die Erfassung von Standort- und anderen personenbezogenen Daten zur Verfolgung von Kontakten und eine zentrale Speicherung und Auswertung dieser Informationen setzten. Es haben sich jedoch schnell auch Projekte gebildet, die einen vertrauenswürdigen und datenschutzrechtlich verträglichen Ansatz verfolgten, wie z.B. PEPP-PT oder DP-3T, deren Design später von Apple und Google in einem bisher beispiellosen gemeinsamen Projekt in Form eines Contact Tracing Protokolls umgesetzt wurde. Die von T-Systems und SAP entwickelte Corona Warn App (CWA), für die sich die Bundesregierung am Ende entschieden hat, ermöglicht die Verfolgung von Kontakten unter Wahrung der Grundsätze der dezentralen Speicherung und der Freiwilligkeit auf datenschutzfreundliche Weise.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hatte die öffentliche Debatte und die Entwicklung der CWA über Monate hinweg begleitet und begrüßt ausdrücklich die Umsetzung eines dezentralen Systems zur Kontakterfassung. Dass die Corona Warn App mittlerweile von mehr als 24 Millionen Menschen (Stand 18. Dezember 2020) heruntergeladen wurde, ist durchaus ein Erfolg. Das Vertrauen großer Teile der Bevölkerung in die Datenschutzkonformität der App wäre bei einer zentralen Erfassung aller Daten auf einem vom Bund betriebenen Server sicherlich nicht zustande gekommen. Ein wichtiger, weiterer Grund war die quelloffene Entwicklung der CWA. Öffentlicher Source Code ermöglicht es, unabhängigen Stellen und der technisch versierten Öffentlichkeit, sich ein eigenes Bild von der App und ihrer Datenverarbeitung zu machen, sowie sich einzubringen, Fehler zu melden und neue Features vorzuschlagen. All dies hat in der Entwicklung der CWA stattgefunden und sollte ein Beispiel für zukünftige Softwareentwicklungen der öffentlichen Hand sein.

Die kürzlich neu aufgekommene Diskussion um eine App-Lösung, die an südostasiatischen Lösungen anknüpfen sollte und ggf. auf einem dezentralen Modell ohne Freiwilligkeit orientieren sollte, darf dieses Vertrauen am Ende nicht aufs Spiel setzen. Bei aller Sorge um die nach wie vor um sich greifende Pandemie und die massivs-

ten persönlichen und gesellschaftlichen Folgen, darf nicht vergessen werden, dass eine Tracking App, die alle Bewegungsdaten zentral erfasst, keineswegs eine Gewähr für eine erfolgreichere Bekämpfung des Virus enthält. Die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht könnten das Vertrauen der Bevölkerung in die CWA erschüttern und so ihre Funktionalität aushöhlen. Wäre die Freiwilligkeit in Frage gestellt, bliebe letztlich auch fraglich, wie eine Lösung aussehen soll, bei der die Menschen daraufhin kontrolliert werden, ob sie ihren Wohnort tatsächlich mit ihrem Handy verlassen oder dieses zu Hause einfach liegen lassen.

Die CWA hat gewiss Verbesserungspotential, insbesondere die fehlende Anbindung vieler Testlabore an ihre Infrastruktur gilt es zu optimieren. Ferner soll die App eine Clustererkennung ermöglichen und den Nutzenden die Funktion eines Kontakttagebuchs bereithalten, mit der diese ihre Begegnungen festhalten können. In Verknüpfung mit weiteren Maßnahmen, wie der Möglichkeit eines häufigeren Abgleichs der gesammelten IDs mit dem Server werden damit klarere Aussagen über Kontaktbegegnungen und eine präzisere Risikoermittlung möglich.

8. Arbeiten im Homeoffice

Die Arbeit im Homeoffice erfordert neben erhöhte technisch-organisatorische Maßnahmen im Umgang mit personenbezogenen Daten stets vorab auch eine Homeoffice-Vereinbarung.

Arbeiten im Homeoffice stellt nicht nur Arbeitnehmerinnen und Arbeitnehmer vor eine große Herausforderung, sondern auch Arbeitgeberinnen und Arbeitgeber, da diese auch im Homeoffice für die Verarbeitung personenbezogenen Daten durch ihre Mitarbeiterinnen und Mitarbeiter verantwortlich bleiben.

Bevor die Arbeit in das Homeoffice verlagert wird, sollten folgende

Punkte aus datenschutzrechtlicher Sicht beachtet werden:

- Eignung der Tätigkeit für das Homeoffice

Arbeitgeberinnen und Arbeitgeber sollten sich stets die Frage stellen, ob die Tätigkeit sich für das Homeoffice eignet. Bei dieser Betrachtung ist zunächst von großer Relevanz die Art der zu verarbeitenden personenbezogenen Daten. Je schützenswerter die personenbezogenen Daten sind, desto weniger eignet sich deren Bearbeitung im Homeoffice. Handelt es sich beispielsweise um Daten nach Artikel 9 DSGVO (z.B. Gesundheitsdaten), Sozialdaten oder Beschäftigtendaten ist daher besonders Vorsicht geboten.

- Homeoffice Vereinbarung

Die Arbeit im Homeoffice bedarf einer ausdrücklichen Vereinbarung – typischerweise eine Betriebsvereinbarung Homeoffice - in der sich mindestens folgender Inhalt wiederfinden sollte:

- Welche Arbeiten dürfen von zu Hause aus erledigt werden
- Wer stellt die technischen Geräte und Internetzugang (einschließlich Wartung und Reparatur) zur Verfügung
- Ist der Einsatz privater Hard- und Software erlaubt
- Muss der Arbeitsplatz besonders gesichert werden
- Regelungen zum Beschäftigtendatenschutz zur Arbeitszeit, zur Erreichbarkeit und Ableistung eines bestimmten Anteils der Arbeitszeit am betrieblichen Arbeitsplatz.

Da Art. 13 Grundgesetz die Unverletzlichkeit der Wohnung garantiert, haben Arbeitgeberinnen und Arbeitgeber kein generelles Zugangsrecht zu Wohnungen von Mitarbeiterinnen und Mitarbeitern. Ist der Zutritt ausdrücklich gewollt, so bedarf es für den Zugang zur Wohnung der Mitarbeiterinnen und Mitarbeitern einer wirksamen Einwilligung.

- Technisch-organisatorische Maßnahmen

Gefahren im Homeoffice können andere sein als am betrieblichen Arbeitsplatz. Diese müssen Arbeitgeberinnen und Arbeitgeber vorab ermitteln und geeignete technisch-organisatorische Maßnahmen ergreifen, um die Sicherheit der personenbezogenen Daten zu gewährleisten (Art. 32 DSGVO).

Geeignet sind Maßnahmen, die

- die die Mitarbeiterinnen und Mitarbeiter für den Datenschutz im Homeoffice sensibilisieren.
  Dies kann durch Schulungen zum Datenschutz erreicht werden.

- die räumliche Sicherheit im Blick haben.
  Gibt es einen gesonderten Arbeitsplatz, gesonderten Raum, ab vom übrigen Wohnbereich, der auch verschlossen werden kann? Können Telefonate oder Videokonferenzen von unberechtigten Dritten (insbesondere von Familienangehörigen oder Nachbarn) in räumlicher Nähe mitgehört werden? Können Arbeitsunterlagen und Notebooks, die personenbezogene Daten enthalten, nach Feierabend verschlossen verwahrt werden? Es sind nur so viele Unterlagen im Homeoffice zu verwahren, wie unbedingt erforderlich. Gegebenenfalls ist für das Homeoffice eine Obergrenze für Unterlagen mit personenbezogenen festzulegen.

- die die Datensicherheit beim IT-Einsatz gewährleisten.
  Wenn möglich sollen nur technische Geräte und Software eingesetzt werden, die vom Arbeitgeber oder von der Arbeitgeberin bereitgestellt werden. Werden eigene Geräte oder Software (Bring your own Device – BYOD) verwendet, so ist sicherzustellen, dass die dienstlichen und privaten Daten voneinander getrennt gehalten werden, Passwort gesichert sind und unterschiedliche Passwörter für den privaten und dienstlichen Gebrauch verwendet werden. Der Zugang zu personenbezogenen Daten sollte nur über eine gesicherte VPN (Virtual Private Network) Verbindung erfolgen und Ende-zu-Ende verschlüsselt werden. Bei der Rufumleitung vom dienstlichen auf das private Tele-

fon sollte sichergestellt werden, dass Gesprächsteilnehmerinnen und Gesprächsteilnehmer außerhalb der Organisation nur die Büronummer sehen.

Werden diese Vorgaben eingehalten, steht einer erfolgreichen Arbeit im Homeoffice nichts im Wege.

9. Covid-19-Prävention in Unternehmen

Unternehmen aller Branchen unternehmen derzeit große Anstrengungen, um Ansteckungen in ihren Geschäftsräumen zu unterbinden. Die Privatsphäre der Beschäftigten sowie der Kundinnen und Kunden darf dabei nicht außer Acht gelassen werden.

Unternehmensleitungen unterliegen einer Fürsorgepflicht gegenüber Beschäftigten sowie einer Verantwortung für Gesundheit ihrer Kundinnen, Kunden und sonstigen Gäste. Um diesen Anforderungen auch während einer Zeit mit außergewöhnlicher Ansteckungsgefahr gerecht zu werden, erscheinen in vielen Betrieben Datenerhebungen als legitim, die noch vor kurzem kaum vorstellbar waren. Sinnvollen Maßnahmen steht der Datenschutz dabei nicht entgegen. Jedoch ist auch die besondere Schutzwürdigkeit von Gesundheitsdaten stets zu beachten und ein angemessener Ausgleich mit der Privatsphäre der betroffenen Menschen zu suchen. Diese anspruchsvolle Aufgabe hat zu zahlreichen Beratungsanfragen beim HmbBfDI geführt. Deren Ergebnisse hat er auch proaktiv auf seiner Internetseite sowie auf Online-Veranstaltungen verbreitet.

Erste Fragen zum Gesundheitsschutz stellen sich bereits beim Zugang zu Geschäftsräumen und Betriebsstätten. Die Befragung von Kunden oder Besuchern von Ladenlokalen nach Krankheitssymptomen ist ebenso wie das Messen der Körpertemperatur mittels Wärmebildkameras oder Fieberthermometern unzulässig. Es handelt sich bei den dabei gewonnenen Informationen um Gesundheitsdaten, de-

ren Verarbeitung gemäß Art. 9 DSGVO nur in streng geregelten Fällen erlaubt ist. Von den Ausnahmetatbeständen kommt bei Kundinnen und Kunden nur die Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO in Betracht. Diese muss freiwillig geschehen, es darf also nicht der Zugang von ihr abhängig gemacht werden. Alternativ sollten Gäste der Geschäftsräume im Eingangsbereich durch Aufstellen oder Aushändigung von Hinweisschildern/-blättern darauf hingewiesen werden, dass sie bei Vorliegen von akuten respiratorischen Symptomen aufgefordert werden, das Unternehmen aus Gründen der Sicherheit für die Mitarbeiter und anderen Besucher/Kunden nicht zu betreten.

Bei Beschäftigten ist die Erfassung von Gesundheitsdaten zur Eindämmung der Pandemie unter Umständen nach § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b DSGVO gerechtfertigt. Die Erfassung der Körpertemperatur und die Erfragung von Covid-19-spezifischen Symptomen sind hier allenfalls gerechtfertigt an Arbeitsplätzen mit engem Körperkontakt oder besonders systemrelevanten Einrichtungen wie etwa Krankenhäusern. In den übrigen Betrieben sind Befragungen der Beschäftigten in eingeschränktem Umfang möglich. Um Kontakte mit potentiell infektiösen Kolleginnen und Kollegen zu vermeiden, ist es in der Pandemiesituation nicht zu beanstanden, wenn vor Betreten des Arbeitsplatzes erfragt wird, ob die betroffene Person selbst mit dem Covid-19-Virus infiziert ist, ob sie im Kontakt mit einer nachweislich infizierten Person stand oder ob sie sich im relevanten Zeitraum in einem vom Robert Koch Institut als Risikogebiet eingestuften Gebiet aufgehalten hat.

Nicht erlaubt ist beispielsweise die offen gestellte Frage, in welchem Land eine Urlaubsabwesenheit verbracht wurde oder mit welchen Personen der Betroffene in Kontakt stand. Eine Negativauskunft des Betroffenen, dass die oben genannten Punkte auf ihn nicht zutreffen, ist ausreichend. Alternativ zur individuellen Abfrage kann auch verlangt werden, dass Beschäftigte sich aktiv melden, wenn sie einen der oben genannten Punkte erfüllen.

Mit Beendigung des ersten Lockdown und der schrittweisen Rück-

kehr von Beschäftigten aus dem Homeoffice im Sommer 2020 kam vermehrt die Frage nach dem Schutz von Risikogruppen auf. Viele Arbeitgeberinnen oder Arbeitgeber beabsichtigten, Personen mit erhöhtem Schutzbedarf länger im Homeoffice zu belassen oder ihnen Einzelbüros zur Verfügung zu stellen. Dabei standen sie vor der Herausforderung, dass die Zugehörigkeit zu einer Risikogruppe nicht ohne weiteres erkennbar ist und dass keine Pflicht besteht, Arbeitgeberinnen und Arbeitgebern Diagnosen oder Krankheitssymptome zu offenbaren. Von diesem arbeitsrechtlichen Grundsatz ist auch in der Pandemie nicht abzuweichen. Es bleibt jedoch Beschäftigten unbenommen, von sich aus auf Vorerkrankungen hinweisen, um besondere Schutzmaßnahmen zu erlangen. Arbeitgeberinnen und Arbeitgeber dürfen dazu aufrufen, sich bei Bedarf zu melden und dürfen in diesem Fall die entsprechenden Daten verarbeiten. Bei der Aufbewahrung der Informationen ist auf einen besonderen Schutz nach § 26 Abs. 3 S. 3 BDSG i.V.m. § 22 Abs. 2 BDSG zu achten. Da von Angehörigen der Risikogruppen keine erhöhte Fremdgefährdung ausgeht, liegt es in der eigenen Verantwortung des jeweiligen mündigen Beschäftigten, darüber zu entscheiden, ob eine Preisgabe der Daten für ihn sinnvoll erscheint oder nicht.

Ist es schließlich trotz aller Vorsichtsmaßnahmen zu einer Infektion unter den Beschäftigten gekommen, kann es geboten sein, die Kolleginnen und Kollegen zu warnen. Die Identitäten positiv auf Covid-19 getesteter Mitarbeiterinnen und Mitarbeiter sind dabei vertraulich zu behandeln, soweit dies ohne Gesundheitsgefahr für andere möglich ist. Die Tatsache, dass ein Betroffener Träger des Virus ist, kann sehr stigmatisierende Wirkung haben. Daher ist die Offenlegung personenbezogener Daten von nachweislich infizierten oder unter Infektionsverdacht stehenden Personen zur Information nur rechtmäßig, soweit die Kenntnis der Identität für die Vorsorgemaßnahmen der Kontaktpersonen erforderlich ist.

Dabei ist je nach Empfängerkreis der Information differenziert vorzugehen. Abhängig von der Unternehmensgröße wird es in der Regel für die meisten Beschäftigte sowie gegebenenfalls für Externe

ausreichend sein, zu wissen, dass eine unbenannte Person aus einer konkreten Abteilung positiv getestet wurde. Gegebenenfalls sind Zusatzinformationen sinnvoll, etwa an welchen Tagen die Person anwesend war, an welchen Meetings sie teilgenommen hat und welche Gemeinschaftseinrichtungen (z.B. Kantine, Bibliothek) sie genutzt hat. Innerhalb der Abteilung wird je nach Abteilungsgröße eine weitere Differenzierung nach untergeordneten Organisationseinheiten möglich sein. Bei Personen, die direkten Kontakt hatten, kann die zielgerichtete Offenlegung der Identität erforderlich sein. Dies betrifft beispielsweise Personen, die sich ein Bürozimmer teilen oder solche, bei denen es wahrscheinlich ist, dass ein Händedruck stattgefunden hat. Die Zulässigkeit folgt dann aus § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b DSGVO.

10. Orientierungshilfe Videokonferenzsysteme

Videokonferenzen sind seit März 2020 fester Bestandteil im Arbeitsalltag vieler Menschen. Für den datenschutzrechtlich konformen Betrieb gilt es dabei einige Punkte zu beachten.

Mit weltweit steigender Verbreitung der Infektionskrankheit COVID-19 wurden auch in Hamburg mehr und mehr Arbeitsplätze in Unternehmen und Behörden auf Homeoffice umgestellt. Neben Fragestellungen zum sicheren Zugriff auf dienstliche Ressourcen waren dabei unter datenschutzrechtlichen Gesichtspunkten insbesondere eine massive Anzahl von Beratungsanfragen rund um Videokonferenzsysteme zu verzeichnen. Der Markt von Videokonferenzdiensten war bereits vor dem pandemischen Entwicklungsgeschehen im höchsten Maße divers und bot für unterschiedliche Nutzungsszenarien mehrere Software-Lösungen. Den Beratungsanfragen an den HmbBfDI war dabei stets immanent, dass Verantwortliche schnelle und leicht nutzbare Lösungen suchten. Rückgriffe auf kommerzielle Videokonferenzanbieter wurden deshalb rasch und oftmals ohne intensive Aus-

einandersetzung mit datenschutzrechtlichen Belangen durchgeführt.

Vor diesem Hintergrund hat der HmbBfDI bereits zu Beginn der Pandemie in einer umfangreichen FAQ die wichtigsten Anforderungen an solche Systeme aufgegriffen und den Verantwortlichen einen soliden Fahrplan zur datenschutzkonformen Nutzung bereitgestellt.

Nach einer näheren technischen und rechtlichen Untersuchung der jeweiligen Dienste konnte festgestellt werden, dass eine Vielzahl der Anbieter zum Teil fortwährend grundlegende Anpassungen der eigenen Dienste umsetzten und eine klare Aussage zum datenschutzkonformen Betrieb und Nutzung der Systeme daher nicht ohne weiteres und mit längerfristiger Gültigkeit getroffen werden konnte. Einige Dienste änderten mehrfach relevante technische Umsetzungen ihrer Dienste innerhalb kürzester Zeit. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 23.10.2020 eine Orientierungshilfe (OH) zum Einsatz von Videokonferenzsystemen veröffentlicht (https://datenschutz-hamburg.de/assets/pdf/OH-Videokonferenzsysteme.pdf), damit Verantwortliche einen verbindlichen Leitfaden für die Einführung und den Weiterbetrieb der Dienste für sich selbst erarbeiten können. Der OH Videokonferenzsysteme flankierend zur Seite gestellt, ist eine Checkliste, die in operationalisierbarer Form die Anforderungen zusammenfasst und für noch mehr Übersichtlichkeit sorgt. Bei der Erstellung hat sich der HmbBfDI aktiv auf allen Ebenen eingebracht und maßgeblich auch die hamburgische Positionierung durchsetzen können, so dass Verantwortliche deutschlandweit nunmehr einheitlichen Anforderungen vorliegen, denen es nachzukommen gilt. Vermehrt kam zudem der Wunsch auf, konkrete Dienste datenschutzrechtlich zu bewerten und Empfehlungen zu geben. Der HmbBfDI hat hierzu bislang keine individuellen Einschätzungen abgegeben, sondern im Zuge aufsichtsbehördlicher Prüfungen und im Rahmen öffentlicher Vorhaben die aus der OH Videokonferenzsysteme ableitbaren Maßnahmen eingefordert. Dies gestaltet sich mit Blick auf die vielen am Markt befindlichen Angebote und deren oft kurzfristige umgesetzte technischen Neuerungen schwierig.

Der HmbBfDI ist bestrebt, den Herstellern gegenüber stets die aus seiner Sicht umzusetzenden datenschutzrechtlichen Anforderungen zu kommunizieren. Dazu gehören natürlich auch grundsätzliche Anforderungen wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

Für eine vergleichende Betrachtung unterschiedlicher Videokonferenzsysteme wird auf die Hinweise der Berliner Beauftragten für Datenschutz und Informationsfreiheit verwiesen (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf). Den darin enthaltenen Ergebnissen schließt sich der HmbBfDI an, verweist jedoch zugleich auf zum Teil technisch überholte Untersuchungsobjekte.

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 16. Juli 2020 (Rechtssache C-311/18) zudem eine weitreichende Entscheidung zur Übermittlung personenbezogener Daten in die USA - die auch im Zusammenhang mit der Nutzung von Videokonferenzsystemen erfolgen - getroffen. Danach kann ein Drittlandtransfer von personenbezogenen Daten nicht mehr auf das sogenannte Privacy Shield gestützt werden. Die bestehenden Standardvertragsklauseln der Europäischen Kommission können allerdings grundsätzlich weiter genutzt werden. Es ist aber jeweils zu prüfen, ob in dem Drittland die Rechte der von der Datenverarbeitung Betroffenen auf einem zur Europäischen Union vergleichbaren Schutzniveau geregelt sind und die Standardvertragsklauseln tatsächlich ausreichend zur Geltung kommen. Bei Datenübermittlungen in die USA beispielsweise können die Klauseln nicht ohne zusätzliche Maßnahmen verwendet werden. Hierzu bedarf es wiederum zusätzlicher Garantien (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supp ementarymeasurestransferstools_en.pdf).

III. PRÜFUNGEN

1. Prüfung von Dateien im Sicherheitsbereich

Der HmbBfDI ist im Berichtszeitraum seiner gesetzlichen Verpflichtung zur Prüfung der Antiterrordatei (ATD) und Rechtsextremismus-Datei (RED) sowohl bei der Polizei Hamburg als auch beim Landesamt für Verfassungsschutz (LfV) Hamburg nachgekommen. Zudem wurde die Prüfung der CRIME-Datei „Aurelia" bei der Polizei Hamburg begonnen.

1.1 Pflichtkontrolle der RED und ATD beim LKA und LfV

Sowohl bei der ATD als auch der RED handelt es sich um eine gemeinsame standardisierte zentrale Datei die jeweils von verschieden Sicherheitsbehörden des Bundes sowie der Landeskriminalämter und der Verfassungsschutzbehörden der Länder beim Bundeskriminalamt geführt wird. Während die ATD dem Zweck der Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland dient (§ 1 Abs. 1 Antiterrordateigesetz (ATDG), wurde die RED zum Zweck der Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus, insbesondere der Verhinderung und Verfolgung von Straftaten mit derartigem Hintergrund geschaffen (§ 1 Abs. 1 Rechtsextremismus-Datei-Gesetz (REDG)). Mit diesen Dateien sollen 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 der Datei zu speichern (vgl. § 2 ATDG bzw. REDG). Die datenschutzrechtliche Verantwortung für die in der Datei gespeicherten Daten, namentlich für die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit und Aktualität der Daten, trägt die Behörde, die die Daten eingegeben hat (vgl. § 9 Abs. 1 S. 1 REDG bzw. § 8 Abs. 1 S. 1 ATDG).

Der HmbBfDI hat bei den in seinen Zuständigkeitsbereich fallen-

den Sicherheitsbehörden am 23.1.2020 (LfV Hamburg) und am 24.1.2020 (Polizei Hamburg LKA 7 – Staatschutzabteilung) eine Vor-Ort-Prüfung dieser Dateien durchgeführt. Neben der Prüfung der vorgelegten Dokumentationen und der technischen Rahmenbedingungen wurde stichprobenhaft die Speicherung von einzelnen Personen auf Plausibilität und Schlüssigkeit in den Dateien überprüft. Bei beiden Stellen konnten keine Mängel erkannt werden, die Prüfung führte somit nicht zu Beanstandungen: Dem HmbBfDI konnte im Hinblick auf beide Dateien jeweils erfolgreich dargelegt und demonstriert werden, dass beim Zugang zu den personenbezogenen Daten deren Sensibilität entsprechend hinreichend technisch gesichert und personell begrenzt ist. Insbesondere wurde dabei der Fokus der technischen Überprüfung auf Zugriffs- sowie Zugangsschutz gelegt und Berechtigungen der Sachbearbeitungen nachvollzogen. Die kontrollierten Speicherungen waren zudem jeweils fachlich nachvollziehbar. Die stichprobenhaften gesichteten Speicherungen entsprachen den gesetzlichen Voraussetzungen des ATDG bzw. REDG. Dabei ließ sich der HmbBfDI pro Datei bei jeweils ca. 10 Prozent der Speicherungen die Voraussetzungen bzw. den Grund der Speicherung darlegen. Ein besonderes Augenmerk wurde dabei darauf gelegt, dass eine aktive Pflege der Datei erkennbar war (z.B. bei laufenden Ermittlungsverfahren zu erwartende Verfahrensausgänge im Blick des Verantwortlichen stehen). Auch wurde geprüft, dass in sog. Freitextfeldern bei betroffenen Personen keine personenbezogenen Daten durch den Verantwortlichen in die Datei eingeführt werden, deren Speicherung das Gesetz nicht vorsieht.

Ähnlich wie der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) gelangt der HmbBfDI im Rahmen seiner Prüfung auch zu dem Schluss, dass andere Kommunikationswege und Kooperationsformen in der Praxis mehr Relevanz bei der Arbeit der Sicherheitsbehörden aufweisen dürften als die ATD- und RED-Dateien (vgl. BfDI 28. Tätigkeitsbericht zum Datenschutz, S. 52 ff.). Anlass für die vom HmbBfDI durchgeführte Prüfung waren die gesetzlichen Vorgaben, die vorschreiben, dass mindestens alle zwei Jahre eine Überprüfung des Datenbestandes durch die Datenschutzaufsicht zu

erfolgen hat. Damit ist der Gesetzgeber wiederum den Vorgaben des Bundesverfassungsgerichts gefolgt (BVerfG, Urteil v. 24.4.2013 – Az. 1 BVR 1215/07). Das höchste deutsche Gericht hatte bezüglich dieser Dateien entschieden, dass im Hinblick auf den schwach ausgestalteten Individualrechtsschutz der Kompensationsfunktion der aufsichtsrechtlichen Kontrolle besondere Bedeutung dann zukommt, wenn es sich um regelmäßige Kontrollen in angemessen Abständen handelt. (BVerfG a.a.O, Rn. 217). Bei der nunmehr im Januar 2020 durchgeführten Prüfung handelt es sich bereits um die jeweils zweite Prüfung des HmbBfDI der fraglichen Dateien bei den genannten Landesbehörden (vgl. zu vorherigen Prüfungen: Tätigkeitsbericht Datenschutz 2014/2015, S. 66 und 2016/17, S. 26). Obwohl das BVerfG die besondere Bedeutung der datenschutzrechtlichen Aufsicht gerade bei für den Bürger undurchsichtiger Datenverarbeitung hervorhebt und ausdrücklich anmahnt, diese besondere Bedeutung bei der Ausstattung der Aufsichtsbehörden zu berücksichtigen (BVerfG a.a.O, Rn. 217), ist es dem HmbBfDI gerade aufgrund von unzureichender personeller Ausstattung nicht möglich gewesen, die gesetzlich verankerte Prüfpflicht im Abstand von zwei Jahren einzuhalten. Auch im Hinblick auf die stets zunehmende Anzahl von turnusmäßig durchzuführenden Pflichtprüfungen von Dateien und Ermittlungsmaßnahmen im Sicherheitsbereich (vgl. § 73 des Gesetz über die Datenverarbeitung der Polizei) deutet sich bereits jetzt an, dass der HmbBfDI Schwierigkeiten haben wird, auch in Zukunft die gesetzlich verankerte Prüfpflicht mindestens alle zwei Jahre zu erfüllen. Dass trotz eindeutiger Vorgabe bislang keine personelle Verstärkung in diesem Bereich erfolgte, ist unverständlich und steht in Widerspruch zu verfassungsgerichtlichen Vorgaben.

1.2 Prüfung CRIME-Datei Aurelia

Der HmbBfDI hat im Berichtszeitraum zudem eine Prüfung der beim Landeskriminalamt 71 (Staatsschutz) geführten Datei „Aurelia“ begonnen. Diese landeseigene CRIME-Datei („Ciminal Research and Investigation Management Software“) dient der Gefahrenabwehr einschließlich der vorbeugenden Bekämpfung von Straftaten, ein-

schließlich extremistischer und terroristischer Straftaten aus den Bereichen politisch motivierter Kriminalität Rechts, Links, sowie ausländische Ideologien und nicht zuzuordnenbare politisch motivierte Kriminalität.

Auftakt der Prüfung des HmbBfDI war ein erster Vor-Ort Termin zur Sichtung der Datei beim LKA im November 2020. Der Schwerpunkt der laufenden Prüfung liegt - neben der Frage einer hinreichenden Zugriffssicherung und Protokollierung - auf der Einhaltung der Lösch-, Prüf- und Speicherfristen. Es ist insbesondere für den HmbBfDI von Interesse, ob bei Verlängerungen der Speicherungen die geforderten Einzelfallprüfungen durchgeführt wurden. Die gespeicherten Daten sind nämlich nach Ablauf von festgelegten Aussonderungsprüfungsfristen dahingehend zu überprüfen, ob die suchfähige Speicherung der Daten weiterhin erforderlich ist. Eine Verlängerung der Speicherung ist nur dann möglich, wenn besondere Gründe im Einzelfall gegeben sind (vgl. § 35 Gesetz über die Datenverarbeitung der Polizei). Der HmbBfDI hat im Berichtszeitraum damit begonnen, stichprobenhaft zu überprüfen, ob anhand von tragfähigen Begründungen die Erforderlichkeit einer weiteren Speicherung für die Erfüllung der Aufgaben nachvollziehbar und plausibel ist.

Anlass dieser Prüfung war, dass der HmbBfDI bei der Prüfung der CRIME-Datei „Gruppen und Szenegewalt" im Berichtszeitraum 2016/2017 erhebliche Defizite bei der polizeilichen Datenverarbeitung feststellen musste und letztlich auch eine formelle Beanstandung gegenüber der Behörde für Inneres und Sport (BIS) ausgesprochen hatte (vgl. HmbBfDI Tätigkeitsbericht Datenschutz 2016/17, S. 23 ff.). Im Rahmen der Beanstandung hatte der HmbBfDI eine Reihe von Empfehlungen an die BIS ausgesprochen um sicherzustellen, dass die Datei(en) in Zukunft datenschutzkonform geführt werden. Diese Umsetzung gilt es auch bei der nun in Prüfung befindlichen CRIME-Datei zu kontrollieren.

Der HmbBfDI wird im nächsten Tätigkeitsbericht über dem Ausgang der Prüfung berichten.

2. Videoüberwachung Hansaplatz

Seit August 2019 wird der Hansaplatz in St. Georg von der Polizei Hamburg videoüberwacht. Der HmbBfDI hat bereits im Berichtszeitraum 2019 eine umfangreiche Prüfung der Zulässigkeit der Videoüberwachung begonnen und diese im gegenständlichen Berichtszeitraum weitgehend abgeschlossen.

In seinem 28. Tätigkeitsbericht 2019 hat der HmbBfDI bereits ausführlich über die Prüfung der am 1. August 2019 gestarteten Videoüberwachung der Polizei Hamburg des Hansaplatzes in St. Georg durch den HmbBfDI berichtet. Nach umfangreicher datenschutzrechtlicher Prüfung kommt der HmbBfDI zu dem Ergebnis, dass keine Anhaltspunkte vorliegen, dass die Voraussetzungen für eine Videoüberwachung des Hansaplatzes und den direkt angrenzenden Straßen durch die Polizei Hamburg nicht vorliegen:

Grundsätzlich greift eine anlasslose Videoüberwachung wie diese in Grundrechte aller Betroffenen ein. Diese sind im Rahmen einer Videoüberwachung ganz überwiegend Passanten und Besucher, von denen keine Gefahr ausgeht und denen auch keine Gefahr droht. Der Einsatz von Videokameras durch die Polizei zum Zwecke Ihrer gesetzlichen Aufgabenerfüllung bedarf daher einer Eingriffsermächtigung in Form einer gesetzlichen Grundlage. Nach § 18 Abs. 3 des Gesetzes über die Datenverarbeitung der Polizei darf die Polizei zur vorbeugenden Bekämpfung von Straftaten öffentlich zugängliche Straßen, Wege und Plätze mittels Bildübertragung offen beobachten und Bildaufzeichnungen von Personen anfertigen, soweit an diesen Orten wiederholt Straftaten der Straßenkriminalität (sog. Schwerpunkt der Straßenkriminalität) begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung derartiger Straftaten zu rechnen ist (sog. offene präventive Videoüberwachung). Der HmbBfDI ist aufgrund von der Polizei Ham-

burg vorgelegten Fallzahlen und Lageanalyse zu dem Ergebnis gelangt, dass es sich bei dem überwachten Gebiet um einen solchen Schwerpunkt der Straßenkriminalität handelt d.h. um eine öffentlich zugängliche Örtlichkeit („Straßen, Wege und Platz"), die über einen längeren Zeitraum erheblich stärker von der sog. Straßenkriminalität belastet ist als das übrige Stadtgebiet. Sowohl die Art, Anzahl als auch Dichte der Straftaten qualifiziert das fragliche Gebiet zu einem Kriminalitätsschwerpunkt auf dem Gebiet der Freien und Hansestadt Hamburg. Der HmbBfDI hat sich im Rahmen der Vor-Ort Prüfung insbesondere konzentriert auf der Frage, ob die Polizei Hamburg die Videoüberwachung auch tatsächlich auf öffentlich zugängliche Orte i.S.d. Norm beschränkt hat. Die Regelung ermächtigt die Polizei nach der Rechtsprechung des Bundesverwaltungsgerichts (vgl. Urteil zur Videoüberwachung der Reeperbahn, Urteil vom 25.01.2012 – 6 C 9/11, Rn. 47) nämlich nicht zur Videoüberwachung von Gebäuden, Gebäudeteilen und Flächen, die zwar öffentlich zugänglich sind, aber nicht zu öffentlich zugänglichen Straßen, Wegen und Plätzen gehören. Durch das Überwachen von z.B. Eingangsbereichen ist der Übergang zum Privatbereich der gefilmten Personen betroffen. Auf diese Weise können ohne weiteres Bewegungs- und Besuchsprofile der Betroffenen erstellt werden (Urteil zur Videoüberwachung Reeperbahn: OVG Hamburg, Urteil v. 22. 6.2010 – 4 Bf 276/07, Rn. 136). Die daraus resultierenden wesentlich intensiveren Eingriffe wären dann nicht mehr von der Norm gedeckt. Es war daher vom HmbBfDI zu prüfen, ob die Polizei durch eine entsprechende Ausrichtung der Kamera oder eine technische „Verpixelung" sichergestellt hat, dass keine Hauseingänge und Fenster von Wohn- und Geschäftsgebäuden überwacht werden. Von einer ausreichenden Unkenntlichmachung konnte sich der HmbBfDI im Rahmen einer Vor-Ort-Prüfung am Polizeikommissariat 11 am Steindamm überzeugen. Zudem wurde stichprobenhaft untersucht, dass auch beim sog. Mitziehen der Kamera und beim Betätigen der Zoomfunktion die Unkenntlichmachung nicht umgangen werden kann. Dabei konnten keine Ausreißer oder Fehlprogrammierungen festgestellt werden.

Nachbesserungsbedarf sieht der HmbBfDI derzeit bei der Umset-

zung von technisch-organisatorischen Maßnahmen im Rahmen der Ausgestaltung der gesetzlichen Protokollierungspflicht. In weiteren Gesprächen mit der Polizei Hamburg soll ein Lösungsweg zu einem automatisierten, revisionssicheren Protokollierungsverfahren eingeschlagen werden.

3. Windows 10 und Updates in der FHH

Die von Microsoft bereitgestellten Konfigurationsmöglichkeiten beim Einsatz von Windows 10 Enterprise, die Übertragung von Telemetriedaten sicher zu unterbinden, reichen nicht aus. Zusatzmaßnahmen der Verantwortlichen sind daher erforderlich.

Die Datenschutzkonferenz positionierte sich Ende vergangenen Jahres in Form eines Prüfschemas zum Einsatz von Windows 10, indem Verantwortlichen, die Windows 10 bereits einsetzen oder dies beabsichtigen, in die Lage versetzt werden, eigenständig die Einhaltung der rechtlichen Vorgaben der DSGVO in ihrem konkreten Fall zu prüfen und zu dokumentieren (https://www.datenschutzkonferenz-online.de/media/dskb/20190403_positionierung_windows_10.pdf). Die datenschutzrechtlichen Fragestellungen rund um den Einsatz von Windows 10 beschäftigt alle Datenschutzaufsichtsbehörden weiterhin und die Beratungsbedarfe bestehen im Berichtszeitraum fort. Aus diesem Grunde hat eine Arbeitsgruppe der Datenschutzkonferenz weitere Untersuchungen von Windows 10 in Hinblick auf die Telemetriestufe Security durchgeführt (https://www.datenschutzkonferenz-online.de/media/dskb/TOP_30_Beschluss_Windows_10_mit_Anlagen.pdf). Im Ergebnis und als Konsequenzen für Verantwortliche kann festgehalten werden, dass zur Unterbindung der Übermittlung personenbezogener Telemetriedaten beim Einsatz der Enterprise-Edition die sog. Telemetriestufe Security genutzt werden kann und mittels vertraglicher, technischer oder organisatorischer Maßnahmen – beispielsweise durch eine Filterung der Inter-

netzugriffe von Windows 10-Systemen über eine entsprechende Infrastruktur – sicherzustellen ist, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfindet. Außerdem ist sich die Datenschutzkonferenz darüber einig, dass Windows 10 in allen angebotenen Editionen die Möglichkeit bieten sollte, die Telemetriedatenverarbeitung durch Konfiguration zu deaktivieren. Dazu und zu den Labor-Untersuchungen der DSK werden die Datenschutzaufsichtsbehörden das weitere Gespräch mit Microsoft führen.

Gleichzeitig gibt es auch in der FHH Neues zum Umgang mit Windows 10 zu berichten. Nachdem der HmbBfDI in den vergangenen zwei Jahren eine Prüfung der eingesetzten Windows 10 Versionen der städtischen Konfiguration durchführte, sicherte der Senat in seiner Stellungnahme zum 28.Tätigkeitsbericht Datenschutz zu, dass „die Prüfung zur Abschaltung ungewünschter Telemetriedaten und potentiell verbleibender Datenflüsse ein regelmäßiger Bestandteil der Prüfung vor dem jeweiligen Rollout" von Windows 10-Updates werde und seit dem Update auf die Version 1809 bereits entsprechend erfolge. Im Zuge des diesjährigen stadtweiten Updates auf die Version 1909 konnten die Senatskanzlei und Dataport keinen solchen Bericht vorweisen. Auf Nachfrage im August 2020 wurde dem HmbBfDI mitgeteilt, dass keine eigenen Telemetrie-Tests durchgeführt worden sind, da durch die Corona-Krise zusätzliche, zum Teil höchst priorisierte Aufgaben wie die Sicherstellung der VPN-Infrastruktur sämtliche Kapazitäten gebunden haben. Zudem fehlte im August noch dediziertes Personal in dem zuständigen Bereich bei Dataport. Bis zum Ende des Berichtszeitraums lagen dem HmbBfDI hierzu auf Nachfrage keinerlei weitere Informationen vor, wann die Besetzung und die damit verbundene Tätigkeitswahrnehmung umgesetzt werden. Vor dem Hintergrund, dass der Senat die dauerhafte Aufnahme einer Telemetrie- und Datenfluss-Prüfung zugesichert hat, ist die Entscheidung der Senatskanzlei, den Rollout-Prozess nicht bis zur Durchführung einer solchen Prüfung auszusetzen, problematisch. Gerade für solche kritischen Infrastrukturen sollte ausreichend Personal zur Verfügung stehen, um die rechtlichen Anforderungen durch technische und organisatorische Maßnahmen mit

ausreichender Sicherheit zu gewährleisten. Dazu gehört auch eine entsprechende Überprüfung vor der Produktivsetzung. Die Senatskanzlei teilte mit, dass die aktuelle Planung nunmehr den Beginn der Prüfungen ab Version 2009 umfasst.

Der HmbBfDI wird weiter mit den beteiligten Akteuren im Gespräch bleiben und sich für eine konsequente Überprüfung datenschutzrechtlicher Belange im Rollout-Prozess der FHH einsetzen.

4. Koordinierte Prüfung von Medienunternehmen

Im Rahmen einer koordinierten länderübergreifenden Prüfung beteiligt sich der HmbBfDI an der Webseitenanalyse und rechtlichen Bewertung der Online-Auftritte von Medienunternehmen.

Im Verbund mit insgesamt 11 deutschen Aufsichtsbehörden hat der HmbBfDI Mitte August die reichweitenstärksten Medienunternehmen in seinem Zuständigkeitsbereich angeschrieben und unter Zusendung eines umfangreichen abgestimmten Fragenkatalogs zur Stellungnahme hinsichtlich der Datenflüsse auf den betriebenen Webseiten aufgefordert. Schwerpunkt der Prüfung bilden das Webtracking und der Einsatz von Cookies und vergleichbarer Techniken.

Bereits im März 2019 hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) die Orientierungshilfe für Anbieter von Telemedien verabschiedet (https://www.datenschutzkonferenzonline.de/media/oh/20190405_oh_tmg.pdf). Danach kommt für die Einbindung von Drittdienstleistern auf der Webseite, insbesondere mit Hilfe von Cookies und andere Trackingmechanismen, die das Verhalten von Nutzern im Internet nachvollziehbar machen, sowie für das Erstellen von Nutzerprofilen regelmäßig nur die Einwilligung als Rechtsgrundlage im Sinne der DSGVO in Betracht. Vor einer solchen Verarbeitung, d.h. bevor Coo-

kies platziert oder auf dem Endgerät der Nutzer gespeicherte Informationen ausgelesen werden, ist daher eine informierte Einwilligung in Form einer Erklärung oder einer sonstigen eindeutig bestätigenden Handlung einzuholen.

Die bloße Weiternutzung des Angebots stellt keine Einwilligung in diesem Sinn dar. Dies haben die europäischen Aufsichtsbehörden in ihren Einwilligungs-Guidelines festgehalten (Guidelines 05/2020 on consent under Regulation 2016/679, Abschnitt 40, 41, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_de.pdf).

Diesen Anforderungen wird durch Online-Medien leider nicht immer entsprochen, was dazu führt, dass bei jedem Webseitenbesuch in die Grundrechte und Grundfreiheiten der Nutzer eingegriffen wird. Ferner ist nicht nur das massive Werbetracking von Nutzern zu beanstanden, sondern häufig auch die mangelnde Transparenz und fehlende Nachverfolgbarkeit der Datenweitergabe an die jeweiligen eingebundenen Werbedienstleister.

Beim HmbBfDI haben sich sämtliche Medienunternehmen mit der Beantwortung unseres Fragebogens zurückgemeldet. Die Auswertung und rechtliche Analyse dauert derzeit noch an und erfolgt wie bereits die Planung der Prüfung national koordiniert. Bei einer Branche, deren Produkte regelmäßig länderübergreifend genutzt werden, sollen möglichst konsistente und harmonisierte Entscheidungen von den beteiligten Aufsichtsbehörden ergehen.

5. Der Datenhunger vernetzter Geräte

Hersteller vernetzter Geräte nutzen deren Internetanbindung oftmals, ums sich darüber an den Daten der Gerätenutzer zu bedienen. Hier ist eine ausreichende Rechtsgrundlage und häufig mehr Transparenz und Einholen von Einwilligungen nötig.

Vielen Herstellern von mit dem Internet verbundenen Geräten (z.B. Musiksysteme, Haushaltsroboter, Video- oder Alarmsysteme) kann zu Recht attestiert werden, dass Sie das Beste ihrer Kunden im Sinn haben - die persönlichen Daten. Diese werden oft ohne deren Wissen und ohne ausreichende Transparenz für die Betroffenen gesammelt und von den Herstellern z.B. für die Erstellung von Profilen, zu Produktverbesserungen oder zu anderen Zwecken verwendet.

Bei Smartphones und Tablets haben sich Nutzer daran gewöhnt, dass die Betriebssysteme umfangreich Daten über den Geräteinhaber und sein Nutzungsverhalten an Server der Anbieter übermitteln. Auch im Bereich PCs und Notebooks wird dieses Konzept bei Windows etabliert (siehe III 3). Zudem werden die Nutzer immer stärker zur Verwendung von Cloud-Diensten angehalten, womit noch mehr persönliche Daten in die Hände der Softwareanbieter gelangen.

Bei vernetzten Geräten ist ein derartiger Datenhunger meist weniger im Bewusstsein der Nutzer. Dennoch sollten Gerätenutzer stets versuchen, möglichst viel Hoheit über ihre Systeme und die dort gespeicherten Daten zu behalten. Informationen zum sog. Selbstdatenschutz finden sich unter genau diesem Suchbegriff bei Suchmaschinen. Hilfreich ist auch z.B. die Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI): https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/empfehlungen_node.html

Auf welche praktischen Schwierigkeiten die Herstellung der Selbstbestimmung über die eigenen Daten stößt, zeigt der Markt der Elektrofahrzeuge. Die Fahrzeuge des Herstellers Tesla übermitteln nahezu jeglichen Bedienvorgang des Fahrers an Server des Herstellers. Den Besitzern und Fahrern wird der genaue Umfang oder der Zweck der Datenerhebung durch die Fahrzeuge kaum transparent dargestellt. Aber nicht nur die Fahrer werden überwacht - auch andere Fahrzeuglenker im Verkehr oder Passanten, die an einem parkenden Tesla vorbeilaufen, können ohne Ihr Wissen Opfer digitaler Erfassung werden. Eine Studie des „Netzwerk Datenschutzexpertise“ hat 2020 die Datenströme bei Tesla-Fahrzeugen näher betrachtet und

kam u.a. zu dem Ergebnis, dass die Funktion „Wächtermodus“, mit dem Tesla-Fahrzeuge Einbruchsversuche oder Parkrempler durch andere Fahrzeuge erkennen sollen, mit der europäischen Gesetzgebung nicht vereinbar ist. Wird bei einem parkenden Tesla der Wächtermodus aktiviert, erfasst das Fahrzeug über die an allen Seiten verbauten Kameras permanent und anlasslos die Umgebung, bei verdächtig eingestuften Vorgängen (z.B. jemand verweilt längere Zeit sehr nahe neben dem Fahrzeug) sendet es die aufgenommen Bilddaten zur Auswertung an Server des Herstellers in den USA. Die Studie kann hier heruntergeladen werden: https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020tesla.pdf

Doch nicht nur auf der Straße nimmt die Überwachung durch vernetzte Geräte zu, auch in den privaten Haushalten halten immer mehr potentielle Spione Einzug. Typischerweise erkennt man entsprechende Geräte an dem Verkaufsattribut „Smart Home“. Wir haben in vergangenen Tätigkeitsberichten bereits die Risiken von Smart-TV-Geräten (25. TB, V 17) oder digitalen Sprachassistenten (26. TB, III 6 und 28. TB, II 16) beleuchtet. Zunehmend verbreiten sich nun computergesteuerte Varianten klassischer Haushalts- oder Gartengeräte wie Saug- oder Rasenmähroboter, die ihren Besitzern Alltagsarbeiten abnehmen. Auch hier werden „smarte“ Modelle angeboten, die per App aus der Ferne bedient und kontrolliert werden können. Einige dieser Geräte legen im Zuge ihrer täglichen „Arbeit“ intern detaillierte Grundrisse der Wohnung oder des Grundstücks ihrer Besitzer an und übertragen diese über das Internet an den Hersteller. Man sollte daher überlegen, ob es wirklich nötig ist, diesen Geräten über das heimische WLAN Internetzugang zu gewähren. Schließlich öffnet man damit dem Hersteller und eventuellen Dritten eine nicht einsehbare digitale Zugangstür in die eigene Wohnung oder auf das eigene Grundstück.

Eine weitere Fortentwicklung eines klassischen Haushaltsgegenstands hat 2020 auch beim HmbBfDI für europaweites Tätigwerden gesorgt. Konkret handelte es sich um sog. vernetzte Lautsprecher. Im Gegensatz zu klassischen Lautsprechern, für die Kabel

quer durch die Wohnung gelegt werden müssen, erfolgt hier die Übertragung des Musiksignals per Funk. Damit wird auch das gleichzeitige Beschallen mehrerer Räume oder von Außenbereichen problemlos möglich, denn die Lautsprecher vernetzen sich über WLAN miteinander. Die Einrichtung und Konfiguration eines solchen Systems sowie die Steuerung der Musikwiedergabe, auf Wunsch direkt gefüttert von Streaming-Diensten aus dem Internet, erfolgt über eine App. Viele Systeme können auch mit Sprachassistenzdiensten wie Echo („Alexa") von Amazon oder Google Home verbunden werden.

Während einige Besitzer solcher Lautsprecher die smarten Anbindungsmöglichkeiten begrüßen, gibt es andere, die ihre Geräte bewusst nicht mit dem Internet verbinden wollen. Bei einem der führenden Gerätehersteller in diesem Bereich war dies lange Jahre kein Problem, denn die Systeme konnten auch ohne Internetzugang betrieben werden. Im Jahr 2017 jedoch hat das Unternehmen die Nutzungsbedingungen geändert. Seither lassen sich die Lautsprecher nur noch einrichten und nutzen, wenn in der Konfigurations-App eine überarbeitete Datenschutzerklärung akzeptiert und ein Nutzerkonto beim Hersteller angelegt wird. Ferner sollen die Gerätebesitzer einwilligen, dass regelmäßig Konfigurations- und Nutzungsdaten über das Internet an den Hersteller gesendet werden. Diese einseitige Änderung der Nutzungsbedingungen verärgerte vor allem Bestandskunden des Unternehmens, da sie nun ihre jahrelang frei nutzbaren Geräte nur noch weiterbetreiben können, wenn sie diese ans Internet anschließen und sich beim Hersteller registrieren. Entsprechend gingen bei den Datenschutzbehörden der EU mehrere Beschwerden ein, auch beim HmbBfDI.

Die Datenschutzbehörden mussten zunächst klären, welche Niederlassung des Herstellers die Hauptniederlassung in der EU ist, denn daraus ergibt sich die federführend zuständige nationale Aufsichtsbehörde. Die Aufgabe fiel der niederländischen Datenschutzbehörde zu, welche 2019 ein Anhörungsverfahren gegen den Hersteller eröffnet hat. Das Ergebnis daraus wurde im Dezember 2019 als sog.

Beschlussentwurf („Draft Decision“) den anderen EU-Aufsichtsbehörden zur Kenntnis gegeben. Gemäß Vorgabe von Art. 60 Abs. 4 DSGVO besteht dann vier Wochen lang die Möglichkeit, Einspruch einzulegen, andernfalls würde der Entwurf als Beschluss rechtskräftig werden.

Der Beschlussentwurf der niederländischen Datenschutzbehörde sah vor, die Forderung des Herstellers nach einem verpflichtenden Nutzerkonto beim Hersteller nicht zu beanstanden und das Verfahren einzustellen, da keine datenschutzrechtlichen Einwände bestünden. Unter anderem folgte man dem Vortrag des Unternehmens, dass nur auf Basis bekannter Kundenkonten nebenvertragliche Pflichten wie Gewährleistung von IT-Sicherheit erfüllt werden könnten. Gemäß Art. 6 Abs. 1 b DSGVO sei der Hersteller daher zu der Erhebung der betreffenden Nutzerdaten berechtigt.

Diese Einschätzung wird vom HmbBfDI sowie anderen Aufsichtsbehörden, vor allem aus Deutschland, nicht geteilt. In der Praxis liefern zahlreiche Hersteller von Computern, Smartphones oder anderen vernetzten Geräten den Beweis, dass die Gewährleistung von IT-Sicherheit und Updates auch erfüllt werden kann, ohne dass die Nutzer ein Konto beim Hersteller einrichten.

Wir haben daher Anfang 2020 Einspruch gegen den Beschlussentwurf eingelegt und im Februar 2020 mit den niederländischen Kollegen vereinbart, dass diese erneut die Sachverhaltsermittlung beim Hersteller aufnehmen. Hierzu wurden gemeinsam vertiefte Prüfungsfragen entwickelt. Aus der erneuten Befassung liegt aktuell noch keine neue Version des Beschlussentwurfes vor.

Wir werden den Vorgang weiter begleiten, denn die dem Fall zugrundeliegende Fragestellung hat grundsätzlichen Charakter: Es gilt zu klären, ob und in welchem Umfang ein Hersteller eines vernetzten oder smarten Gerätes auch nach dem Kauf noch Daten von den Kunden erheben darf und wenn ja, auf Basis welcher Rechtsgrundlage und in welchem Umfang.

6. Erstes Verfahren nach Artikel 65 DSGVO

Das erste Streitbeilegungsverfahren nach DSGVO führt im konkreten Einzelfall wie auch auf grundsätzlicher Ebene zu einem unbefriedigenden Ergebnis.

Der Europäische Datenschutzausschuss (EDSA) hat in einem ersten Fall seit Bestehen der DSGVO ein Streitbeilegungsverfahren nach Art. 65 DSGVO durchlaufen, dem ein Aufsichtsverfahren der irischen Datenschutzbehörde (IDPC) gegenüber der Twitter International Company zu Grunde lag. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit nahm für Deutschland als national federführende Aufsichtsbehörde eine koordinierende Rolle ein, da Twitter seinen Deutschlandsitz in Hamburg hat.

Der Streitbeilegung vorausgegangen war ein Verfahren nach Art. 60 DSGVO, in dem die IDPC als federführende Aufsichtsbehörde (LSA) den anderen betroffenen Aufsichtsbehörden in Europa (CSA) einen Beschlussentwurf vorgelegt hat, gegen den eine Reihe von Einsprüchen eingelegt wurden. Diesen hat sich die IDPC jedoch nicht angeschlossen und stattdessen das Kohärenzverfahren eingeleitet.

Die Ausgangslage bestand in der Meldung einer Schutzverletzung nach Art. 33 DSGVO durch die Twitter International Company (TIC) mit Sitz in Irland. Diese wurde nach Auffassung der IDPC nicht ordnungsgemäß, insbesondere nicht fristgerecht eingereicht. Die Schutzverletzung lag darin, dass aufgrund eines Programmfehlers als privat eingestellte Accounts ohne Zutun der Nutzer dennoch öffentlich zugänglich waren. Betroffen waren knapp 90.000 europäische Nutzer über einen mehrjährigen Zeitraum. In der Folge beschloss die IDPC als LSA für das Fristversäumnis der Art. 33-Meldung ein Bußgeld in niedriger sechsstelliger Höhe zu verhängen und legte einen entsprechen Beschlussentwurf vor.

Wir haben gegen diesen Beschlussentwurf mit Unterstützung anderer deutscher Aufsichtsbehörden Einspruch eingelegt und dabei im Wesentlichen folgende Aspekte thematisiert:

- Zunächst halten wir die Bewertung der Rollen der Twitter International Company als Verantwortliche und der Twitter Inc. (mit Sitz in den USA) als Auftragsverarbeiter für fragwürdig. Vieles spricht hier für eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO, was sich wiederum auf die gesamte Bewertung der Schutzverletzung niedergeschlagen hätte.
- Der Untersuchungsgegenstand wurde durch die IDPC unnötig verengt. Außer Verstößen gegen Art. 33 DSGVO kommen auch solche gegen Art. 5, 25 und 32 DSGVO in Betracht.
- Die Höhe des vorgeschlagenen Bußgelds halten wir für deutlich zu niedrig. Es handelt sich um einen erheblichen Verstoß und ein Unternehmen mit einem großen Jahresumsatz. Der vorgeschlagene Betrag erfüllt daher nicht die Anforderungen des Art. 84 DSGVO. Konkret wurde ein Alternativvorschlag auf Grundlage des Bußgeldkonzepts der DSK unterbreitet.

Insgesamt wurden Einsprüche durch acht CSA eingelegt, die teilweise überlappende Aspekte berührten, insgesamt aber ein breites Spektrum abdeckten. Den überwiegenden Teil der eingelegten Einsprüche wies die IDPC als unzulässig zurück, da sie das Kriterium „maßgeblich und begründet" nicht erfüllten. Den anderen Einsprüchen trat die IDPC inhaltlich entgegen und hielt an ihrem Beschlussentwurf vollständig fest. Für einen solchen Fall sieht Art. 65 DSGVO eine Befassung durch den EDSA vor, der schließlich mit einer Zweidrittel-Mehrheit eine für die LSA verbindliche Entscheidung erlässt.

Eine solche Entscheidung in diesem Fall ist nach einer Fristverlängerung Anfang November 2020 erfolgt. Dabei wurde die nach Art. 65 DSGVO festgeschriebene Zweidrittelmehrheit beim ersten Abstimmungsdurchgang knapp erreicht. Deutschland hat gegen die vorgeschlagene Entscheidung gestimmt. Diese Position wurde im Rahmen eines gemeinsamen Standpunkts nach § 18 BDSG vorab festgelegt. Unsere Ablehnung hatte folgende Hintergründe:

- Wesentliche Teile der Einsprüche aus Deutschland wurden auch vom EDSA als nicht „maßgeblich und begründet“ i.S.v. Art. 4 (24) DSGVO abgewiesen.
- Bei den verbleibenden Punkten in diesem Verfahren sah sich der EDSA nicht in der Lage, zu einer Entscheidung zu kommen. Dies lag im Wesentlichen daran, dass bereits die materielle Untersuchung des Falls durch die LSA erhebliche Lücken erkennen ließ. Das Plenum konnte sich nicht dazu durchringen, der LSA eine entsprechende Nachuntersuchung aufzugeben, um offene Fragen – etwa zu den Rollen der Unternehmen – zu klären.
- Vom EDSA-Plenum wurde lediglich der Aspekt der Bußgeldhöhe aufgegriffen. Hierbei wurde abstrakt auf die Einhaltung von Art. 84 DSGVO verwiesen, ohne der LSA konkretere Vorgaben zu machen. Das Plenum konnte sich zwar dazu durchringen, der LSA eine Erhöhung des Bußgelds aufzugeben, einen Rahmen hierfür legt der verbindliche Beschluss jedoch nicht fest.

Das Ergebnis ist in mehrfacher Hinsicht unbefriedigend. Zum einen wurde ein immenser Aufwand getrieben, um unter Beteiligung aller europäischen Aufsichtsbehörden zu einer verbindlichen Entscheidung zu kommen. Es waren dazu insgesamt sieben mehrstündige Sitzungen von unterschiedlichen Arbeitsgruppen des EDSA erforderlich, bevor in einer weiteren aufwändigen Sitzung des Plenums eine letztlich wenig gehaltvolle Entscheidung beschlossen wurde. Dies ist sehr ineffizient und sollte in dieser Form nicht wiederholt werden. Es ist zu erwarten, dass noch viele Verfahren nach Art. 65 folgen werden. Sie sind ein integraler und wichtiger Bestandteil des gemeinsamen und kohärenten europäischen Datenschutzvollzugs.

Zum anderen wurde durch diese Entscheidung eine nahezu vollständige Determinierung des Untersuchungsgegenstands durch die LSA festgeschrieben: Wenn die LSA eine dem Sacherhalt naheliegende Verletzung der DSGVO von vornherein nicht adressiert, besteht für die anderen CSA keine Gelegenheit, die Befassung mit diesen Aspekten im Rahmen des Kohärenzverfahrens einzufordern, nicht zuletzt aufgrund der engen Fristen nach Art. 65 DSGVO. Sie wären stets auf die Bereit-

schaft der LSA angewiesen, auf solche Wünsche schon im Rahmen der Zusammenarbeit nach Art. 60 DSGVO kooperativ einzugehen. Tut sie dies nicht oder verweigert die Kooperation insgesamt, bliebe der CSA so auch der Weg im Streitbeilegungsverfahren versperrt.

Das Plenum hat sich in diesem ersten Verfahren nach Art. 65 DSGVO unnötig um die Chance gebracht, zu wesentlichen Fragen der Auslegung und Anwendung der DSGVO Position zu beziehen. Das Ergebnis des Verfahrens widerspricht unserem Verständnis eines der zentralen Ziele der DSGVO, ein einheitliches Datenschutzniveau im gesamten europäischen Wirtschaftsraum zu schaffen. Dies kann nur gelingen, wenn die jeweiligen LSA und CSA kooperieren und die wesentlichen Aspekte von grenzüberschreitender Datenverarbeitung gemeinsam festlegen. Die LSA hat hierbei eine besondere, jedoch keineswegs allein bestimmende Rolle. Spätestens im Kohärenzverfahren müssten Alleingänge unterbunden und unzureichende Beschlussentwürfe der LSA durch den EDSA zurückgewiesen werden können. Es bleibt daher nur zu hoffen, dass die ausdrückliche Forderung des EDSA, schon im Kooperationsverfahren den Informationsaustausch zwischen der LSA und CSA so engmaschig und die Zusammenarbeit so konstruktiv wie möglich zu gestalten, künftig eingelöst wird.

Im Übrigen darf die Auslegung des Streitbeilegungsverfahrens nicht dazu führen, dass die federführende Behörde den Untersuchungsbereich von Verstößen gegen die DSGVO selbst bestimmen kann. Mit seiner Entscheidung im vorliegenden Verfahren entmachtet sich der EDSA selbst und gibt eine eigenständige Kontrolle der Entscheidung der federführenden Behörde aus der Hand. Ist dies der Maßstab, mit dem künftig Entscheidungen im Streitbeilegungsverfahren durch den EDSA überprüft werden, bleibt eine einheitliche Anwendung der DSGVO in der EU auf der Strecke. Es läge dann bei der federführenden Behörde, zusammenhängende Sachverhalte so zu verkürzen, dass es eigentlich keines gemeinsamen Verfahrens auf EU-Ebene mehr bedarf. Insoweit gilt es, die bisher in der Beschlussfassung des EDSA zum Ausdruck gekommene Auffassung für künftige Verfahren zu revidieren.

BERICHTE IV.

1. Digitale Souveränität, Entwicklungen in der FHH, GAIA-X

Digitale Souveränität gewinnt immer mehr an Bedeutung in politischen und wirtschaftlichen Entscheidungsprozessen. Es ist zu beobachten, dass bei Entscheidungsträgern langsam ein Umdenken einsetzt und Abhängigkeiten sowie die mit ihr verbundenen Risiken mit Blick u.a. auf Entscheidungen wie dem EuGH-Urteil zu Schrems II auch in der Praxis greifbar werden.

Viele Institutionen erkennen die Risiken, die aus Abhängigkeiten von externen Dienstleistern, proprietären Softwaresystemen und Cloud-Anwendungen erwachsen. Update-Zyklen von Software werden insbesondere durch die Hersteller von Betriebssystemen und weitverbreiteten Büro-Anwendungen vordiktiert. Die einzelnen Anwenderinnen und Anwender haben keinerlei Handhabe und müssen sich den Abhängigkeiten fügen. Implikationen wirtschaftlicher Art stellen dabei ebenso ein Risiko dar, wie IT-Sicherheits- und Datenschutz-Aspekte. Beispielsweise führt der Wechsel von on-premise - also selbstbetriebenen Software-Instanzen hin zu vermehrter Cloud-Nutzung dazu, dass Prozesse und Datenflüsse der Anwendungen für die firmeneigene IT und erst recht für den einzelnen Anwender intransparent und zum großen Teil nicht mehr überprüfbar werden. Vertragliche Garantien greifen unter Umständen nicht weit genug und stehen mit rechtlichen Anforderungen anderer Staaten im Konflikt. Um deshalb mehr Kontrolle über die eigenen Daten zu erlangen, findet auf mehreren Entscheidungsebenen ein Umdenken statt, das unter dem Schlagwort Digitaler Souveränität zusammengefasst werden kann.

Auf europäischer Ebene wird beispielsweise seit einem Jahr das Projekt GAIA-X mit Schirmherrschaft Frankreichs und Deutschlands vorangetrieben. Es soll ein architektonischer Standard für eine dezentrale und föderierte Infrastruktur entstehen, auf der die Verhaltensweisen unterschiedlicher Plattformen geregelt werden können. Großer Fokus liegt auf Daten und ihrer Echtzeitnutzung, der grundsätzlichen Verwendungsbestimmungen dieser und der Daten-

portabilität zwischen Plattformen. Kurz vor Redaktionsschluss des Tätigkeitsberichts wurde berichtet, dass Google, Amazon AWS und Palantir beim Start an GAIA-X beteiligt sein sollen. Sollte dies so zutreffen, bestünde die Befürchtung, dass GAIA-X keineswegs eine europäische souveräne Plattform, sondern abhängig von großen IT-Konzernen aus den Vereinigten Staaten sein könnte.

Die Fokusgruppe Digitale Souveränität des Bundesministeriums für Wirtschaft und Energie definiert den Begriff als Teilaspekt der allgemeinen Souveränität und umfasst die Selbstbestimmtheit im Digitalen. Erforderliche Bestandteile stellen dabei Vertrauenswürdigkeit der Kommunikation, Kontrolle über Datenflüsse und Möglichkeiten zu selbstbestimmter Handlung dar. Betroffene Personen können dann digital souverän auftreten, wenn Sie eine umfassende Digitalbildung mitbringen. Laut Einschätzung der Fokusgruppe zahlt sich der damit verbundene Kompetenzaufbau auch positiv auf die wirtschaftlichen, wissenschaftlichen und politischen Erfordernisse an Digitale Souveränität aus.

Auch in der Freien und Hansestadt Hamburg vereinbarte der seit 10. Juni 2020 amtierende rot-grüne Senat im Abschnitt „Digitale Souveränität des Staates stärken" des Koalitionsvertrages konkrete Maßnahmen, die in der Legislaturperiode vorangebracht werden sollen. Insbesondere sollten „unverhältnismäßige Abhängigkeiten von externen Berater*innen und Dienstleister*innen" vermieden werden. Als wesentlichen Faktor zur Transparenz und Offenheit der eingesetzten Technologien wird dabei der Einsatz von quelloffenen Software-Produkten angesehen, um Überprüfbarkeiten zu ermöglichen, die mit marktmächtigen Cloud-Anbietern nicht ohne erheblichen Aufwand leistbar ist.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit begrüßt ausdrücklich die geschilderten Absichtserklärungen und fordert den Senat auf, sich mit voller Kraft an den bestehenden Entwicklungen innerhalb der Stadt, beim städtischen IT-Dienstleister Dataport und in länderübergreifenden Arbeitskreisen aktiv zu

beteiligen. Dabei steht er mit seinen Referentinnen und Referenten stets beratend zur Verfügung und wird seine Expertise in den kommenden Projekten gern einbringen.

Konkrete Entwicklungen gibt es bereits zu verzeichnen. Dataport bietet mit dem Projekt Phoenix seit diesem Jahr eine Bürosoftware-Anwendung an, die vollständig auf Basis quelloffener Software-Komponenten betrieben wird und den Trägerländern Dataports für erste Tests und teilweise auch bereits produktiv zur Verfügung steht.

Laut Koalitionsvertrag soll als erstes die Bürgerschaftsverwaltung das Projekt Phoenix testen, sobald die Erfahrungen im Vorreiterland Schleswig-Holstein positiv verliefen.

2. Neue Maßnahmenbausteine des Standard-Datenschutzmodells Version 2.0b

Seit dem 6. November 2019 bietet das von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) veröffentlichte Standard-Datenschutzmodell (SDM) in Version 2.0 eine grundlegend überarbeitete Version, die die rechtlichen Anforderungen der DSGVO nun vollständig erfasst und mit Hilfe der Gewährleistungsziele systematisiert.

Seit Herbst 2020 wurde der zum SDM gehörende Referenzmaßnahmen-Katalog um vier neue Bausteine erweitert. Der Katalog kann herangezogen werden, um bei jeder einzelnen Verarbeitung zu prüfen, ob das rechtlich geforderte „Soll" von Maßnahmen mit dem vor Ort vorhandenen „Ist" von Maßnahmen übereinstimmt. Das SDM und der Referenzmaßnahmen-Katalog bieten zudem eine Grundlage für die Planung und Durchführung der von der DSGVO geförderten datenschutzspezifischen Zertifizierung (Art. 42 DSGVO) und der in bestimmten Fällen erforderlichen Datenschutz-Folgenabschätzung (Art. 35 DSGVO). Die rechtlichen Anforderungen der DSGVO über

die Gewährleistungsziele werden durch detaillierte Beschreibungen innerhalb des Referenzmaßnahmen-Katalogs umgesetzt und unterstützen somit die Transformation abstrakter rechtlicher Anforderungen in konkrete und direkt umsetzbare technische und organisatorische Maßnahmen.

Die Unterarbeitsgruppe SDM hat in den vier neuen Bausteinen des Katalogs die Themen „Aufbewahren", „Trennen", „Berichtigen" und „Einschränken der Verarbeitung" thematisiert und dem Arbeitskreis Technik zur Abstimmung überreicht. Seit diesem Jahr ist auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit in der UAG SDM aktiv eingebunden und übernimmt gemeinsam mit anderen Aufsichtsbehörden die weitere Ausarbeitung der Bausteine. Hierbei liegt der Fokus klar auf den Themen, die in der aufsichtsbehördlichen Praxis von übergreifender Relevanz sind und dadurch eine große Zahl von Verantwortlichen und umsetzenden Personen in ihrer täglichen Arbeit unterstützen werden.

Anwender in der Praxis sind dabei stets aufgerufen, Anmerkungen, Verbesserungsvorschläge und Kritiken mitzuteilen und somit zur Weiterentwicklung von Methoden und Maßnahmen beizutragen. Der HmbBfDI wird sich weiter dafür einsetzen, dass die Auslegung der DSGVO und damit verbunden die Forderung technischer und organisatorischer Maßnahmen an einem einheitlichen Standard orientiert sind. Die Unterarbeitsgruppe Standard-Datenschutzmodell trägt ihren Teil dazu bei.

3. Digitalisierung der Verwaltung - mit OZG, eIDAS, Servicekonto und Online-Ausweisfunktion

Einige datenschutzrechtliche Verbesserungen konnten verankert werden. Gleichzeitig enthält der Zugangsschutz zu den Servicekonten der FHH noch einen gravierenden Mangel.

Die Vorgaben für die Digitalisierung der Verwaltung sind im Onlinezugangsgesetz (OZG) kurz und bündig formuliert. Danach sind Bund und Länder verpflichtet, bis spätestens Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Dies bedeutet, dass bundesweit über 500 Verwaltungsleistungen einen digitalen Zugang erhalten müssen. Damit die Bürgerinnen und Bürger einen einfachen Zugang haben, wenn sie eine Dienstleistung in einem anderen Bundesland in Anspruch nehmen möchten, sind Bund und Länder auch verpflichtet, ihre Verwaltungsportale miteinander zu einem Portalverbund zu verknüpfen. Zur Vorbereitung und Koordinierung dieser anstehenden bundesweiten Digitalisierungsaufgabe hat der IT-Planungsrat die Projetgruppe „eID-Strategie" eingesetzt, in der der HmbBfDI seit längerem als Vertreter der Datenschutz-Aufsichtsbehörden insbesondere für die technisch-organisatorischen Fragen des Datenschutzes beratendes Mitglied ist.

Im Berichtszeitraum wurde die „Handreichung mit Empfehlungen für die Zuordnung von Vertrauensniveaus" fortgeschrieben. Ausgehend von der Sensibilität der in der Verwaltungsdienstleistung verarbeiteten Daten und den Gefährdungen und potentiellen Schäden wird in der Handreichung ein Vorgehensmodell beschriebenen, um Verwaltungsdienstleistungen zu den drei unterschiedlichen Vertrauensniveaus „niedrig", „substanziell" und „hoch" zuzuordnen. Diese drei Niveaus sind in der zugrundeliegenden eIDAS-Verordnung EU-weit vorgegeben. Mit diesen unterschiedlichen Niveaus werden in den Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) insbesondere spezifische Anforderungen und technische Verfahren für die Prozesse „Identifizierung" der Betroffenen sowie für die „Authentifizierung" der Betroffenen verbunden. Ein Beispiel: Mit einem Authentifizierungsverfahren, das alleine auf Benutzerkennung und Passwort basiert, kann man gemäß der einschlägigen Technischen Richtlinie TR-03107-1 des BSI nur das untere Vertrauensniveau erreichen. Obwohl dieses in der deutschen und englischen Fassung der eIDAS-Verordnung klar mit „niedrig" bzw. „low" benannt wird, wurde dieses Niveau

in der Handreichung wie auch in den technischen Richtlinien mit „normal" bezeichnet. Auch wenn die Angabe von Benutzerkennung und Passwort als alleinige Grundlage einer Authentifizierung sehr weit verbreitet ist, so zeigen doch auch die häufigen Berichte über den Missbrauch von Zugangsdaten und ein Eindringen in Web-Portale sehr drastisch auf, dass mit diesem Merkmalen nur das Niveau „niedrig" erreicht werden kann. Ein höheres Niveau kann nur durch eine sog. 2-Faktor-Authentifikation erfolgen. Dabei kommt beim Authentifizierungsprozess ein zweiter Faktor zum Einsatz, z.B. ein Softwarezertifikat oder für das Vertrauensniveau „hoch" ein Hardware-Faktor, etwa die Online-Ausweisfunktion des Personalausweises. Um den Betroffenen und den Verantwortlichen für die zu digitalisierenden Verwaltungsdienstleistungen das niedrige Vertrauensniveau von Benutzerkennung und Passwort transparent aufzuzeigen, hat sich der HmbBfDI dafür eingesetzt, die Begrifflichkeit aus der EU-Verordnung zu übernehmen. Das „Wording" und die Einbindung sicherer Authentisierungsmittel gehören zusammen. In der Handreichung ist dies auch so aufgegriffen worden. In den Technischen Richtlinien des BSI steht diese Fortschreibung leider immer noch aus, obwohl mit den TR-03160-1 und -2 zwei Richtlinien ebenfalls intensiv in der Projektgruppe eID-Strategie erörtert wurden.

In der TR-03160-1 des BSI sind auch Merkmale festgeschrieben, die mindestens in den Servicekonten gespeichert sein müssen, mit denen die Betroffenen über die Verwaltungsportale Zugang zu den digitalen Verwaltungsdienstleistungen erhalten können. Rechtliche Grundlage sind hier ebenfalls die eIDAS-Verordnung und das OZG. Gerade wenn das Mittel für das Authentifizierungsverfahren gewechselt wird, gilt es dabei sicherzustellen, dass sich mit einem Wechsel nicht unberechtigte Personen Zugang zu sensiblen personenbezogenen Daten verschaffen können. Der Entwurf der Technischen Richtlinie sah hier zunächst einen Prozess vor, bei dem nur ein Teil der verfügbaren Daten genutzt werden sollte. Gerade bei Personen, die in Großstädten wie Hamburg oder Berlin geboren sind, kann auf einem hohen Vertrauensniveau dann jedoch nicht

gewährleistet werden, dass allein der Geburtsname, das Geburtsdatum und der Geburtsort zu einer eindeutigen Zuordnung führen. Aus Sicht des HmbBfDI wurden zunächst auch nicht alle Vorgaben der eIDAS-Durchführungsbestimmungen in ausreichendem Maß berücksichtigt, wenn das Vertrauensniveau „hoch" erreicht werden soll, das insbesondere mit der Online-Ausweisfunktion des Personalausweises zur Verfügung steht. Da Personalausweise nur eine begrenzte Gültigkeit von regelhaft 10 Jahren haben, müssen sie zum Ablauf erneuert werden. Hier wurde der Vorschlag der Datenschutz-Aufsichtsbehörden aufgegriffen, mit dem nunmehr ein Wechsel des Personalausweises auch bei gleichzeitigem Namens- und Anschriftenwechsel in den allermeisten Fallkonstellationen sicher online erfolgen kann.

Diese bundesweit einheitlichen Anforderungen müssen im nächsten Schritt unter Beachtung der rechtlichen und technischen Vorgaben bei den Servicekonten der Länder und des Bundes umgesetzt werden. In Hamburg erfolgte dies im Wesentlichen mit dem Umstieg auf die Online-Service-Infrastruktur (OSI); eine Digitalisierungsplattform für die öffentliche Verwaltung. Dieses Serviceportal steht den Bürgerinnen und Bürger sowie Organisationen und Behörden zur Registrierung bzw. Anmeldung am eigenen Servicekonto zur Verfügung. Auch wenn OSI für „offen, sicher und innovativ" stehen soll, musste der HmbBfDI bei einer ersten Prüfung feststellen, dass die Anforderungen, die bei einem hohen Vertrauensniveau bestehen, derzeit noch nicht umgesetzt werden. So sind beispielsweise immer noch nicht alle Merkmale gespeichert, um die Anforderungen der eIDAS-Verordnung zu gewährleisten. Ein gravierender Mangel ist auch, dass ein bestehendes Servicekonto, das der Nutzer mit der Online-Ausweisfunktion seines Personalausweises auf das Vertrauensniveau „hoch" erweitert hat, allein mit Benutzerkennung und Passwort und der Online-Ausweisfunktion eines beliebigen anderen Personalausweises übernommen werden kann. Ein Beispiel: Eine unberechtigte Person meldet sich auf niedrigem Vertrauensniveau nur mit Benutzerkennung und Passwort an. Mit diesem ersten Schritt besteht noch kein Zugriff auf sensible Daten im Postfach, die ein

hohes Vertrauensniveau erfordern. Aber diese unberechtigte Person kann mit wenigen Klicks jeden beliebigen Personalausweis als Zugangsberechtigung auf dem Vertrauensniveau „hoch" für das bereits bestehende Servicekonto aktivieren und gegen den Ausweis des berechtigten Nutzers tauschen. Bei einem solchen Austausch des Personalausweises erfolgt derzeit kein Abgleich der Daten des alten und des neuen Personalausweises. Dies könnte dazu führen, dass sich eine unberechtigte Person mit diesem zweiten Schritt Zugriff auf sensible Inhalte verschafft, die im Postfach des Servicekontos gespeichert sind. Dieser Mangel beim Zugriffsschutz muss unverzüglich beseitigt werden, bevor mit der Pilotierung der Interoperabilität von Servicekonten begonnen wird, die bislang für das erste Quartal 2021 geplant ist.

4. Programmprüfung eines Zertifizierungsprogramms

Seit Geltungserlangung der DSGVO besteht die Möglichkeit für Unternehmen und Behörden, einen datenschutzrechtlichen Akkreditierungsprozess unter Beteiligung der Datenschutzaufsichtsbehörden zu durchlaufen. Das vorgelagerte Genehmigungsverfahren stellt dabei die Bewertung eines Zertifizierungsprogramms dar.

Zur Vorbereitung einer Akkreditierung muss die Zertifizierungsstelle oder der Programmeigner ein Zertifizierungsprogramm erstellen und durch die Deutsche Akkreditierungsstelle (DAkkS) gemäß DIN EN ISO/IEC 17011 auf Eignung prüfen lassen (vgl. DAkkS-Regel 71 SD 0016). Einen wesentlichen Teil des Zertifizierungsprogramms stellen dabei die Zertifizierungskriterien zur Umsetzung der datenschutzrechtlichen Anforderungen dar, die gemäß Art. 57 Abs. 1 lit. n DSGVO i.V.m. Art. 42 Abs. 5 DSGVO von der jeweils zuständigen Datenschutzaufsichtsbehörde genehmigt werden müssen (https://www.datenschutzkonferenz-online.

de/media/ah/20180828_ah_DIN17065-Ergaenzungen-full-V10-final_V3_DSK.pdf).

Dem HmbBfDI liegt als einer der ersten Datenschutzaufsichtsbehörden in Deutschland ein Antrag auf Prüfung für ein solches Zertifizierungsprogramm im Hinblick auf Produkte und Services nach der DSGVO zur Genehmigung vor. Im Rahmen des Verfahrens orientiert sich der HmbBfDI an gemeinsam erarbeiteten Kriterien der Aufsichtsbehörden des Bundes und der Länder, deren Veröffentlichung voraussichtlich Anfang des nächsten Jahres geplant ist. Das weit fortgeschrittene, aber noch nicht finalisierte Papier konkretisiert die Anforderungen der Aufsichtsbehörden an Zertifizierungsprogramme und soll insbesondere einen konsistenten Prüfmaßstab aller deutschen Aufsichtsbehörden gewährleisten.

Die vom Antragsteller eingereichten und sehr umfangreichen Unterlagen werden derzeit noch vom HmbBfDI geprüft. Sobald eine Genehmigung für das eingereichte Programm erfolgt ist, wird es möglich sein, dieses im Rahmen konkreter Zertifizierungen für spezifische Datenverarbeitungsvorgänge zu nutzen. So kann künftig sukzessive ein höherer Vertrauensstandard im Bereich des Datenschutzes begründet werden.

Wollen Antragsteller selbst als Zertifizierungsstellen auftreten und Zertifikate erteilen, müssen sie sich bei der DakkS ergänzend akkreditieren lassen. Die Akkreditierung erfolgt gemäß § 39 BDSG durch die Aufsichtsbehörden und die DakkS gemeinsam. Die Aufsichtsbehörden übernehmen dabei die Rolle der Fachbegutachtung als Spezialisten im Bereich datenschutzrechtlicher Akkreditierungsverfahren. Beim HmbBfDI haben mehrere Mitarbeiter und Mitarbeiterinnen eine Begutachterschulung durchlaufen und sind ausgebildet, zusammen mit den Systembegutachtern der DakkS die Befugnis zu erteilen, als Zertifizierungsstelle tätig zu werden.

In der Regel erfolgt die Befugniserteilung nach einer mehrtägigen Prüfung bei der Zertifizierungsstelle vor Ort. Dabei werden sowohl

die systematischen Anforderungen, wie bspw. das Vorhandensein von ausreichend qualifiziertem Personal oder die Gewährleistung von Objektivität, als auch datenschutzspezifische Anforderungen begutachtet. Sowohl das Akkreditierungsverfahren als auch das Verfahren zur Genehmigung der Zertifizierungskriterien sind mit einem erheblichen Prüfaufwand verbunden, für die seit dem 3. Dezember 2019 neue Gebührentatbestände mit der Datenschutzgebührenordnung vorliegen (https://datenschutz-hamburg.de/assets/pdf/ DSGebO.pdf).

5. Internationaler Datenverkehr nach Schrems II

Der Europäische Gerichtshof hat in seinem wegweisenden Urteil zu einer grundsätzlichen Kehrtwende bei der Praxis von Drittstaatentransfers aufgefordert. Zur Durchsetzung seiner Anforderungen koordiniert der HmbBfDI eine bundesweite Prüfaktion.

In seiner Entscheidung vom 6.7.2020 hat der Europäische Gerichtshof (EuGH) weit verbreitete Maßnahmen zur Datenübermittlung in Drittstaaten für nicht ausreichend erklärt. In die USA dürfen fortan keine personenbezogenen Daten mehr auf Grundlage des EU-US Privacy Shields versendet werden. Findet in Staaten außerhalb des EWR anlasslose behördliche Massenüberwachung statt, sind auch die Standardvertragsklauseln der Europäischen Union keine geeignete Basis mehr, solange ihre Schutzwirkung nicht durch individuell angemessene Zusatzmaßnahmen ergänzt wird. Das Urteil ist in seiner Zielrichtung sehr klar. Der Gerichtshof verdeutlicht, dass es kein „Weiter so" im internationalen Datenverkehr geben darf.

Zu der im Urteil offen gelassenen Frage, welche Zusatzmaßnahmen in Frage kommen, um weiterhin die Standardvertragsklauseln

zu nutzen, hat der Europäische Datenschutzausschuss die vielbeachteten Recommendations 01/2020 herausgegeben. Darin hat sich der Ausschuss gegen einen etwaigen risikobasierten Ansatz ausgesprochen. In Staaten mit umfassender geheimdienstlicher Massenüberwachung muss auch bei vermeintlich belanglosen Daten damit gerechnet werden, dass sie behördlich erhoben und mit anderen Informationen zu einem Gesamtprofil verkettet werden. Sollen persönliche Daten in solche Drittländer transferiert werden, ist es deshalb von großer Bedeutung, dass sie dort vollständig vor behördlichen Nutzung geschützt werden. In der Praxis kann dies zumeist nur durch Anonymisierung, wirksame Verschlüsselung sowie unter Umständen durch Pseudonymisierung gewährleistet werden. Viele bisherige Geschäftsmodelle sind damit nicht mehr ohne Änderung der technischen bzw. standortpolitischen Ausgestaltung möglich.

Die Rolle der Datenschutzbehörden hat der EuGH nachdrücklich verdeutlicht. Erhalten sie entsprechende Beschwerden betroffener Personen, so müssen sie alle nach den oben dargestellten Maßstäben unzulässigen Übermittlungen „aussetzen oder verbieten“. Für das zu erreichende Ziel bei der Beschwerdebearbeitung ist damit kein Spielraum eingeräumt. Die Art und Weise, wie eine Aussetzung der Übermittlung erzielt werden kann, liegt im Ermessen der jeweils zuständigen Behörde. In dem Wissen, dass ein Umstieg von jahrelang genutzten, in den Betriebsablauf integrierten Tools Verantwortliche im Einzelfall vor große Schwierigkeiten bringen kann, tritt der HmbBfDI mit Unternehmen, zu denen eine entsprechende Beschwerde vorliegt, zunächst in einen Dialog. Wenn in dem Zuge bereits begonnene Bemühungen aufgezeigt werden und überzeugende Konzepte zur Schaffung eines rechtmäßigen Zustandes vorgelegt werden, kann oftmals von Anordnungen auf dem Verordnungswege abgesehen werden. Die Frage, wieviel Zeit für den Wechsel eines Dienstleisters oder die Implementierung zusätzlicher Schutzmaßnahmen gewährt wird, hängt von den Umständen des Einzelfalls ab. Dafür kann es unter anderem von Bedeutung sein, ob ein Dienst beim Verantwortlichen bereits länger etabliert ist oder

erst nach der EuGH-Entscheidung eingeführt wurde. Relevant ist ferner, ob es sich um ein für den Fortbestand eines Unternehmens essenzielles System handelt und ob ein Wechsel auf alternative europäische Anbieter einfach möglich ist.

Um Marktverzerrungen zu vermeiden und um der Entscheidung des Gerichts breite Wirksamkeit zu verleihen, beschränkt der HmbBfDI sich nicht darauf, individuellen Beschwerden nachzugehen. Auf seine Initiative hin hat die Datenschutzkonferenz eine Task Force zur Durchführung einer länderübergreifenden Stichprobenaktion eingerichtet. Unter Leitung des HmbBfDI wurden gemeinsam Softwaredienste identifiziert, die in Deutschland verbreitet sind und typischerweise durch Einbindung externer Dienstleister aus Drittstaaten abgewickelt werden. Die teilnehmenden Behörden werden Anfang 2021 jeweils in ihrem Zuständigkeitsbereich an Stellen herantreten, bei denen Grund zur Annahme besteht, dass sie solche Dienste nutzen. Dies erfolgt unter Verwendung gemeinsam entwickelter Fragenkataloge und Schreiben. Auch die Behandlung der dabei ermittelten Verstöße soll abgestimmt erfolgen. Dabei wird jedoch die Einzigartigkeit jedes Falls individuell zu berücksichtigen sein.

6. 101 Beschwerden der Organisation NOYB

Im August wurden durch die Nichtregierungsorganisation NOYB 101 Beschwerden gegen in der EU und im EWR ansässige Unternehmen bei den jeweiligen Aufsichtsbehörden eingereicht. Zwei dieser Beschwerden fallen in den Zuständigkeitsbereich des HmbBfDI.

Gegenstand der Beschwerden ist der Datentransfer durch die verantwortlichen Unternehmen in die USA als sogenanntes Drittland, indem diese die Dienste Google Analytics oder Facebook Connect

auf ihren Webseiten einbinden und dadurch personenbezogene Daten in die USA übermitteln. Bis zur Entscheidung des EuGH vom 16.07.2020, C-311/18 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, Schrems II) konnten derartige Datentransfers auf das Privacy Shield gestützt werden. Mit dem o.g. Urteil, das die entsprechende Adäquanzentscheidung der EU-Kommission für ungültig erklärte, ist eine Übermittlung auf Grundlage des Privacy Shield nicht mehr möglich und daher einzustellen.

Das Privacy Shield wurde vom EuGH für ungültig erklärt, weil das US-Recht nach Auffassung des Gerichts kein Schutzniveau bietet, das dem in der EU im Wesentlichen gleichwertig ist. Das US-Recht, auf das der EuGH in seiner Entscheidung Bezug genommen hat, betrifft z. B. die nachrichtendienstlichen Erhebungsbefugnisse nach Section 702 FISA und Executive Order 12 333. (https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_ schrems2.pdf)

Zugleich hat der EuGH festgestellt, dass die Entscheidung 2010/87/EG der Kommission über Standardvertragsklauseln (Standard Contractual Clauses - SCC) grundsätzlich weiterhin gültig ist. Dabei betonte der EuGH die Verantwortung des Verantwortlichen und des Empfängers, zu bewerten, ob die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der Union genießen. Nur dann kann entschieden werden, ob die Garantien aus den Standardvertragsklauseln in der Praxis verwirklicht werden können bzw. welche zusätzlichen Maßnahmen zur Sicherstellung eines dem in der EU im Wesentlichen gleichwertigen Schutzniveaus ergriffen werden müssen. Zwar hat Google zwischenzeitlich öffentlich mitgeteilt, dass eine Umstellung von Privacy Shield auf Standardvertragsklauseln erfolgt, allerdings ist uns derzeit keine zusätzliche Maßnahme bekannt, die ein ausreichendes Datenschutzniveau bei der Drittlandübermittlung sicherstellen würde.

Da die 101 Beschwerden von NOYB die Zuständigkeit von Aufsichtsbehörden in vielen europäischen Staaten betreffen und aufgrund der Tatsache, dass die Beschwerden inhaltlich identisch sind, wurde durch den Europäischen Datenschutzausschuss (EDSA) eine Task Force eingerichtet. Sie soll die Aufsichtsbehörden dabei unterstützen, einen möglichst harmonisierten Ansatz für den gesamten Prozess der Beschwerdebearbeitung zu gewährleisten.

Unter Verwendung eines von der Task Force erarbeiteten und abgestimmten Fragenkatalogs wurden die in den Zuständigkeitsbereich des HmbBfDI verantwortlichen Unternehmen angeschrieben und zur Stellungnahme hinsichtlich des Drittlandtransfers von personenbezogener Daten aufgefordert. Eine Rückmeldung ist aufgrund der noch laufenden Stellungnahmefrist bisher nicht eingegangen.

7. Google Suchmaschine – neue Rechtsprechung des BGH

Suchergebnisse in der Google Suchmaschine sind häufig Gegenstand von Beschwerden von Betroffenen, wenn die Google LLC eine Auslistung abgelehnt hat. Im Rahmen seiner Zuständigkeit als Aufsichtsbehörde prüft der HmbBfDI, ob die Auslistung gegenüber der Google LLC anzuordnen ist.

Stellt eine betroffene Person gegen ein Suchergebnis zu ihrem Namen einen Antrag auf Auslistung bei der Google LLC und lehnt diese die Auslistung ab, so ist eine Beschwerde beim HmbBfDI hiergegen möglich. Der HmbBfDI prüft im Rahmen seiner Zuständigkeit (siehe hierzu auch IV. 8), ob die Voraussetzungen für einen Auslistungsanspruch vorliegen und hört, sofern er dies annimmt, die Google LLC zum Sachverhalt an. Nach erneuter Prüfung durch das Unternehmen werden Suchergebnisse in der Folge häufig blockiert. Wenn dies nicht erfolgt, prüft der HmbBfDI, ob die Aus-

listung gegenüber dem Unternehmen behördlich anzuordnen ist.

Der HmbBfDI berücksichtigt bei seiner Entscheidung die zum sog. Recht auf Vergessenwerden ergangene Rechtsprechung insbesondere des Europäischen Gerichtshofs (EuGH), des Bundesverfassungsgerichts (BVerfG) und des Bundesgerichtshofs (BGH) (siehe auch 28. TB IV. 5). Der BGH hat 2020 seine 2018 - vor Geltung der DSGVO - entwickelte Rechtsprechung aufgegeben. Danach musste ein Suchmaschinenbetreiber ein Suchergebnis erst dann auslisten, wenn er von einer offensichtlichen und auf den ersten Blick klar erkennbaren Rechtsverletzung der oder des Betroffenen Kenntnis erlangt. Vielmehr hat, so der BGH jetzt, eine gleichberechtigte Abwägung der Grundrechte der oder des Betroffenen mit denen des Inhalteanbieters, des Suchmaschinenbetreibers sowie der Nutzerinnen und Nutzer der Suchmaschine und der Öffentlichkeit zu erfolgen (VI ZR 405/18).

Zu weiteren Fragen rief der BGH im Rahmen eines Vorabentscheidungsverfahrens den EuGH an (VI ZR 476/18). Dieses betrifft zum einen die Frage, wie mit Tatsachenbehauptungen in Suchergebnissen umzugehen ist, deren Wahrheit die oder der Betroffene in Abrede stellt. Hier soll der EuGH klären, ob der Suchmaschinenbetreiber bei der Grundrechtsabwägung zu berücksichtigen hat, ob es für die oder den Betroffenen zumutbar wäre, zunächst gegen den Inhalteanbieter vorzugehen und die Unwahrheit der Behauptungen gerichtlich feststellen zu lassen. Eine weitere Vorlagefrage ist, ob bei der Abwägung, ob Fotos von Betroffenen als Vorschaubilder in der Suchmaschine angezeigt werden dürfen, auch der übrige Inhalt der Webseite mit zu berücksichtigen ist, auf der das Bild veröffentlicht ist.

Die Einschätzung des HmbBfDI zu Beschwerden gegen die Nichtlöschung von Suchergebnissen wurde in bisherigen Entscheidungen vom Verwaltungsgericht (VG) Hamburg und vom Hamburgischen Oberverwaltungsgericht (OVG) stets bestätigt. Derzeit sind sechs Klageverfahren vor dem VG Hamburg gegen den HmbBfDI

anhängig - davon drei aus 2020 - in denen die Kläger begehren, den HmbBfDI zu verpflichten, gegenüber der Google LLC die Entfernung von Suchergebnissen anzuordnen (Stand: 31.12.2020). Zwei der im Jahr 2019 erhobenen Klagen wurde von den Klägern zurückgenommen. In einer siebten anhängigen Klage begehrt der Kläger den Erlass von Anordnungen gegen Google mit Bezug auf (negative) Rezensionen in seinem bei Google angezeigten Unternehmensprofil. Einen gleichzeitig gestellten Antrag auf Erlass einer einstweiligen Verfügung gegen den HmbBfDI lehnte das VG Hamburg bereits mangels Eilbedürftigkeit ab.

8. Der Begriff der „Hauptniederlassung" – Unklarheit zu Lasten des Grundrechtsschutzes

Die Definition der „Hauptniederlassung" in der Datenschutz-Grundverordnung (DSGVO) bietet Spielraum für Interpretationen. Gleichermaßen fehlen in der Verordnung schlagkräftige Mechanismen, um unterschiedliche Rechtsansichten zwischen Aufsichtsbehörden sinnvoll aufzulösen. Um Rechtsschutzlücken zu vermeiden, muss der HmbBfDI seine Zuständigkeit neu definieren.

Die Hauptniederlassung eines Verantwortlichen wird in Art. 4 Nr. 16 a) DSGVO definiert. Demnach ist diese jene Niederlassung, welche die „Hauptverwaltung" des Verantwortlichen darstellt, es sei denn, die Zwecke und Mittel der Verarbeitung werden in einer anderen Niederlassung bestimmt. Was genau die „Hauptverwaltung" darstellt, wird im Gesetzestext nicht weiter erklärt. Es stellt sich daher die Frage, ob die Hauptverwaltung durch ein Unternehmen frei bestimmbar ist. Die einschlägige Kommentarliteratur erteilt dieser Vorstellung eine klare Absage. Notwendig für eine „Hauptverwaltung" sei zumindest, dass die Hauptniederlassung einen organisatorischen Geschäftsschwerpunkt bildet. Es dürfte damit

schwerfallen, regelmäßig wesentliche Managementstrukturen zwischen Mitgliedsstaaten zu verschieben, um sich die Aufsicht der jeweils günstigen Behörde zu sichern.

Der HmbBfDI musste sich seit Einführung der DSGVO mit der Frage der Hauptniederlassung beschäftigen. Einige große Technologie-Unternehmen wie z.B. Google haben zwar ihren deutschen Unternehmenssitz in Hamburg, jedoch häufig eine zentrale Verwaltung im europäischen Ausland. Aus diesem Grund ist es zur Bearbeitung vieler Beschwerden notwendig, dass die Zusammenarbeit mit anderen Aufsichtsbehörden nach den Verfahren der Art. 60ff. DSGVO durchgeführt wird. Die Zusammenarbeit mit der irischen Aufsichtsbehörde, der IDPC, hat dabei noch nicht den Zustand erreicht, der für eine reibungslose Kooperation wünschenswert wäre.

Im Zuge einer unternehmerischen Umstrukturierung Anfang 2019 hat Google die Verantwortlichkeit für Google-Dienste im europäischen Wirtschaftsraum – bis auf einige Ausnahmen – auf die Google Ireland Limited übertragen. Die von dieser Änderung ausgenommenen Bereiche, welche weiterhin von der Google LLC in den USA verwaltet werden, haben zu Schwierigkeiten in der Zusammenarbeit der Aufsichtsbehörden geführt. Bereits vor der Umstrukturierung hat die Google LLC die Google Ireland Limited zu ihrer Hauptniederlassung erklärt. Von dieser Arbeitshypothese ausgehend, hat der HmbBfDI stets die Zusammenarbeit mit der IDPC als federführende Aufsichtsbehörde gesucht.

Im Tätigkeitsberichts Datenschutz 2019 hat der HmbBfDI u.a. von Gerichtsverfahren vor dem Hamburgischen Oberverwaltungsgericht berichtet (s. 28. TB, IV. 5.). In diesen Verfahren ist das Gericht davon ausgegangen, dass viele Argumente für das Bestehen einer Hauptniederlassung in Irland bestehen – nicht zuletzt aufgrund des Vortrags von Google selbst.

Die IDPC hat eine Annahme entsprechender Beschwerde jedoch

seit den Strukturänderungen 2019 abgelehnt, mit dem Verweis, dass eine Zuständigkeit für Beschwerden gegen die Google LLC in Irland nicht bestehe. Auch andere europäische Aufsichtsbehörden sind diesem Weg gefolgt und haben den Status der Google Ireland Limited als Hauptniederlassung nicht anerkannt. Als Gründe hierfür wurde u.a. vorgetragen, dass die Google Ireland Limited die Zwecke und Mittel der Datenverarbeitung nicht ausreichend kontrolliere.

Eine einheitliche Ansicht darüber, welche Kriterien eine Niederlassung eines Verantwortlichen erfüllen muss, um als Hauptniederlassung zu gelten und ob dieser Zustand bei einem Unternehmen, welches derart zahlreiche Verarbeitungstätigkeiten durchführt, anhand von einzelnen, dedizierten Verarbeitungsvorgängen stets neu bewertet werden muss, konnte der HmbBfDI unter den europäischen Aufsichtsbehörden nicht feststellen. Gleichzeitig fehlen die Mechanismen in der DSGVO, solche Fragen anhand einzelner Beschwerden und einzelner Verantwortlicher verbindlich unter den Aufsichtsbehörden klären zu lassen. Der Europäische Datenschutzausschuss, als Gremium eigentlich geeignet für die Klärung von Grundsatzfragen, hatte in der Vergangenheit bereits die Bearbeitung von „Einzelfällen" abgelehnt.

Der HmbBfDI musste sich daher damit befassen, dass die für zuständig erachtete IDPC die Bearbeitung der Beschwerden mit Verweis auf ihre Unzuständigkeit abgelehnt hat. Hier besteht die Gefahr einer kritischen Rechtschutzlücke, wenn gegenüber Betroffenen alle Aufsichtsbehörden ihre eigene Zuständigkeit ablehnen und jeweils auf eine andere verweisen. Eine Klärung auf gerichtlicher Ebene könnte hier allenfalls durch Betroffene selbst erfolgen. Diese müssten zu allem Überfluss im europäischen Ausland die jeweiligen Aufsichtsbehörden zur Bearbeitung der Beschwerden verklagen – ein kostspieliges Unterfangen, welchem Einzelpersonen häufig machtlos gegenüberstehen.

Um eine sinnvolle Bearbeitung der strittigen Beschwerden zu ge-

währleisten, muss auch der HmbBfDI seine Haltung zu der Frage einer Hauptniederlassung überdenken. Es ist nicht im Sinne Betroffener, dass Beschwerden im Urwald der Zuständigkeiten untergehen. Es darf daher nicht die Situation eintreten, dass ein Unternehmen sich in den Machtbereich einer Aufsichtsbehörde zurückzieht, die jedoch jegliche Überwachungsverantwortlichkeit ablehnt. Unter diesen Gesichtspunkten wird der HmbBfDI davon ausgehen, dass er die Zuständigkeit, mangels Hauptniederlassung, innehat.

RECHTSVERBINDLICHE ANORDNUNGEN UND BUSSGELDER V.

1. Einleitung zum Themenbereich Anordnungen und Bußgelder

Der HmbBfDI hat der durch den Gesetzgeber angeordneten Änderung der Ahndungspraxis entsprochen. Im Berichtszeitraum wurde eine Bußgeldstelle geschaffen. Verstöße wurden vermehrt mit Bußgeldern geahndet.

Mit der Datenschutzgrundverordnung (DSGVO) hat der europäische Normgeber den Aufsichtsbehörden nicht nur starke Mittel an die Hand gegeben, Verstöße gegen datenschutzrechtliche Vorgaben zukünftig mit wirksamen Bußgeldern zu ahnden. Er hat durch die Gesamtkonstruktion der DSGVO auch deutlich gemacht, dass an Aufsichtsbehörden die Erwartung gestellt wird, dass Geldbußen nicht mehr die Ausnahme sind. Vielmehr soll Verstößen abgeholfen und diese geahndet werden, was auch durch Geldbußen erfolgen kann. Nach dem Wirksamwerden der DSGVO hat es noch einige Zeit gedauert, bis Verstöße, die zeitlich in den Anwendungsbereich der DSGVO fallen, beim HmbBfDI entscheidungsreif wurden. Inzwischen ist dies aber der Fall und hat die Arbeit des HmbBfDI grundlegend verändert. Zunächst hat die Tatsache, dass die Geldbuße ihren Ausnahmecharakter verlieren sollte, dazu geführt, dass beim HmbBfDI eine Bußgeldstelle eingerichtet werden musste, die für die Ahndung von Datenschutzverstößen durch Geldbußen zuständig ist. Haben die Fachreferate einen Fall abschließend aufgeklärt und halten sie die Verhängung einer Geldbuße für angezeigt, so erfolgt die Abgabe an die Bußgeldstelle (das Justiziariat), welches dann die erforderlichen Anhörungen durchführt und im Anschluss die Bußgelder verhängt.

Die Vorgabe zur Änderung der Arbeitsweise der Aufsichtsbehörden wurde vom HmbBfDI in der täglichen Arbeit umgesetzt und führte dazu, dass allein im Jahr 2020 25 Bußgeldverfahren eröffnet wurden. In 18 Fällen wurden bereits Bußgelder verhängt. Hinzu kommen Bußgelder in drei Verfahren, die bereits im Jahr 2019 eröffnet wurden. Nur zwei Verfahren wurden eingestellt, fünf weitere sind noch nicht abgeschlossen. Es ist daher festzustellen, dass die vom

Gesetzgeber erwartete und angeordnete Änderung der Ahndungspraxis vom HmbBfDI umgesetzt wurde.

Die Fälle, die den einzelnen OWi-Verfahren zugrunde liegen, spiegeln die Arbeit des HmbBfDI sehr gut wider. An einem Ende des Spektrums geht es um einfach gelagerte Fälle, die immer wieder auftauchen, wie zum Beispiel der nicht hinreichend datenschutzkonforme Umgang mit erhobenen Kontaktdaten in der Gastronomie nach der HmbSARS-CoV-2-EindämmungsVO oder die persönlich motivierte – und daher unzulässige – Abfrage von Daten aus polizeilichen Datenbanken durch Polizistinnen und Polizisten. Am anderen Ende der Skala stehen Einzelfälle, die massive Datenschutzverstöße von erheblichem Umfang zum Gegenstand haben und mit Bußgeldern in Millionenhöhe geahndet werden. Im Folgenden geben wir einen Überblick über einige berichtenswerte Fälle.

2. H&M

Im Fall der Überwachung von mehreren hundert Mitarbeiterinnen und Mitarbeitern des H&M Servicecenters in Nürnberg durch die Center-Leitung hat der HmbBfDI ein Bußgeld in Höhe von ca. 35,3 Mio. Euro gegen die H&M Hennes & Mauritz Online Shop A.B. & Co. KG wegen der Verletzung datenschutzrechtlicher Vorschriften erlassen. Die Entscheidung ist rechtskräftig.

Die H&M Hennes & Mauritz Online Shop A.B. & Co. KG mit Sitz in Hamburg betreibt ein Servicecenter in Nürnberg. Mindestens seit dem Jahr 2014 kam es bei einem Teil der Beschäftigten zu umfangreichen Erfassungen privater Lebensumstände. Entsprechende Notizen wurden auf einem Netzlaufwerk dauerhaft gespeichert. Nach Urlaubs- und Krankheitsabwesenheiten – auch kurzer Art – führten die vorgesetzten Teamleader einen sogenannten Welcome Back Talk durch. Nach diesen Gesprächen wurden in etlichen Fällen nicht nur konkrete Urlaubserlebnisse der Beschäftigten festgehal-

ten, sondern auch Krankheitssymptome und Diagnosen. Zusätzlich eigneten sich einige Vorgesetzte über Einzel- und Flurgespräche ein breites Wissen über das Privatleben ihrer Mitarbeitenden an, das von eher harmlosen Details bis zu familiären Problemen sowie religiösen Bekenntnissen reichte. Die Erkenntnisse wurden teilweise aufgezeichnet, digital gespeichert und waren mitunter für bis zu 50 weitere Führungskräfte im ganzen Haus lesbar. Die Aufzeichnungen wurden bisweilen mit einem hohen Detailgrad vorgenommen und im zeitlichen Verlauf fortgeschrieben. Die so erhobenen Daten wurden neben einer akribischen Auswertung der individuellen Arbeitsleistung u.a. genutzt, um ein Profil der Beschäftigten für Maßnahmen und Entscheidungen im Arbeitsverhältnis zu erhalten. Die Kombination aus der Ausforschung des Privatlebens und der laufenden Erfassung, welcher Tätigkeit sie jeweils nachgingen, führte zu einem besonders intensiven Eingriff in die Rechte der Betroffenen.

Bekannt wurde die Datenerhebung dadurch, dass die Notizen infolge eines Konfigurationsfehlers im Oktober 2019 für einige Stunden unternehmensweit zugreifbar waren. Nachdem der HmbBfDI über die Datensammlung durch Presseberichte informiert wurde, ordnete er zunächst an, den Inhalt des Netzlaufwerks vollständig „einzufrieren“ und verlangte dann die Herausgabe. Das Unternehmen kam dem nach und legte einen Datensatz von rund 60 Gigabyte zur Auswertung vor. Vernehmungen zahlreicher Zeuginnen und Zeugen bestätigten nach Analyse der Daten die dokumentierten Praktiken.

Die Aufdeckung der erheblichen Verstöße hat die Verantwortlichen zur Ergreifung verschiedener Abhilfemaßnahmen veranlasst. Dem HmbBfDI wurde ein umfassendes Konzept vorgelegt, wie von nun an am Standort Nürnberg Datenschutz umgesetzt werden soll. Zur Aufarbeitung der vergangenen Geschehnisse hat sich die Unternehmensleitung nicht nur ausdrücklich bei den Betroffenen entschuldigt. Sie folgte auch der Anregung, den Beschäftigten unbürokratisch einen Schadenersatz in beachtlicher Höhe auszuzahlen. Es handelte sich insoweit um ein bislang beispielloses Bekenntnis zur Unternehmensverantwortung nach einem Datenschutzverstoß.

Weitere Bausteine des neu eingeführten Datenschutzkonzepts sind unter anderem ein neu berufener Datenschutzkoordinator, monatliche Datenschutz-Statusupdates, ein verstärkt kommunizierter Whistleblower-Schutz sowie ein konsistentes Auskunfts-Konzept.

3. Clearview AI

Die U.S.-amerikanische Firma Clearview AI Inc. geriet Anfang des Jahres 2020 durch ihre Gesichtserkennungs-App weltweit in die Schlagzeilen. Eine Beschwerde gab dem HmbBfDI Anlass, ein Verwaltungsverfahren gegen die Verantwortliche zu eröffnen.

Anfang des Jahres 2020 wurde aus zahlreichen Medienberichten bekannt, dass die Clearview AI Inc. mit Sitz in New York in den letzten Jahren eine riesige Datenbank erstellt hat. Nach Medienberichten soll diese Milliarden von Fotos von Gesichtern enthalten. Mit ihrer Gesichtserkennungs-App bietet die Verantwortliche für angemeldete Nutzer eine Suchmaschine an, die bei Vorlage eines Gesichtsfotos alle so erschlossenen öffentlich verfügbaren Fotos dieser Person bzw. ihr biometrisch ähnelnder Personen anzeigt. Dies erfolgt jeweils einschließlich der Quellenangabe, etwa aus öffentlichen Profilen in sozialen Netzwerken oder von Bildern, die Unternehmensseiten entnommen wurden. Die Suchabfrage wird durch ein Hochladen eines Fotos in der App in Gang gesetzt und liefert mittels Abgleichs mit einem biometrischen Profil eine Trefferliste mit Fotos, die der hochgeladenen Vorlage am nächsten kommen. Daneben bietet Clearview AI auf ihrer Homepage den Betroffenen die Möglichkeit an, eine Auskunft über die sie betreffenden Daten einzuholen oder diese Daten aus der Unternehmensdatenbank löschen zu lassen. Dafür stellt sie entsprechende Formulare zur Verfügung.

Nicht nur die Medien ließen den HmbBfDI aufhorchen, ihn erreichte alsbald auch die Beschwerde eines Betroffenen. Dieser Beschwerde ging eine wie oben beschrieben eingeholte Auskunft an den Betroffenen voraus. Dieser fand in der Auskunft tatsächlich Fotos von sich und ande-

ren, dem Algorithmus ähnlich erscheinende Personen als Treffer zu seinem hochgeladenen Foto vor und wandte sich anschließend in der Annahme der Rechtswidrigkeit der Datenverarbeitung an den HmbBfDI.

Am 19.03.2020 verschickte der HmbBfDI sein erstes Schreiben an die Verantwortliche, das einen umfassenden Fragenkatalog enthielt. So wollte der HmbBfDI u.a. wissen, woher die Verantwortliche die Datenbestände entnimmt, zu welchem Zweck und ob die Betroffenen im Rahmen der Auskunft erfahren, welcher App-Nutzer sich über sie bereits erkundigt hatte. Die Verantwortliche reagierte auf dieses Schreiben zwar fristgemäß, allerdings ging sie kaum auf die Fragen des HmbBfDI ein. Sie beschrieb vage die Verarbeitungsvorgänge und verwies im Übrigen auf die angebliche Nichtanwendbarkeit der DSGVO. Dieser Auffassung tritt der HmbBfDI entschieden entgegen. Den räumlichen Anwendungsbereich der DSGVO sieht der HmbBfDI in diesem Fall über Art. 3 Abs. 2 b) DSGVO eröffnet und geht von einer eigenen Zuständigkeit aus. Art. 3 Abs. 2 b) DSGVO eröffnet einen weiten Anwendungsbereich. Der Wortlaut des Art. 3 Abs. 2 DGSVO verlangt lediglich den Zusammenhang einer Datenverarbeitung mit den genannten Umständen und schließt damit nachfolgende Datenverarbeitungen in die Betrachtung mit ein. Bei diesen handelt es sich um eine Beobachtung ihres Verhaltens, insofern die Nutzer der App erkennen können, in welchen privaten und beruflichen Zusammenhängen ein Betroffener mit Fotos in Erscheinung tritt, soweit dies in der Union erfolgt.

Für eine weite Auslegung spricht die Intention des Gesetzgebers, den hohen Schutz der Betroffenen in der Union vor Datenverarbeitung durch einen ausschließlich im Drittland ansässigen Verantwortlichen zu gewährleisten. Dieser Schutz ist hier angesichts der massenhaften, unterschiedslosen Datenverarbeitung durch Clearview und der faktischen Unmöglichkeit, die Betroffenenrechte in den USA gegenüber den App-Nutzern (U.S. amerikanische Strafverfolgungsbehörden, Unternehmen etc.) geltend zu machen, notwendig.

Zudem ist von der Rechtswidrigkeit der Datenverarbeitung für den weit überwiegenden Teil der unter die DSGVO fallenden Daten auszugehen.

Die biometrische Verarbeitung fällt unter den besonderen Schutz des Art. 9 DSGVO. Es wird hier regelmäßig an einer Einwilligung der Betroffenen in die Verarbeitung biometrischer Daten nach Art. 9 Abs. 1 DSGVO fehlen. Zwar mögen die Fotos der Betroffenen anfänglich offensichtlich öffentlich gemacht worden sein, wenn beispielsweise ein Profilbild aus einem sozialen Netzwerk bewusst öffentlich gestellt worden ist, so dass hier der Ausnahmetatbestand des Art. 9 Abs. 2 e) DSGVO in Betracht käme. Zu beachten wäre dann aber jedenfalls die nachträgliche biometrische Verarbeitung der Fotos für die Erstellung der Datenbank, die nur mit Einwilligung des Betroffenen stattfinden kann.

Auch das zweite Schreiben des HmbBfDI vom 26.05.2020 wurde nur ausweichend beantwortet, so dass er schließlich am 14.08.2020 einen Auskunftsheranziehungsbescheid erließ, der für die Nichtbereitstellung der erforderlichen Informationen ein Zwangsgeld i.H.v. 10.000 Euro pro Frage vorsah. Die Clearview AI Inc. ist inzwischen auf die Fragen hinreichend eingegangen. Der HmbBfDI prüft nunmehr weitere Schritte im Rahmen seiner Abhilfebefugnisse.

4. Videmo

Bereits im letzten Tätigkeitsbericht (28. TB 2019, Kapitel IV 3) hat der HmbBfDI über das Videmo-Verfahren berichtet. Hintergrund des Verfahrens ist der Einsatz einer Software zur automatisierten Gesichtserkennung anlässlich der Ermittlungen zu Ausschreitungen im Zusammenhang mit Protesten gegen den G20-Gipfel in Hamburg im Sommer 2017. Diese Software trägt den Namen Videmo. Für ihren Einsatz durch die Polizei Hamburg wurde eine Datenbank mit einem wachsenden Umfang von anfänglich 17 Terabyte angelegt, in die von Bürgerinnen und Bürgern bei der Polizei hochgeladene private Aufnahmen, polizeieigenes Videoüberwachungsmaterial sowie Material aus öffentlichen Verkehrsmitteln und aus den Medien – insgesamt ca. 32.000 Video- und Bilddateien (Stand August 2018) – eingeflossen sind.

Der HmbBfDI ist der Ansicht, dass für den Einsatz der Software keine hinreichende Rechtsgrundlage besteht und hat daher gegenüber der

Polizei die Löschung einer sog. Template-Datenbank, d.h. einer Datenbank, die sämtliche Gesichter des Videoüberwachungsmaterials in mathematische Modelle umgerechnet enthält, angeordnet. Die Löschungsanordnung bezog sich daher nicht auf das Videomaterial an sich, sondern auf die massenhafte biometrische Datenverarbeitung aller, zumeist völlig unbeteiligter, auf dem Videomaterial abgebildeten Personen. Die Polizei hat hiergegen Klage erhoben und war damit vor dem VG Hamburg erfolgreich.

Der HmbBfDI hat bereits im letzten Tätigkeitsbericht angekündigt, gegen diese Entscheidung Rechtsmittel einlegen zu wollen. Dies wurde auch umgesetzt. Der HmbBfDI hat fristgerecht die Zulassung der Berufung beantragt, die vom Verwaltungsgericht ausdrücklich ausgeschlossen wurde.

Zur Überraschung aller Verfahrensbeteiligten und auch der Öffentlichkeit kam die Polizei in der Zwischenzeit jedoch der Anordnung nach und löschte die Template-Datenbank. Dies geschah nach Angaben der Polizei aus Gründen der Erforderlichkeit: Es bestünde keine Notwendigkeit mehr für die Nutzung der Template-Datenbank. Zum einen ist es erfreulich, dass die Template-Datenbank gelöscht wurde und somit keine Eingriffe mehr in die Datenschutzrechte von tausenden unbescholtenen Bürgerinnen und Bürgern erfolgen, für die es nach Ansicht des HmbBfDI eindeutig an einer tauglichen Rechtsgrundlage fehlt. Zum anderen ist es aus Sicht der Rechtsklarheit jedoch problematisch, dass die Polizei den Rechtsstreit vorzeitig beenden will. Sie geht davon aus, dass die Zulassung der Berufung durch das OVG Hamburg nicht erfolgen dürfe und das erstinstanzliche Urteil damit unangreifbar würde. Damit wäre die gerichtliche Überprüfbarkeit der Anordnung durch das OVG nicht mehr möglich. Die grundsätzlichen Fragestellungen, die dieser Fall für die Praxis der Ermittlungsbehörden und für den Schutz massenhaft unbeteiligter Personen aufwirft, bliebe letztlich für die Zukunft offen.

Zum Bedauern des HmbBfDI kam es jedoch im Berichtszeitraum zu keiner Entscheidung des OVG Hamburg, obwohl das erstinstanzliche

Urteil bereits im November 2019 erging. Damit bleibt auch die prozessuale Frage der Zulassung der Berufung bislang unentschieden.

Diese Situation ist für alle Beteiligten unbefriedigend. Die Polizei hat ein erfolgreiches Urteil erstritten, von dem sie nicht weiß, ob es Bestand haben wird. Der HmbBfDI sieht sich mit Aussagen des Verwaltungsgerichts Hamburg konfrontiert, nachdem es ihm nicht erlaubt ist, bei einer hoheitlichen Datenverarbeitung zu kontrollieren, ob hierfür überhaupt eine Rechtsgrundlage existiert. Tausende Bürgerinnen und Bürger sind auch nach Jahren noch darüber im Unklaren, ob die Verarbeitung ihrer biometrischen Daten zu Recht erfolgte oder nicht. Der HmbBfDI hofft, im nächsten Tätigkeitsbericht über eine klärende Sachentscheidung berichten zu können.

5. Polizei-Abfragen: Übersicht der Verfahren

Im Berichtszeitraum hat der HmbBfDI insgesamt acht Ordnungswidrigkeitenverfahren (OWi-Verfahren) gegen Polizeibeamtinnen und Polizeibeamte abgeschlossen, die rechtswidrig Daten verarbeitet hatten.

In zwei Fällen hatten Polizeibeamtinnen bzw. Polizeibeamte Daten aus Anzeigen genutzt, um einen Kontakt zu der Anzeigeerstatterin herzustellen, der auf die Anbahnung einer privaten Beziehung gerichtet war. Diese Problematik ist aus anderen Bundesländern bekannt und im Übrigen nicht auf die Polizei beschränkt. Auch bei den Corona-Kontaktdaten kommt es bisweilen zu einem derartigen Fehlverhalten. Im Hinblick auf die Polizei besteht die Besonderheit, dass diese mit Hoheitsbefugnissen tätig wird und die Beschwerdeführerinnen sich deswegen in besonderem Maße belästigt fühlten. Der HmbBfDI hat dies jeweils mit Bußgeldern in Höhe von 300 bis 400 Euro geahndet. Es gab auch Fälle, in denen die Beschwerdeführerinnen zunächst mit der Kontaktaufnahme

einverstanden waren und sich erst dann über das Verhalten der Polizeibeamtinnen bzw. Polizeibeamten beschwerten, als die Beziehung nicht ihren Vorstellungen entsprach. In diesen Fällen haben wir von einer Verfolgung abgesehen.

In einem anderen Fall haben insgesamt drei Polizeibeamtinnen und Polizeibeamte von einer dienstlichen Präsentation, die personenbezogene Daten enthielt, Fotos angefertigt und diese in einer WhatsApp-Gruppe geteilt. Dies war unzulässig und der HmbBfDI hat hier ebenfalls Geldbußen in Höhe von 300 bis 400 Euro verhängt.

In drei weiteren Fällen haben Polizeibeamtinnen und Polizeibeamte zu unterschiedlichen privaten Zwecken Datenabfragen aus polizeilichen Datenbanken durchgeführt. Es ging dabei um Abfragen über Ex-Partnerinnen und Nachbarn. Die Fälle unterscheiden sich im Hinblick auf die Häufigkeit der Datenabfragen und wurden mit Geldbußen in Höhe von 400 bis 600 Euro geahndet.

Sämtliche dieser Fälle wurden von der Polizei dem HmbBfDI als zuständige Stelle zur Anzeige gebracht. U.a. gab es auch Anzeigen zur Einleitung eines OWi-Verfahrens im Hinblick auf sog. Eigenabfragen, also die Abfrage eigener Daten aus polizeilichen Datenbanken. Dies ist unzulässig und stellt einen Verstoß gegen Dienstvorschriften der Polizei dar, es handelt sich aber nicht um datenschutzrechtliche Verstöße. Der Geschädigte eines Datenschutzverstoßes kann mit dem Schädiger niemals identisch sein. Auch bei Verstößen im Rahmen eines dienstlichen Handelns besteht keine Möglichkeit der datenschutzrechtlichen Ahndung. Nimmt eine Polizeibeamtin oder ein Polizeibeamter Datenverarbeitungen zu dienstlichen Zwecken vor, zu denen er nicht befugt ist, handelt sie oder er nicht als Privatperson. Die DSGVO findet dann keine Anwendung, und für das Handeln von Behörden besteht gem. § 24 Abs. 3 HmbDSG nicht die Möglichkeit, Geldbußen gegenüber Behörden und öffentlichen Stellen zu verhängen. Dies bedeutet aber nicht, dass derartige Verstöße ungeahndet bleiben. Die Polizeibeamtinnen und Polizeibeamten können in diesem Fall im Rahmen von Disziplinarverfahren zur Verantwortung gezogen werden.

In allen Fällen haben die Polizeibeamtinnen und Polizeibeamten die Geldbußen akzeptiert und keinen Einspruch eingelegt. Im Anschluss an die OWi-Verfahren übersendet der HmbBfDI die Akten an die Disziplinarstelle der Polizei, die dann auf der Grundlage der Ermittlungen des HmbBfDI und der verhängten Geldbußen entscheidet, ob noch ein sog. disziplinarrechtlicher Überhang besteht. Sollte die Geldbuße aus dienst- und disziplinarrechtlicher Sicht das Geschehene nicht hinreichend sanktionieren, kann die Polizei im Anschluss an die Geldbuße noch eine Disziplinarmaßnahme verhängen, die zum Beispiel in einem Verweis, einer weiteren Geldbuße, einer Kürzung der Dienstbezüge, einer Zurückstufung oder im schlimmsten Fall sogar zu einer Entfernung aus dem Beamtenverhältnis führen kann.

6. Aktenlagerung eines Klinikums in Büren – Patientendatenschutz mit erheblichen Lücken

Die Lagerung von Patientenakten in einem ehemaligen Krankenhaus stellt nach Ansicht der hamburgischen Gerichtsbarkeit keine Datenverarbeitung dar. Dies hat den HmbBfDI daran gehindert, wirksame Schutzmaßnahmen für ein umfassendes Aktenarchiv durchzusetzen. Es ist ungewiss, wie diese Rechtsschutzlücke zu schließen ist.

Eine Krankenhausträgergesellschaft in Büren (NRW) meldete im April 2010 Insolvenz an, im Oktober desselben Jahres wurde der Klinikbetrieb eingestellt. Der Insolvenzverwalter gab die Krankenhausimmobilie im Jahr 2011 an eine Grundstücksgesellschaft zurück, die eine 100%ige Tochter des Krankenhauskonzerns ist, welcher auch die Krankenhausträgergesellschaft in Büren gehörte. Nach Einstellung des Klinikbetriebs verblieben die in Papierform geführten Behandlungsdokumentationen (Patientenakten) in zwei auch ursprünglich zur Unterbringung der Akten vorgesehenen Kellerräumen. Das Krankenhausgebäude stand in der Folgezeit leer und wurde zeitweise

durch unterschiedliche Hausmeister betreut.

Im Mai 2020 betrat ein Youtuber das ehemalige Krankenhausgebäude einschließlich der beiden im Keller befindlichen Aktenräume, wobei er auf die zurückgelassenen Patientenakten stieß. Das hierüber veröffentliche Video sorgte für ein breites mediales Echo sowie für datenschutzrechtliche Beschwerden ehemaliger Patienten. Der HmbBfDI hat umgehend versucht, das in Hamburg ansässige Mutterunternehmen zu veranlassen, die Patientenakten angemessen zu sichern. Dies scheiterte nicht zuletzt an einer Verweigerungshaltung des Klinikkonzerns. Dieser antwortete lediglich mit dem Hinweis auf die aus seiner Sicht fehlende örtliche Zuständigkeit des HmbBfDI.

In der Folge hat der HmbBfDI eine Anordnung erlassen, mit der der Grundstücksgesellschaft aufgegeben wurde, die Unterlagen angemessen zu sichern und die Erfüllung datenschutzrechtlicher Auskunftsansprüche sicherzustellen. Die Anordnung wurde für sofort vollziehbar erklärt, wogegen die Grundstücksgesellschaft Rechtsschutz beim VG Hamburg suchte.

Das Gericht hat dem Antrag mit Beschluss vom 30.7.2020 (17 E 2756/20) stattgegeben. Zur Begründung führte es im Wesentlichen aus, dass der Ausdruck „Verarbeitung“ nach der in Art. 4 Ziffer 2 DSGVO enthaltenen Begriffsbestimmung jeden Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten bezeichne wie das Erheben, das Erfassen, die Speicherung usw. Das bloße Vorhandensein der Aktenbestände in dem Gebäudekomplex unterfalle nicht den Anforderungen an den Begriff der Datenverarbeitung. Der Begriff des „Vorgangs“ zeige an, dass Verarbeitung nicht einen Zustand, sondern eine Handlung, also die Veränderung eines Zustands, beschreibe. Eine Verarbeitung erfordere damit die Überführung eines Zustands in einen anderen Zustand.

Der HmbBfDI hält diese Rechtsauffassung für problematisch. Sie entzieht die personenbezogenen Daten in Form von Patientenakten dem Datenschutzrecht, weil der bisherige Verarbeiter in Insolvenz ging.

Dies führt in der Folge zu einem Zustand der datenschutzrechtlichen Verantwortungslosigkeit in der Hinsicht, dass kein Verantwortlicher mehr existiert und Anfragen ehemaliger Patienten ins Leere laufen. Sie müssen schlicht nicht mehr beantwortet werden.
Da das VG Hamburg mit dieser Rechtsauffassung juristisches Neuland beschritten hat, legte der HmbBfDI Beschwerde zum OVG Hamburg ein. Mit Beschluss vom 15.10.2020 (5 Bs 152/20) hat das OVG Hamburg jedoch die Auffassung des Verwaltungsgerichts bestätigt. Der Beschluss enthält keine nennenswerten eigenen Erwägungen, sondern schließt sich den Ausführungen des VG Hamburg an.

Auch wenn diese Rechtsauffassung aus Sicht des HmbBfDI bedauerlich ist und nur schwer zu rechtfertigende Schutzlücken für das Grundrecht auf Datenschutz reißt, war einzusehen, dass der HmbBfDI sich mit seiner Gegenansicht nicht durchsetzen konnte, da eine weitere Beschwerde gesetzlich nicht vorgesehen ist. Der HmbBfDI hat daher die Anordnung aufgehoben und der Stadt Büren mitgeteilt, dass man gerichtlich daran gehindert sei, datenschutzrechtliche Anforderungen durchzusetzen.

Die Entscheidungen der hamburgischen Verwaltungsgerichtsbarkeit wurden in der juristischen Fachpresse kritisch besprochen. Es bleibt abzuwarten, ob sich diese Auffassung durchsetzen wird. Für den Schutz der personenbezogenen Daten und die Rechte von Patienten wäre dies jedenfalls ein nicht unerheblicher Rückschritt.

7. Rechtswidrige Videoüberwachung von Beschäftigten

Eine verdachtsunabhängige Videoüberwachung von Beschäftigten ist unzulässig. Der HmbBfDI sanktioniert solche Verstöße mit dem Mittel der Geldbuße. Die Bemessung der Geldbuße bemisst sich am Grundsatz der Verhältnismäßigkeit. In einem Fall wurden die besonderen Umstände der Corona-Pandemie berücksichtigt.

Ein Unternehmen betreibt mehrere Restaurants in Hamburg. In einer dieser Filialen waren sechs Videoüberwachungskameras installiert und in Betrieb. Die Kamerabilder wurden in Echtzeit aufgezeichnet und für 72 Stunden gespeichert. Als Zweck gab die Geschäftsführung die Verhinderung von Diebstählen an. Nach den Feststellungen des HmbBfDI diente die Hälfte der Kameras vor allem der Überwachung der Beschäftigten. Dies geschah in einem unzulässigen Ausmaß.

Diese drei Kameras haben während der Geschäftszeiten den vorderen Verkaufsbereich gefilmt sowie Küche und Kühllager der Filiale. Das Kühllager wurde nur teilweise aufgezeichnet. Etwaige Diebstähle hätten mit der dokumentierten Kameraeinstellung kaum aufgeklärt werden können. Festgehalten wurde lediglich, wer wann den Kühlraum betreten hat. Schon die Eignung dieser Dokumentation zur Aufklärung oder Verhinderung von Eigentumsdelikten erscheint deshalb fraglich, da aus einem Kühllager während des Betriebs ständig Waren entnommen werden müssen. Vor allem aber ist es seit der Übernahme der Filiale durch das Unternehmen zu keinerlei Warendiebstählen gekommen. Die Aufzeichnung erfolgte vielmehr präventiv. Von ihr mag eine gewisse Abschreckungswirkung ausgegangen sein. Jedoch war zu berücksichtigen, dass nicht allein das Kühllager, sondern daneben weitere Betriebsbereiche aufgezeichnet wurden, in denen sich Beschäftigte dauerhaft aufhielten. Der mit der Aufzeichnung verbundene Eingriff in die Rechte der Beschäftigten war erheblich. Dies gilt in noch stärkerem Maße für die anderen beiden Kameras, welche die Küche und den Verkaufsbereich aufzeichneten. Hier war schlicht nicht ersichtlich, welchem legitimen Zweck die Aufzeichnung dienen soll. Gefilmt wurde der Küchenbereich, in dem sich unter gewöhnlichen Umständen ausschließlich Beschäftigte aufhalten. Diese wurden lückenlos bei ihrer täglichen Arbeit aufgezeichnet, ohne dass irgendein Anlass hierzu bestand. Weder sind seitens des Unternehmens regelmäßige Verfehlungen von Beschäftigten vorgetragen worden noch bestanden Anhaltspunkte für sonstige schutzwürdige Belange. Die Beschäftigten wurden in der Küche und im Bereich der Vorbereitung kalter

Speisen dauerüberwacht, ohne sich der Videoaufzeichnung wenigstens teilweise entziehen zu können. Nach der Rechtsprechung des Bundesarbeitsgerichts ist eine dauerhafte, verdachtsunabhängige Videoüberwachung von Beschäftigten unverhältnismäßig und damit unzulässig (BAG, Beschl. v. 29.6.2004 – 1 ABR 21/03, Rn. 23, BAG, Urt. v. 28.3.2019 – 8 AZR 421/17, Rn. 39). Durch die Videoüberwachung wurde in schwerwiegender Weise in das allgemeine Persönlichkeitsrecht der Arbeitnehmer eingegriffen. Diese wurden einem ständigen Überwachungsdruck ausgesetzt.

Für den HmbBfDI erschien die Verhängung eines Bußgelds deswegen unausweichlich. Allerdings war bei der Berechnung der Geldbuße nicht nur zu berücksichtigen, dass sich das Unternehmen kooperativ gezeigt hatte. Hinzu kam, dass sich durch die Corona-Pandemie die Umsätze des Unternehmens fast halbiert hatten und für das Geschäftsjahr ein negatives Ergebnis erwartet wurde. Unter diesen Umständen war das Bußgeld moderat zu berechnen. Die Verhängung des Bußgeldes sollte nicht zuletzt dem Schutz der Beschäftigten dienen. Es wäre nicht in deren Interesse gewesen, ein Bußgeld zu verhängen, das für das Unternehmen das Risiko der Insolvenz mit sich gebracht hätte. Der HmbBfDI hat sich daher für ein Bußgeld in Höhe von 3.000,- Euro entschieden. Dies wurde vom Unternehmen akzeptiert.

8. Ortsinformationen in Bildern eines Fetisch-Portals

Wird online auf der Webseite eine Foto-upload-Funktion bereitgestellt, müssen die Metadaten wie z.B. GPS-Daten bereinigt werden. Andernfalls könnten in einem sensiblen Kontext diese Metadaten von unbefugten Dritten mit Schädigungsabsicht genutzt werden.

Der HmbBfDI hat einen Bußgeldbescheid gegen ein Unternehmen

erlassen, das einen Online-Marktplatz insbesondere für getragene Unterwäsche betreibt. Der Shop richtet sich an Kunden, die ein Interesse daran haben, unterschiedlich lange getragene Unterwäsche mit entsprechend intensivem Eigengeruch zu erwerben. Das Unternehmen wirbt damit, hundertprozentige Anonymität zu gewährleisten.

Anlass für die Eröffnung des Bußgeldverfahrens war ein Hinweis eines besorgten Bürgers, welcher dem HmbBfDI zahlreiche GPS-Koordinaten von Nutzerinnen der Plattform zur Verfügung stellte.

Eine Überprüfung hat ergeben, dass die Restinformationen bzw. Metadaten bei den hochgeladenen Fotos nicht bereinigt worden waren. Folglich konnten die Daten bei beliebigen Kartendiensten eingegeben und der genaue Standort ermittelt werden, an dem das Foto erstellt wurde. Teilweise waren zusätzlich Höheninformationen in den Bildern vermerkt, die eine grobe Aussage über das im Aufnahmemoment bewohnte Stockwerk ermöglichten.

Die Zahl der betroffenen Personen belief sich im Kontrollzeitraum auf ca. 760 Frauen zwischen 18 und 50 Jahren. Auf den Amateuraufnahmen werden die Betroffenen in Unterwäsche abgebildet. Bei einigen Fotos ist auch das Gesicht erkennbar.

Der Verantwortliche ist verpflichtet, den Nachweis erbringen zu können, dass er am Risiko gemessene geeignete technische und organisatorische Maßnahmen zum Schutz vor Datenschutzverletzungen ergriffen hat (Art. 24 und 32 DSGVO). Daneben verlangt Art. 25 DSGVO dem Datenschutz durch datenschutzfreundliche Technikgestaltung („privacy by design“) und Voreinstellungen („privacy by default“) Rechnung zu tragen. Maßstab für das angemessene Schutzniveau der zu ergreifenden Maßnahmen ist neben der Sensibilität der Verarbeitung auch der Stand der Technik.

Eine Upload-Funktion für Bilder gehört seit Jahren zum Standard aktueller Web-Technologien. Bei der Plattform besteht der Dienst

konkret darin, dass angemeldete Nutzer Fotos von Unterwäsche u.ä. hochladen können. Zumeist wurden zur Aufnahme der Fotos Smartphones bzw. andere mobile Endgeräte oder Digitalkameras genutzt. Dabei ist es häufig eine Standardeinstellung, dass die Kamera-Apps der Smartphones bzw. GPS-Module der Kameras neben dem eigentlichen Bild auch zusätzliche Informationen in die Bilddatei speichert, die sog. Exchangeable Image File Format (EXIF-Daten). Mittels dieser EXIF-Daten ist eine ziemlich genaue Lokalisierung möglich, womit ein hohes Sicherheits- und Vertraulichkeitsrisiko einhergehen kann. Diese Art von Informationen wird seit der Erstveröffentlichung dieses Standards im Jahre 1995 in immer mehr Geräten mit optischen Sensoren eingesetzt und ist heutzutage de facto in sämtlichen Smartphones und Tablets mit Kamera und digitalen Kamerasystemen zu finden. Inhalt dieser EXIF-Daten können verschiedene Metadaten, darunter auch die GPS-Daten (Standortinformationen) in der Bilddatei, sein.

Als Konkretisierung des Standes der Technik für den Bereich der Datensicherheit stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das IT-Grundschutzkompendium bereit. Dort werden allgemeine „Standard-Anforderungen" festgehalten, die dem Stand der Technik entsprechen. Auch das Bereinigen von EXIF-Daten als Restinformationen bei einem Foto-Upload gehört nach den Feststellungen des BSI und zur Überzeugung des HmbBfDI zu solchen Standard-Anforderungen bei Onlineshop-Plattformen, die ein Foto-Upload zur Verfügung stellen. Demnach müssen sämtliche hochgeladene Bilder vollständig von ihren Metadaten befreit werden, bevor die Bilder dem eigentlichen Dienst zur Verfügung stehen und öffentlich einsehbar werden.

Bei diesen GPS-Daten handelte es sich teilweise um personenbezogene Daten im Sinne des Art. 4 Nr. 1 Alt. 2 DSGVO. Für den Personenbezug einer Information reicht es danach aus, wenn die betroffene Person identifizierbar ist, wenn also durch eine Anzahl von weiteren Verarbeitungsschritten oder durch Zusatzwissen zwischen der Information und der Person eine Beziehung hergestellt werden kann. Bei

der großen Anzahl von nicht bereinigten Fotos mit Standortdaten war im Rahmen einer Stichprobe eine Identifizierbarkeit mehrerer Betroffener mit verhältnismäßig geringem Aufwand möglich. Die Eingabe der Koordinaten und eine zusätzliche Recherche über Suchmaschinen ermöglichte eine Identifizierung der betroffenen Person. In einem Fall konnten neben der Wohnanschrift sogar weitere Informationen wie die Handynummer erschlossen werden.

Allein wegen der kontextuell sexuellen Ausrichtung der Plattform waren hohe Risiken durch mögliche Nachstellungen oder Diskriminierungen zu bedenken, die zu physischen – etwa durch zu befürchtende Gewaltstraftaten – aber auch zu materiellen (Kündigungen) oder immateriellen Schäden (Rufschädigung, Diskriminierungen) hätten führen können. Letzteres war zu befürchten, wenn z.B. öffentlich bekannt gemacht würde, dass eine betroffene Person durch Angabe der Anschrift und ggf. des Namens, ihre wochenlang getragene und damit entsprechend stark riechende Unterwäsche auf einer Plattform zum Verkauf angeboten hat.

Schließlich wurden die Daten unberechtigt übermittelt bzw. offengelegt, was zudem einen Verstoß gegen Art. 6 Abs. 1 i.V.m. Art. 5 Abs. 1 lit. a) DSGVO darstellt. Die Offenlegung stellt eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar, für welche es einer konkreten Rechtsgrundlage bedurfte. Maßgebend für eine Offenlegung an einen Dritten ist die Bekanntgabe, welche bei einem Bildupload im Internet der Fall ist, wenn ein Dritter diese Daten tatsächlich abruft. Vorliegend hat ein Abruf zahlreicher GPS-Daten zumindest durch den Hinweisgeber selbst stattgefunden. Ursache des geschilderten Umgangs mit Metadaten war ein fehlkonfiguriertes Add-On des eingesetzten Content-Management-Systems.

Der Mangel wurde behoben, sodass nunmehr die Metadaten systemseitig automatisiert bereinigt werden. Der HmbBfDI hat ein mit Blick auf den geringen Umsatz des Unternehmens niedriges Bußgeld verhängt. Gegen den Bußgeldbescheid wurde kein Einspruch eingelegt und das Bußgeld bezahlt.

9. Fehlende Vereinbarung nach Art. 26 DSGVO

Führen mehrere demselben Unternehmensverbund angehörende Gesellschaften eine Kundendatenbank, sind sie gemeinsam für die Verarbeitung Verantwortliche. Dies erfordert eine Vereinbarung gem. Art. 26 DSGVO. Das Fehlen einer solchen Vereinbarung wurde mit einer Geldbuße sanktioniert.

Ein Unternehmen, das Kurse für Erwachsenenbildung anbietet, gehört mit verschiedenen anderen Unternehmen mit ähnlichen Angeboten zum selben Mutterkonzern. Der spätere Beschwerdeführer hatte einen Kurs bei einem der Unternehmen gebucht und auch teilgenommen, aber die entstandenen Kursgebühren nicht bezahlt. Einige Zeit später meldete er sich bei einem anderen Unternehmen des Konzerns zu einem Kurs an und wurde dort abgelehnt. Als Begründung teilte man ihm mit, dass er noch Zahlungsrückstände hätte bei dem Unternehmen, dessen Kurse er bereits besucht hatte. Auf seine Beschwerde hin hat der HmbBfDI die Unternehmen untersucht und dabei festgestellt, dass diese Unternehmen eine gemeinsame Datenbank nutzten. Bucht ein Kunde einen Lehrgang, wird er von diesem Zeitpunkt an unter einer einheitlichen Kundennummer in der Datenbank geführt. Die Verwaltungen der Verbundunternehmen können anhand der Kundennummer erkennen, ob und an welchen anderen Lehrgängen der Verbundunternehmen der Kunde bereits teilgenommen hat und ob Zahlungsrückstände bei Verbundunternehmen bestehen.

Es ist fraglich, ob ein solches Vorgehen zulässig ist, immerhin kennt die DSGVO kein Konzernprivileg, nach dem die Daten zwischen Unternehmen eines Konzerns frei(er) ausgetauscht werden. Allerdings ist es unbestritten, dass das Führen einer gemeinsamen Kundendatenbank durch mehrere, rechtlich selbstständige Unternehmen, zu einer gemeinsamen Verantwortung gem. Art. 26 DSGVO führt.

Dies erfordert gem. Art. 26 Abs. 2 DSGVO eine Vereinbarung, welche die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. Eine solche existierte jedoch nicht, weshalb der HmbBfDI ein Bußgeld in Höhe von 13. 000 Euro verhängte.

10. „Private“ Aufnahmen von Dritten

Die Anfertigung von Fotos und Videos fremder Person fällt in den Anwendungsbereich der DSGVO. Die Haushaltsausnahme des Art. 2 Abs. 2 lit c) DSGVO findet keine Anwendung, da es sich nicht um eine ausschließlich persönliche Tätigkeit handelt. Rechtswidrig erstellte Aufnahmen können mit einer Geldbuße sanktioniert werden.

Aufnahmen, die Privatpersonen mit dem Mobiltelefon oder einer Digitalkamera auf der Straße von Fremden anfertigen, zu denen sie keinerlei Beziehung haben, stellen einen sehr viel größeren Teil der Arbeit des HmbBfDI dar als zu erwarten war. Es kommt immer wieder vor, dass Menschen sich gegenseitig filmen. Auch wenn der Gefilmte nicht einverstanden ist, kann dies gerechtfertigt sein, weil ein berechtigtes Interesse vorliegt, zum Beispiel wenn es im Nachgang eines Verkehrsunfalls zu einer Streitigkeit mit Drohungen auf der Straße kommt. Dann ist das Anfertigen von Aufzeichnungen anlassbezogen und häufig auch zulässig. Besteht hingegen keinerlei Kontakt zwischen der filmenden und der gefilmten Person und geht es bei den Aufnahmen konkret um die gefilmte Person, ist diese also nicht bloßes Beiwerk zum Beispiel einer Straßenszene, so ist das Anfertigen von Aufnahmen unzulässig. Die Motivation für derartige Aufnahmen, zu denen beim HmbBfDI Beschwerden eingereicht werden, ist häufig sexueller Natur.

Im Berichtszeitraum hatte der HmbBfDI verschiedene derartige Beschwerden zu verfolgen: So hatte ein Taxifahrer auf der Straße

ihm fremde Jugendliche fotografiert und diese Aufnahmen in einem Ordner gespeichert, der einen sehr hohen Anteil an pornografischen Aufnahmen hatte. In einem anderen Fall soll ein Mann auf einem Stadtteilfest gezielt Kinder gefilmt haben, die mit ihren Eltern dort zum Feiern waren. Im Wohlerspark in Altona hat ein Mann heimlich junge Frauen gefilmt, die sich dort leicht bekleidet zum Sonnenbaden aufgehalten haben. In der Europapassage ist ein Mann einer Familie gefolgt und hat dabei durchgehend und gezielt die minderjährige Tochter der Familie gefilmt. Auch gehen immer wieder Beschwerden ein, weil Frauen unter den Rock in den Intimbereich gefilmt wird. Der Gesetzgeber hat das „Upskirting" zwar im Sommer 2020 zur Straftat nach § 184k StGB erklärt. Nach dieser Norm können aber keine Taten bestraft werden, die vor dem Wirksamwerden der Gesetzesänderung begangen wurden.

Diese Fälle werden regelmäßig von der Polizei und der Staatsanwaltschaft Hamburg an den HmbBfDI abgegeben. Der Erfolg der Maßnahme hängt häufig von der Ermittlungstätigkeit der Polizei ab. Hat diese schnell reagiert, das Tatwerkzeug gesichert und vor allem die damit angefertigten Aufnahmen, so können derartige Fälle regelmäßig mit Geldbußen abgeschlossen werden. In einem Fall hat der Verteidiger des Filmenden eingewandt, dass der HmbBfDI dies nicht mit einem Bußgeld belegen dürfe. Es handele sich beim Anfertigen derartiger Aufnahmen um eine „ausschließlich persönliche oder familiäre Tätigkeit", die gem. Art. 2 Abs. 2 lit c) DSGVO nicht in den Anwendungsbereich des Datenschutzrechts falle. Da der HmbBfDI ohnehin eine richterliche Bestätigung der polizeilichen Beschlagnahme des Tathandys einholen musste, bot sich hier eine gute Gelegenheit, diese Frage gerichtlich klären zu lassen.

Wie zu erwarten war, ist der zuständige Ermittlungsrichter des AG Hamburg der Argumentation des Verteidigers nicht gefolgt. In einem Beschluss vom 3.7.2020 (163 Gs 656/20) hat das Gericht in erfreulicher Deutlichkeit ausgeführt: „Der Betroffene versteht diese Regelung [gemeint ist die Haushaltsausnahme nach Art. 2 Abs. 2 lit c) DSGVO] jedoch ersichtlich falsch, wenn er daraus schließen sollte,

dass es ihm jederzeit frei steht, in der Öffentlichkeit eigenmächtig, gezielt Fotographien von ihm fremden Personen zu fertigen.“ Fremde Personen, die sich in der Öffentlichkeit bewegten, könnten nicht durch das Anfertigen von Fotografien zu persönlichen Zwecken in die Privatsphäre desjenigen „hineingezogen“ werden, der derartige Fotos anfertigt.

Die Anwendbarkeit des Datenschutzrechts führt nicht automatisch zu einer Unzulässigkeit des Filmens. Bei derartigen Aufnahmen, denen eine sexuelle Motivation zugrunde liegt, fehlt es jedoch an einer Rechtsgrundlage. Die Aufnahmen sind dann rechtswidrig und der HmbBfDI ahndet dies entsprechend.

VI. BERATUNGEN UND DATENSCHUTZ-KOMMUNIKATION

1. Mail-Verschlüsselung beim Allgemeinen Sozialen Dienst

Die Pilotierung beim Allgemeinen Sozialen Dienst wurde im Sommer 2020 erfolgreich durchgeführt. Der weitere Einführungsprozess für eine flächendeckende Nutzung im ASD ist jedoch immer noch offen.

Die Kommunikation zwischen dem Allgemeinen Sozialen Dienst (ASD) und den externen Stellen läuft weiterhin ohne Inhaltsverschlüsselung der teilweise hochsensiblen Daten der betreuten Kinder und Jugendlichen. Aber im Vorhaben, zu einer datenschutzgerechten Übertragung zu kommen, ist zumindest ein Zwischenschritt zu verzeichnen. In einem Gespräch zwischen der Behördenleitung der Sozialbehörde und dem HmbBfDI wurde im Januar 2020 vereinbart, eine Pilotierung im ASD mit der bereits 2018 angedachten Technik, dem sog. Governikus MultiMessenger (GMM), durchzuführen. Dazu wurden einerseits die zur Verschlüsselung erforderlichen Zertifikate der ASD-Mitarbeiterinnen und Mitarbeiter sowie der dortigen Funktionspostfächer im GMM gespeichert. Andererseits haben auch exemplarisch zwei externe Stellen ihre Zertifikate dort implementiert. Im Sommer 2020 konnte die Pilotierung der Mail-Verschlüsselung in einer ASD-Dienststelle erfolgreich abgeschlossen werden. Die Lenkungsgruppe zu dieser Pilotierung hat sich im Ende August 2020 einstimmig dafür ausgesprochen, mit der dabei angewandten Technik den Roll-out zu starten.

Die Pilotierung hat gezeigt, dass es wichtig war, die Sachbearbeitung so wenig wie möglich mit den erforderlichen technischen Prozessen zu belasten. Dataport hat für die Pilotierung diese erforderlichen Vorbereitungsaufgaben im Auftrag ausgeführt. Auch soll die Handreichung für die Beschäftigten des ASD aufgrund der Erfahrungen aus der Pilotierung verbessert werden. Zur Erhöhung der Benutzerfreundlichkeit kann auch beitragen, wenn nunmehr die seit langem angekündigte Einbindung von Adressbüchern im GMM in 2021 umgesetzt werden wird.

Eine Erfahrung aus der Pilotierung ergab gleichzeitig, dass auch die externen Stellen mehr Informationen benötigen. Dazu können insbesondere Handreichungen dienen, wie die externen Stellen die Zertifikate im GMM und in ihren eigenen Mail-Systemen speichern können und welche Abläufe sich im Mailverkehr mit dem ASD verändern werden. Durch frühzeitige Informationen an die externen Stellen könne sich diese inhaltlich ggf. unter Einschaltung ihres IT-Dienstleisters auf die erforderlichen Anpassungen der IT-Systeme einstellen.

Trotz des klaren Votums aus der Lenkungsgruppe zur Pilotierung konnte bis zum Redaktionsschluss des vorliegenden Tätigkeitsberichts die Sozialbehörde ihren internen Klärungsbedarf für ein Roll-out-Projekt zur Mail-Verschlüsselung beim ASD noch nicht abschließen. Ob und wie es dem Roll-Out im Jahr 2021 weiter gehen wird, ist somit auch drei Jahre nach der Prüfung des HmbBfDI im ASD des Bezirksamts Wandsbek immer noch offen.

2. Beihilfe Digital

Der Abrechnungsprozess von Beihilfedaten über die „Beihilfe Digital" beinhaltet in großem Umfang die Verarbeitung sensibler Gesundheitsdaten von Mitarbeitern. Hinsichtlich der gemäß Art. 32 Abs. 1 DSGVO zu treffenden Maßnahmen konnte dennoch bislang keine Einigkeit mit dem ZPD erzielt werden.

Während die Bearbeitungsprozesse der zentralen Beihilfestelle der Freien und Hansestadt Hamburg (FHH) beim Zentrum für Personaldienste (ZPD) bereits weitestgehend digital erfolgen, konnten die Beihilfeberechtigten ihre Anträge und die dazugehörenden Belege (wie Arzt- und Medikamentenrechnungen) bislang ausschließlich mittels eines schriftlichen Antrages einreichen. Dies sollte sich ändern. Die Beihilfeberechtigten sollten neben der klassischen schriftlichen Antragstellung zusätzlich nicht nur die Möglichkeit erhalten, ihren Beihilfeantrag beim ZPD digital einzureichen, sondern über

das gleiche Portal auch die Erstattungsanträge bei ihren privaten Krankenversicherungen (PKV) einreichen können. Hierzu wurde das Projekt „Beihilfe Digital" eingesetzt, welches der HmbBfDI seit Ende 2018 begleitet.

In Kooperation von ZPD, Dataport, der CompuGroup Medical Mobile GmbH (CGM) und dem Anbieter MGS Meine Gesundheit Services GmbH (MGS) wurde dessen App „Meine Arztrechnung", welche auch von einigen privaten Krankenversicherern bereits verwendet wird, entsprechend angepasst. Der Nutzung dieser Systeme liegen separate Nutzungsvereinbarungen mit der MGS und der CGM zugrunde. Die Nutzung ist für die Beihilfeberechtigten freiwillig.

Beihilfeberechtigte können ihre Arztrechnung und sonstigen Belege mit ihrem Smartphone fotografieren, diese in der App hochladen und perspektivisch sowohl an ihre PKV (sofern diese angeschlossener Partner ist), als auch an ihre Beihilfestelle versenden. Der Versand zwischen den angeschlossenen Partnern erfolgt transportverschlüsselt, der App-Anbieter erhält keinen Zugriff auf die hochgeladenen Rechnungen.

Die Nutzer können die hochgeladenen Belege ohne zeitliche Befristung wieder abrufen und verwalten. Eine Bescheidzustellung über die App ist für eine spätere Ausbaustufe geplant.

Der HmbBfDI hat von Beginn an darauf hingewiesen, dass insbesondere wenn vom Nutzer und damit auch von potentiellen Angreifern auf die eingereichten Daten zugegriffen werden kann oder auch Rückmeldungen/Bescheide über diesen Weg an den Nutzer gesandt werden sollen, ein dem hohen Schutzniveau angemessener Identifizierungs- und Authentisierungsprozess vorzusehen ist.

Mit dem ZPD besteht Übereinkunft, dass die Daten der Mitarbeiter, Versorgungsempfänger und ihrer Angehörigen, welche im Rahmen der Beihilfebearbeitung verarbeitet werden, einem hohen Schutzniveau unterliegen.

Die derzeitige Lösung des ZPD sieht vor, dass der Nutzer bei der Online-Registrierung für die App „Meine Arztrechnung“ ein Benutzerkonto anlegt, indem er einen Benutzernamen (gültige E-Mail-Adresse) angibt. Der für die Nutzung erforderliche Benutzerzugang („CGM LIFE Key“) sowie das Benutzerkonto („CGM LIFE Konto“) wird wiederum von der CGM angeboten und bei der Online-Registrierung eingerichtet.

Im weiteren Registrierungsprozess wird der Beihilfeberechtigte zur Identifizierung aufgefordert, seine Personalnummer und sein Geburtsdatum einzugeben. Ergibt der Abgleich der eingegebenen Daten eine Übereinstimmung mit den beim ZPD hinterlegten Personalstammdaten, wird ein Brief mit einem persönlichen Freischaltcode an die aktuell in beim ZPD gespeicherte private Postadresse des Mitarbeiters versandt.

Als zweiter Authentisierungsfaktor ist die Verwendung einer durch den Nutzer frei wählbaren Authenticator-App (TOTP-Verfahren; zeitlich limitierte Einmalkennworte) vorgesehen. Der Nutzer kann nach Installation der App und nach Eingang des Code-Briefes die Registrierung mit der Eingabe des Codes abschließen. Die Authentisierung erfolgt dann bei jeder Anmeldung an der App mit den Zugangsdaten Benutzerkennung und Passwort und einem von der Authenticator-App erzeugten Einmalkennwort gegenüber dem ZPD.

Während in dem HmbBfDI vorgelegten datenschutzrechtlichen Unterlagen daneben die geplante Einbindung der Online-Ausweisfunktion des elektronischen Personalausweises dargestellt und auch noch in der Mitteilung über die im März 2020 erfolgte Produktivsetzung des Verfahrens für Ende 2020 in Aussicht gestellt wurde, ist eine Implementierung bislang nicht erfolgt und seitens des ZPD auch nicht mehr beabsichtigt.

Welche technischen Maßnahmen zur Datensicherheit, u.a. damit auch zur Authentifizierung von Nutzern erforderlich sind, richtet sich nach Art. 32 und 25 DSGVO. Hierbei ist der Stand der Technik zu berücksichtigen. Der HmbBfDI hat dem ZPD bereits im Mai 2020 in einer

ausführlichen Stellungnahme mitgeteilt, dass aufgrund der hohen Risiken ein Authentisierungsverfahren unter Nutzung eines Hardwaretokens – wie beispielsweise den neuen Personalausweis oder andere RFID-fähige Karten – erforderlich ist. Nur so können die umfangreich verarbeiteten Gesundheitsdaten ausreichend sicher vor einem unberechtigten Abruf geschützt werden. Die Weiternutzung des aktuell vom ZPD zur Verfügung gestellten Verfahrens unter Nutzung von Einmalkennworten wäre für einen Zeitraum bis Ende 2022 nur unter konkret benannten Voraussetzungen denkbar: Dazu gehören einerseits, dass konkrete Schritte eingeleitet werden, um unverzüglich ein Authentisierungsverfahren unter Nutzung eines Hardwaretokens zu implementierten. Andererseits müssen die Nutzer über die bestehenden Restrisiken des Verfahrens mit den Einmalkennworten informiert werden und einer solchen Lösung zustimmen.

Der Bundesgesetzgeber hat mit dem von den Datenschutz-Aufsichtsbehörden stark kritisierten Patientendatenschutzgesetz vom 14.10.2020 auch die Zugriffsbedingungen normiert, mit dem Betroffene auf ihre sensiblen Gesundheitsdaten zugreifen können. Diese sind im § 336 SGB V neu festgelegt. Die flächendeckende Umsetzung des § 336 SGB V wird den Stand der Technik in einem mit der Beihilfe-App inhaltlich vergleichbaren Bereich mit prägen. Zwar ermöglicht die neue Vorschrift Zugriffe der Betroffenen auf ihre Gesundheitsdaten unter Umständen auch mittels eines Softwaretokens, wie einem Einmalkennwort. Sie stellt aber gleichzeitig klar, dass die Option eines Hardwaretokens anzubieten ist und der Betroffene insofern ein Wahlrecht hat. Darüber hinaus wird im § 336 SGB V n.F. ausdrücklich dargelegt, dass der Betroffene auf die Besonderheiten des Zugriffs unterrichtet werden muss, wenn keine Absicherung des Zugriffs durch einen Hardwaretoken erfolgt. Dieser Lösung muss der Betroffene ausdrücklich vorher zustimmen, wenn er diese nutzen möchte.

Der HmbBfDI wird sich weiter für eine sichere Lösung für die Beihilfe-App einsetzen, bei der die Betroffenen zwischen den beiden Authentisierungsverfahren wählen können.

3. Videokonferenzsysteme in der Lehre

Der Einsatz von Videokonferenzsystemen zur Durchführung von Lehrveranstaltungen und zur Überwachung von Studierenden beim Schreiben von Klausuren bringt verschiedene datenschutzrechtliche Probleme mit sich und sollte von verantwortlichen Stellen gut überdacht werden.

Aufgrund der durch den Virus SARS-CoV-2 bedingten Einschränkungen des öffentlichen Lebens waren Präsenzveranstaltungen an den öffentlichen und privaten Hochschulen nur eingeschränkt möglich, so dass Lehrveranstaltungen unter Zuhilfenahme von digitalen Videokonferenzsystemen durchgeführt und teilweise Prüfungen auf digitalem Wege von den Studierenden an ihren privaten Endgeräten zu Hause geschrieben wurden.

Die in der Folge beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zur Verarbeitung der in diesem Zusammenhang verwendeten personenbezogenen Daten der Studierenden eigehenden Fragen zeigten insbesondere, welche Bedeutung den Informationspflichten nach den Art. 12 und 13 Datenschutz-Grundverordnung (DSGVO) oder nach Art. 4 Nr. 11 DSGVO (als Grundlage für einen Einwilligung) zukommt.

Die Bucerius Law School (BLS) ließ beispielsweise im Zeitraum vom 16.03.2020 – 31.03.2020 die Abschlussklausuren des Frühlingstrimesters von den Studierenden in Form von Fernklausuren schreiben. Um Täuschungsversuchen vorzubeugen, wurde für das Schreiben der Fernklausuren die Verwendung des digitalen Videokonferenzdienstes der Zoom Inc. (Zoom) vorgeschrieben. Die BLS setzte Zoom als sog. „software as a service" ein, so dass der Videokonferenzdienst über die Server von Zoom genutzt wurde. Für die Teilnahme an den Videokonferenzen war ein Anmeldeverfahren durch die Teilnehmer zu durch-

laufen, wobei es für die Studierenden offen gelassen wurde, sich über eine zu installierende App des Dienstanbieters Zoom oder über dessen Internetseite an der Videokonferenz für die Klausur anzumelden.

Die nach den Art. 12 und 13 DSGVO erforderlichen Datenschutzhinweise erteilte die Hochschule den Studierenden zunächst nicht. Es blieb für die Studierenden aufgrund fehlender Informationen Art und Umfang der Verarbeitung ihrer personenbezogenen Daten im Rahmen der Videoüberwachung während der Klausur unklar. Insbesondere wurde nicht ersichtlich, welche Daten genau verarbeitet wurden, wo diese Daten gespeichert wurden und welche Funktionen des Videokonferenzdienstes genau zum Einsatz kommen sollten. Dabei ist zu bedenken, dass zum damaligen Zeitpunkt Zoom über Funktionen wie das sog. Aufmerksamkeitstracking verfügte, welche erhebliche Zweifel an der datenschutzrechtlichen Zulässigkeit der damit verbundenen Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO mit sich brachte. Auch gab es eine Aufzeichnungsfunktion, wobei für die Studierenden mangels ausreichender Hinweise nicht deutlich wurde, ob eine Aufzeichnung seitens der BLS vorgenommen und wo diese Aufzeichnung gespeichert werden sollte. Auch war unklar, ob ggf. ausreichende organisatorische und technische Maßnahmen gegen einen Einsatz dieser Zusatzfunktionen getroffen wurden. Hinweise auf Konfigurationsmöglichkeiten zum Schutz der Privatsphäre, wie z.B. dem Einsatz von Filtern zur Unkenntlichmachung des privaten Hintergrunds im Videobild, gab die BLS zudem ebenfalls nicht.

Die Studierenden sahen sich durch den Einsatz der Videotechnik einem Einblick in ihre Privaträume und damit in ihre Privatsphäre gegenüber, ohne Art und Umfang der Datenverarbeitung und das Vorhandensein entsprechender technischer Schutzmaßnahmen absehen zu können. An diesem Beispiel zeigt sich: Der Einsatz digitaler Techniken durch zunächst unüberblickbare Funktionen ohne die erforderlichen Informationen gemäß den Art. 12 und 13 DSGVO macht die Datenverarbeitung zu einem Black-Box-Verfahren. Transparenz und Informationen sind für die Betroffenen unabdingbar zur Grundrechtswahrung und nicht nur ein bloßer Formalismus.

Durch Intervention des HmbBfDI wurden im Laufe der weiteren Klausurphase erstmals Datenschutzhinweise erteilt, die aber gemessen an den Inhaltsanforderungen aus Art. 13 Abs. 1 und 2 DSGVO unvollständig waren. Hierin wurde in bruchstückhafter Weise über die Verarbeitung von Bild- und Tondaten, die hierbei verfolgten Zwecke und eine fehlende Speicherung aufgeklärt. Erst nach weiterer Beanstandung gab die BLS schließlich eine weitere überarbeitete Fassung der Datenschutzhinweise an die Studierenden heraus.
Vergleichbare Probleme zeigten sich auch bei dem Einsatz digitaler Videokonferenzdienste in den einzelnen Fachbereichen der Universität Hamburg zur Durchführung von Lehrveranstaltungen. Fehlende Datenschutzhinweise führten auch hier zu Anfragen von Studierenden beim HmbBfDI.

Mangelnde Information der Studierenden ließen das Bestehen einer Rechtsgrundlage für die Verarbeitung ihrer personenbezogenen zweifelhaft erscheinen. Sowohl die BLS wie auch die Universität Hamburg beriefen sich als Rechtsgrundlage für die Verarbeitung der Studierendendaten auch auf eine Einwilligung nach Art. 6 Absatz 1 Satz 1 Nr. 1 DSGVO. Dafür ist gemäß Art. 4 Nr. 11 DSGVO zwingend über Art und Umfang der Datenverarbeitung aufzuklären, da nur dann eine Einwilligungserklärung „in informierter Weise" abgegeben werden kann, was in den vorliegenden Fällen nicht erfolgt war.

Es verblieben weitere offene datenschutzrechtliche Fragestellungen, wie z.B. das Vorliegen einer gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO hinsichtlich der Metadatenverarbeitung während der Nutzung eines digitalen Dienstes durch die Studierenden, bzw. bei deren Anmeldung zu einer Videokonferenz über die Homepage eines Anbieters des verwendeten digitalen Dienstes. Auch die daran anschließende Frage nach der Geeignetheit der von den Hochschulen beauftragten digitalen Dienste als Auftragsverarbeiter, konnte nicht gelöst werden. Die BLS hat beispielsweise von einer Klausurüberwachung über Zoom Abstand genommen, setzt nach Kenntnis des HmbBfDI diesen Dienst weiter für die Durchführung von Lehrveranstaltungen ein. Hier wird zu prüfen sein, in wie weit die Entscheidung des Europäische Gerichtshof

vom 16. Juli 2020 (Rechtssache C-311/18, Schrems II) Einfluss auf die datenschutzkonforme Verwendung von Zoom an der BLS haben kann.

Die Problematik des Bestehens einer gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO in Bezug auf die Verarbeitung von Metadaten der Studierenden und der Übermittlung personenbezogener Daten der Studierenden an Auftragsverarbeiter in Drittländer im Sinne der Art. 44 ff. DSGVO könnte Anlass sein, auf eine selbstbetriebene Instanz für den datenschutzkonformen Lehrbetrieb zu setzen. Durch eine sog. „on-premise" Lösung können Videokonferenzdienste, soweit der Dienstanbieter tatsächlich diese Lösung anbietet, durch die Hochschulen auf eigenen Servern betrieben werden, so dass ein Drittlandbezug im Sinne der Art. 44 ff. DSGVO ausgeschlossen werden kann. Auch die Anmeldeprozesse zu einer Videokonferenz können auf diese Weise derart ausgestaltet werden, dass die Studierenden nicht notwendigerweise die Homepage eines Dienstanbieters für die Anmeldung aufsuchen müssen und so die Erfassung und Weitergabe ihrer Metadaten vermeiden können. Der gesamte Bereich des Einsatzes von Videokonferenzsystemen in der universitären Lehre sollte künftig eine gesetzlich klare Regelung erhalten, durch die möglichst einheitliche und rechtssichere Strukturen für Studierende, Dozenten, aber auch für die zuständigen Stellen geschaffen werden.

4. Vertretung der Aufsichtsbehörden der Länder auf EU-Ebene

Auch im aktuellen Berichtsjahr nahm der HmbBfDI die Position des Ländervertreters im Europäischen Datenschutzausschuss wahr. Aus dieser Rolle ergab sich eine Reihe zusätzlicher Aufgaben.

Bestätigt durch die Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder (DSK) wurde durch den HmbBfDI weiterhin der neben dem BfDI zweite Vertreter im EDSA gestellt. Nach wie vor ist – mehr als zweieinhalb Jahre seit Geltung der DSGVO – keine

formale Wahl dieses Ländervertreters durch den Bundesrat erfolgt, wie es § 17 BDSG vorsieht.

Corona-bedingt stieg die Sitzungsfrequenz des EDSA deutlich an. Teilweise fanden im wöchentlichen Rhythmus virtuelle Treffen über die Videokonferenzinfrastruktur des Europäischen Parlaments statt, die hierfür genutzt werden konnte. Zusätzliche Tagesordnungspunkte bescherte dem Gremium die Schrems-II-Entscheidung des EuGH bzw. der Wegfall des Privacy Shield (siehe IV 6) und die erste Entscheidung des EDSA nach Art. 65 DSGVO (siehe III 6).

Auf den insgesamt 27 Sitzungen im Jahr 2020 wurden über zehn öffentliche Leitlinien und eine Reihe weiterer, teilweise interner Papiere beschlossen. Dabei war Deutschland mit seiner Vielzahl von Aufsichtsbehörden stark involviert. Allein der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit trug durch inhaltliche Mitarbeit oder Federführung zum Zustandekommen folgender Ergebnisse bei:

- Guidelines 08/2020 on the targeting of social media users (Hauptberichterstatter zusammen mit ULD in der Social Media Subgroup)
- Guidelines 09/2020 on relevant and reasoned objection under Regulation 2016/679 (Unterstützung des Ländervertreters in der Enforcement Subgroup)
- Internal Document "EDPB Guidance on its plenary minutes" (Hauptberichterstatter gemeinsam mit dem Sekretariat des EDSA)
- Internal Document on how to deal with complaints relating to data protection infringements started before the entry into application of GDPR that continue after 25 May 2018 (Hauptberichterstatter)

Zudem sind weitere Leitlinien unter Beteiligung des HmbBfDI in Arbeit.

Neben den Routineaufgaben wie Sitzungsvorbereitung mit den anderen Länderkollegen und schriftlicher Berichterstattung haben diese Aktivitäten beachtliche Ressourcen in Anspruch genommen. Es geht hierbei nicht nur darum, unserem Selbstverständnis als Behörde mit einem starken europäischen Bezug gerecht zu werden. Vielmehr ermöglicht nur die aktive Mitarbeit eine inhaltliche Steuerung und Prä-

gung der Ergebnisse, wie sie im letzten Schritt der formalen Beschlussfassung im EDSA-Plenum nur noch in sehr geringem Maß möglich ist.

Der HmbBfDI hat die Vertretung der Datenschutzaufsichtsbehörden der Länder auf europäischer Ebene seit 2015 inne. Bis 2018 erfolgte die Vertretung auf der Ebene des Vorläufergremiums, der sog. Art. 29 Working Group, danach im Rahmen des Europäischen Datenschutzausschusses. Letzterer wurde durch die Datenschutzgrundverordnung als eigenständiges EU-Rechtsorgan mit eigenen Rechten und Pflichten geschaffen. Viele Hoffnungen, die mit der Implementierung des EDSA verbunden waren, konnten seither nicht erfüllt werden. Das Gremium, das aus den Aufsichtsbehörden aller Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten besteht, ist schwerfällig und wird seiner Aufgabe als Entscheidungsinstanz für Fragen des Rechtsvollzugs bei der grenzüberschreitenden Datenverarbeitung bislang nicht gerecht. Die Ursachen hierfür sind vielfältig und lassen sich letztlich auf gesetzgeberische Defizite bez. Fehleinschätzungen zurückführen.

Wesentliche Fragen, etwa nach einem gesamteuropäischen Bußgeldkonzept oder nach einer zügigen Bestimmung von Hauptniederlassungen von Daten verarbeitenden Unternehmen, sind zudem nach wie vor offen. Künftig wird das Gremium seine Aufgaben nur bei klarerer Prioritätensetzung und einer stärkeren Zurücknahme nationaler Interessen bei mit dem Rechtsvollzug verbundenen Entscheidungen der beteiligten Behörden wirksam erfüllen können.

5. Presse- und Öffentlichkeitsarbeit

Das Jahr 2020 brachte mit Blick auf die Anzahl der Presseanfragen einen neuen Rekord mit sich – den HmbBfDI erreichten etwa 400 entsprechende Eingänge. Für dieses Hoch sorgten insbesondere Datenschutzaspekte rund um Corona, aber auch Themen wie das EuGH-Urteil zu Schrems II oder das Bußgeldverfahren gegen H&M.

Der seit längerem zu beobachtende Trend einer stetig steigender Zahl an Anfragen seitens der Presse und der Medien zu unterschiedlichsten Themen des Datenschutzes dauert unvermindert an. Im Berichtsjahr 2020 ist hierfür vor allem die Corona-Pandemie als maßgeblicher Grund zu nennen. Zahlreiche Anfragen thematisierten die Erfassung von Corona-Gästelisten, die missbräuchliche Verwendung der Daten sowie den pandemiebedingten Einsatz von Videokommunikationssystemen im Bildungsbereich. Des Weiteren waren das EuGH-Urteil im Verfahren Schrems II mit der Suspendierung des Privacy Shield sowie das Bußgeldverfahren des HmbBfDI gegen H&M für zahlreiche Presseanfragen verantwortlich.

Weitere wichtige Themenbereiche waren der Fall ungesicherter Patientenakten eines ehemaligen Krankenhauses in Büren und ein Auskunftsheranziehungsbescheid gegen das US-Unternehmen Clearview AI, einen Anbieter einer Gesichtserkennungs-App. Wie schon in den Vorjahren sind gerade auch zu solch grenzüberschreitenden Themen zahlreiche Anfragen ausländischer Medien beim HmbBfDI eingegangen.

Mit Blick auf lokal-hamburgische Datenschutzthemen ist an erster Stelle das o.g. Bußgeld-Verfahren gegen H&M zu nennen, das auch international Beachtung fand. Des Weiteren gab es neue Entwicklungen hinsichtlich des Verwaltungsgerichtsverfahrens zu VIDEMO rund um die Frage der Berufungszulassung und die Löschung der biometrischen Datenbank. Zuletzt sei noch das Thema der Datenabrufe über Computer der Polizei Hamburg ohne dienstlichen Anlass erwähnt.

Anlässlich des zweiten Jahrestages der DSGVO erreichten den HmbBfDI erneut statistische Anfragen zur Zahl der Beschwerden, der Data Breaches und der Sanktionen. Außerdem interessierten sich die Medien für den DSGVO-Evaluationsbericht der EU-Kommission und für grundsätzliche Fragen rund um die grenzüberschreitende Datenverarbeitung und das Kohärenzverfahren im Europäischen Datenschutzausschuss.

Im Berichtszeitraum 2020 haben den HmbBfDI insgesamt 398 Presseanfragen erreicht, das sind ca. 20% mehr als im Vorjahr 2019 (332).

Im Durchschnitt wurden im Berichtsjahr 2020 rund 33 Anfragen pro Monat bearbeitet.

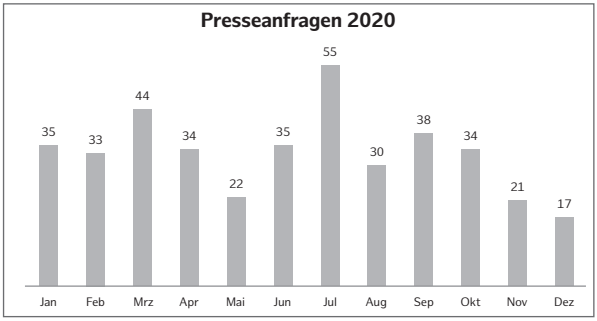


Abb. 1: Presseanfragen 2020 pro Monat mit Kennzeichnung „besonderer Ereignisse“

Wie Abb. 1 verdeutlicht, sticht der Juli mit einem Anfragen-Peak zur Erfassung der Corona-Gästelisten und die EuGH-Entscheidung zu Schrems II hervor. Bezüglich der beiden Internet-Konzerne Facebook und Google lässt sich sagen, dass die Anfragen hierzu deutlich zurückgegangen sind, von ca. 26% der Gesamtanfragenzahl in 2019 auf nur noch ca. 8% in 2020. Von den beiden Konzernen liegt Facebook (5%) vor Google (3%).

Mit Blick auf die örtliche Herkunft der anfragenden Medien ist erneut zu konstatieren, dass die mit Abstand meisten Anfragen von überregionalen Medien stammen. Anfragen ausländischer Medien sind im Jahr 2020 aufgrund auch international wahrgenommener Themen wie das H&M-Bußgeld, die EuGH-Entscheidung zu Schrems II oder Fragen rund um den EDSA deutlich angestiegen, wie die nachstehende Tabelle zeigt:

Presseanfragen...	2019	2020
regionaler Medien:	75	107
überregionaler Medien:	212	219
ausländischer Medien:	45	72
Gesamt:	332	398

Tabelle1: Presseanfragen beim HmbBfDI 2019 und 2020

Neben dem vorliegenden Tätigkeitsbericht Datenschutz 2020 gab es im Berichtsjahr keine weiteren Veröffentlichungen im Printbereich. Das Internet-Angebot des HmbBfDI wird stets aktuell weiterentwickelt. Im Berichtszeitraum hat der HmbBfDI 25 Pressemitteilungen veröffentlicht.

Zudem haben der Hamburgische Datenschutzbeauftragte sowie einige Mitarbeiterinnen und Mitarbeiter der Behörde erneut Vorträge und Präsentationen zu Aspekten der DSGVO sowie verschiedenen Themen des Datenschutzes durchgeführt und sich an Gesprächsrunden oder Podiumsdiskussionen beteiligt. Corona-bedingt fanden diese Veranstaltungen zumeist als Videokonferenzen statt. Im Rahmen der Datenschutz- und Medienkompetenzförderung des HmbBfDI gab es ebenfalls eine Beteiligung an zahlreichen entsprechenden Veranstaltungen (siehe hierzu ausführlich VI 6).

6. Medienbildung

Datenschutzkompetenzförderung gehört auch zu den Kernaufgaben von Datenschutzbehörden, denn die Fähigkeiten zum Selbstschutz junger Menschen vor möglichen Risiken in der digitalen Welt müssen gestärkt werden. Datenschutz ist eben nicht nur Rechtsvollzug und der Erlass von Bußgeldern und Verwaltungsanordnungen.

Am 11. Februar 2020 fand der Safer Internet Day unter dem Motto „Together for a better Internet“ statt. Der HmbBfDI partizipierte gemeinsam mit weiteren Partnern (Medienanstalt Hamburg/Schleswig-Holstein (MA HSH), Polizei Hamburg, Verein Blinde Kuh e.V. und Bücherhallen Hamburg) an einem Aktionstag rund um das Thema „Internetsicherheit und Datenschutz“. Durch eine enge Zusammenarbeit der verschiedenen Institutionen konnte ein vielfältiges Informationsangebot anboten werden. Der HmbBfDI informierte große und kleine Besucherinnen und Besucher, wie spielerisch ein sicheres

und trotzdem leicht zu merkendes Passwort erstellt werden kann.

Anfang 2020 wurde zudem das Informationsangebot des HmbBfDI ausgebaut. So befinden sich nun auf der Seite https://datenschutz-hamburg.de/medienbildung umfangreiche medienpädagogische Informationen für Kinder und Jugendliche, Eltern und Sorgeberechtigte sowie Pädagoginnen und Pädagogen. Der HmbBfDI stellt dort stetig neue Informationen zur Verfügung und gibt Tipps und Tricks zur sicheren Nutzung des Internets.

Die Corona-Pandemie hat schonungslos aufgezeigt, dass viele deutsche Schulen bei der Digitalisierung hinterherhinken. Oft fehlt es an einer funktionierenden digitalen Schul-Infrastruktur, den entsprechenden Lehr-Lern-Konzepten und einer zeitgemäßen Ausbildung angehender Lehrkräfte. Auch wenn Finanzmittel aus dem Digital-PaktSchule abfließen und Schulen in Hamburg mit digitalen Endgeräten ausgestattet werden, bleibt noch viel zu tun. Dieser Rückstand machte sich Anfang dieses Jahres während der coronabedingten Schließungen der Schulen deutlich bemerkbar. Da für einen ausschließlichen digitalen Distanzunterricht weder eine Strategie noch ein entsprechendes Konzept vorlag, nutzten viele Schulen verschiedene Lösungen und Produkte, ohne datenschutzrechtliche Fragstellungen hinreichend zu berücksichtigen. Dies führte zu zahlreichen Eingaben und Beschwerden beim HmbBfDI (siehe hierzu Kapitel II 5. „Videokonferenzsysteme im Schulunterricht“).

Einen Höhepunkt erreichte die durchaus emotional geführte Debatte zum E-Schooling mit der (Falsch-) Meldung, der HmbBfDI würde Skype für den Fernunterricht verbieten. Bereits 2019 forderte der HmbBfDI eine Anlaufstelle für pädagogisches Fachpersonal, aber auch für Schulleiterinnen und Schulleiter, bei der sie sich (bestenfalls lokal) zu rechtlichen Fragestellungen beraten, informieren, weiterbilden und absichern können. Alternativ wäre denkbar, dass die zuständige Stelle vermehrt Informationsmaterial und Leitfäden zur Verfügung stellt, um so Unsicherheiten abzubauen.

Außerdem wurde deutlich, dass noch mehr in die Lehr- und Weiterbildungsangebote für Lehrerinnen und Lehrer investiert werden muss. Eine aktuelle Studie zeigt, dass sich nur 40 Prozent aller aktuellen Lehramtsstudierenden gut auf die digitalen Herausforderungen ihres späteren Arbeitsalltags vorbereitet fühlen (https://studitemps.de/magazin/frauen-fuehlen-sich-durch-studium-weniger-gut-auf-digitalisierung-vorbereitet-als-maenner-%e2%80%92-brandenburger-hochschulen-sind-vorreiter/). Es ist daher wichtig, dass die Medienpädagogik und ein dazugehöriges juristisches Grundwissen bereits in die Ausbildung angehender Lehrerinnen und Lehrer, aber natürlich auch von Erzieherinnen und Erziehern und weiteren pädagogischen Fachkräften, integriert werden. Die Forderungen, die der HmbBfDI bereits in seinem letzten Tätigkeitsbericht an das Bildungswesen formuliert hat (vgl. 28. TB 2019, Kapitel V 11), verlieren daher keineswegs an Wichtigkeit und Aktualität.

Gleichwohl muss an dieser Stelle anerkannt werden, dass einige Forderungen - teilweise durch den massiven Digitalisierungsdruck - dieses Jahr umgesetzt werden konnten. So wurden Finanzmittel freigegeben, die den Ausbau der digitalen (schulischen) Infrastruktur und die Ausstattung der Lehrerinnen und Lehrer mit digitalen Endgeräten weiter vorantreiben werden. Letzteres ist auch aus Datenschutz-Sicht zu begrüßen. Auch wird der Hamburger Medienpass überarbeitet und aktualisiert. Die verpflichtenden modularen Unterrichtseinheiten zur Digitalisierung beinhalten auch einen Baustein zum Thema „Soziale Medien und Datenschutz“.

Anfang des Jahres konnte der HmbBfDI zudem noch Workshops an Schulen und weiteren Bildungseinrichtungen durchführen. Ziel dieser Workshops ist, mögliche Unsicherheiten abzubauen und die Kompetenzen der Teilnehmenden in Bezug auf den Umgang mit persönlichen Daten und Privatsphäre zu fördern. Medienpädagogik gilt als eine der Schlüsseldisziplinen in einer zunehmend komplexen mediatisierten Welt („Medienpädagogik als Schlüsseldisziplin in einer mediatisierten Welt. Perspektiven aus Theorie, Empirie und Praxis“ in MedienPädagogik Heft 37). Die Förderung dieser „21-Century“-Kompetenzen (Mehr

dazu hier: https://www.oecd.org/site/educeri21st/40756908.pdf) ist sowohl für pädagogische Fachkräfte, aber auch für Kinder und Jugendliche unabdingbar. Denn nur mit diesen Kenntnissen können Kinder und Jugendliche auf eine Welt von morgen vorbereitet werden. Natürlich wurden wegen der coronabedingten Einschränkungen auch beim HmbBfDI viele Workshops und Schulungen von Schulen und Institutionen der Offenen Kinder- und Jugendarbeit (OKJA) abgesagt. Diese Entwicklung ist vollkommen nachvollziehbar. Wichtig ist dennoch, auch nach der Pandemie, nicht zum Status quo ante zurückzukehren, sondern auch Medienkompetenz in der Schule zu vermitteln. Erfreulicherweise treffen seit Ende dieses Jahres wieder vermehrt Anfragen zu Datenschutz-Workshops und -Schulungen beim HmbBfDI ein.

Für die Förderung von Datenschutzkompetenz in Schulen hat der HmbBfDI die Produktion des Schulfilmprojektes „Datenschutz – Regeln und Rechte in der Onlinewelt" der FWU als Fachberatung unterstützt. Der Schulfilm richtet sich an Jugendliche und erläutert zielgruppengerecht die gesellschaftliche Relevanz von Datenschutz. Auch erstellte der HmbBfDI in Zusammenarbeit mit einer didaktischen Fachberaterin auf den Film abgestimmte Lernmaterialien. Der Film, inklusive der Begleitmaterialien, ist ab dem kommenden Jahr in allen Schulbibliotheken der Bundesländer frei abrufbar, die über eine Kooperation mit der FWU verfügen.

Zur Vermittlung der vielfältigen "21-Century-Skills" ist eine institutionelle Öffnung von Schule mit außerschulischen Lernorten und Institutionen unabdingbar. Einer dieser Lernorte kann auch die Offene Kinder- und Jugendarbeit sein. Gemeinsam mit dem Bezirksamt Eimsbüttel hat der HmbBfDI daher ein Projekt ins Leben gerufen, das Pädagoginnen und Pädagogen dabei unterstützt, eigene Medienkompetenz-Projekte zu konzipieren, die praxistauglich und zielgruppengerecht sind. So stehen Ende des Projektzeitraumes verschiedene praxiserprobte Projektkonzepte zur Verfügung, die dann an andere Institutionen weitergegeben werden können.

Gemeinsam mit der Schulbehörde, der Behörde für Kultur und Me-

dien (BKM), der Behörde für Arbeit, Gesundheit, Soziales, Familie und Integration (Sozialbehörde), dem Mediennetz Hamburg und weiteren Partnern wurde auf Basis eines bürgerschaftlichen Ersuchens (Drucksache 21/15381) ein Entwurf eines Monitoring-Systems und eines Fonds zur Medienkompetenzförderung erarbeitet. Mit dem Medienkompetenzfonds steht demnach ein Programm bereit, durch das medienpädagogische Projekte gefördert werden können. Es gilt nun politischen Willen zu zeigen, die Wichtigkeit von Medienbildung anzuerkennen und den Fond mit den angemessenen Finanzmitteln auszustatten. Gleiches gilt auch für bereits etablierte Medienkompetenz-Maßnahmen.

Eltern gelten als die wichtigsten Lernunterstützer der Kinder („Lernen zu Hause" von der Telekom Stiftung aus 2020, Seite 40). Daher ist es unabdingbar, auch zunehmend in die medienpädagogische Elternarbeit zu investieren. Eine etablierte medienpädagogische Maßnahme stellt „ElternMedienLotse" dar. „ElternMedienLotse" ist eine von der Schul- und Sozialbehörde geförderte Maßnahme, in der Erwachsene geschult werden, um medienpädagogische Elternabende zu veranstalten. Hier mag argumentiert werden, dass dies eine klassische Aufgabe der Lehrerinnen und Lehrer darstelle. Allerdings verfügen viele Lehrerinnen und Lehrer momentan noch nicht über die entsprechende Qualifikation, um Eltern über neue, sich ständig ändernde Medienphänomene aufzuklären und bei medienpädagogischen Fragestellungen zu beraten (siehe hierzu: E-Goverment Monitor 2020 – Digitale Daseinsvorsorge – Bildung). Der Träger der „ElternMedienLotse"-Maßnahme, der gemeinnützige Hamburgische Bürger- und Ausbildungskanal TIDE, wird mit Blick auf die große Relevanz von medienpädagogischer Elternarbeit das Konzept der „ElternMedienLotse" 2021 überarbeiten. So sollen die Ausbildung zukünftig modular aufgebaut und aktuelle Mediengeschehnisse und -entwicklungen gezielt integriert werden. Der HmbBfDI wird TIDE bei diesem Prozess begleiten und inhaltlich bei Fragestellungen zum Thema Datenschutz unterstützen. Für diesen Prozess wird eine finanzielle Planungssicherheit benötigt, die über Ein-Jahres-Zeiträume hinausreicht, um Angebote verlässlich und effektiv zu gestalten. Der HmbBfDI setzt sich hierfür ein.

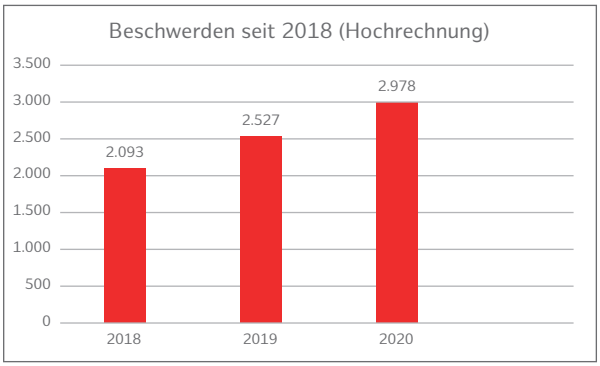
INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT VII.

1. Zahlen und Fakten

Die Eingangszahlen beim HmbBfDI waren auch im Jahr 2020 nicht nur ungebrochen hoch, es wurden teilweise auch wieder neue Höchststände erreicht. So haben den HmbBfDI im Berichtszeitraum insgesamt 3.900 schriftliche Eingänge erreicht, das sind 261 mehr als 2019 und 2.281 (abzüglich IFG-Eingaben) mehr als 2017 vor Inkrafttreten der DSGVO. Unter dem Begriff der schriftlichen Eingänge versteht der HmbBfDI insbesondere schriftliche datenschutzrechtliche Beschwerden und Beratungsanfragen, aber auch Auskunftsersuchen, die sich an den HmbBfDI als Verantwortlicher im Sinne der DSGVO oder als auskunftspflichtige Stelle nach dem Hamburgischen Transparenzgesetz (HmbTG) richten sowie informationsfreiheitsrechtliche Beratungsanfragen. Da die genaue Spezifizierung von den zuständigen Fachreferentinnen und –referenten vorgenommen wird, vergeht immer eine gewisse Zeit, bis alle Eingänge statistische ausgewertet sind. Dies ist der Grund dafür, dass zum Zeitpunkt der Drucklegung dieses Tätigkeitsberichts nur 3.698 (rund 95%) der Eingänge ausgewertet sind. Bei den im Folgenden aufgeführten Zahlen handelt es sich um Hochrechnungen, die zur besseren Vergleichbarkeit angestellt wurden.

1.1 Beschwerden und Beratungen

Datenschutzrechtliche Beschwerden sind schriftliche und verschriftete Eingänge, bei denen eine natürliche Person ihre persönliche Betroffenheit darlegt und bei denen Art. 78 DSGVO („das Recht auf einen wirksamen Rechtsbehelf gegen eine Aufsichtsbehörde“) anwendbar ist. Bei rund 76% der schriftlichen Eingänge des Jahres 2020 handelt es sich um datenschutzrechtliche Beschwerden. In der Hochrechnung bedeutet das, dass beim HmbBfDI insgesamt 2.978 Beschwerden, d.h. etwa 8 Beschwerden pro Tag, eingereicht wurden. Damit ist das bereits sehr hohe Beschwerdeaufkommen des Vorjahres bereits deutlich übertroffen und wird, auch nach weiterer statistischer Auswertung, ein neues Allzeithoch markiert:



Datenschutzrechtliche Beratungen sind schriftliche und mündliche Auskünfte, die den verantwortlichen Stellen, den betroffenen Personen und Behörden auf Nachfrage erteilt werden. Im Berichtszeitraum wurden hochgerechnet 358 Bürgerinnen und Bürger (Vorjahr: 415), 143 verantwortliche Stellen der Privatwirtschaft (181) und 17-mal Behörden (20) vom HmbBfDI beraten, insgesamt wurden also 518 schriftliche Beratungen durchgeführt. Damit liegt dieser Wert deutlich unter dem Wert des Vorjahres (617).

Zusätzlich wurden in diesem Jahr 634 telefonische Beratungen durchgeführt (betroffene Personen: 524; verantwortliche Stellen: 100; Behörden: 10). Insgesamt wurden also 1.152 datenschutzrechtliche Beratungen durchgeführt, was auch insgesamt deutlich weniger ist als die 1.446 im Vorjahr durchgeführten Beratungen.

Im Berichtszeitraum stehen also den deutlich gestiegenen Beschwerdezahlen den ebenso deutlich gesunkenen Beratungszahlen gegenüber. Ob sich hier ein Trend abzeichnet, wird zu beobachten sein.

1.2 Meldepflicht nach Art. 33 DSGVO

Nach Art. 33 DSGVO hat der Verantwortliche der Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden eine Mitteilung zu machen, nachdem ihm die Verletzung des Schutzes personenbezogener Daten bekanntgeworden ist, wenn durch die Verletzung voraussichtlich ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Die bekannteste Verletzung des Schutzes personenbezogener Daten ist der Hackerangriff, mit dem oftmals Schwachstellen der Datensicherheit offengelegt werden. Obwohl auch im Jahr 2020 die hauptsächlichen Gründe für die Verletzung des Schutzes personenbezogener Daten in der Mehrzahl weniger spektakulär und oftmals im menschlichen Versagen zu suchen sind (262-mal wurden E-Mails und Postsendungen an falsche Adressaten versandt, was annähernd dem Niveau des Vorjahres - 275 - entspricht), ist auffällig, dass sich die Zahl der gemeldeten Hackerangriffe von 74 auf 156 etwas mehr als verdoppelt hat. Das ist eine besorgniserregende Entwicklung, die weiter zu beobachten sein wird. Entsprechend hat sich auch die Gesamtzahl der Meldungen von Verletzungen des Schutzes personenbezogener Daten von 611 (28. TB VI 1.3) auf 686 deutlich erhöht.

1.3 Abhilfemaßnahmen

Auch im Berichtszeitraum hat der HmbBfDI wieder von seinen verschiedenen Möglichkeiten zur Abhilfe von datenschutzrechtlichen Verstößen (Art. 58 Abs. 2 DSGVO) Gebrauch gemacht. Im Einzelnen wurden im Jahr 2020 folgende Maßnahmen ergriffen:

Maßnahme	Rechtsgrundlage	Anzahl 2020
Warnungen	Art 58 Abs. 2 lit. a	1
Verwarnungen	Art 58 Abs. 2 lit. b	5
Anweisungen und Anordnungen	Art 58 Abs. 2 lit. c – g und j	2
Geldbußen	Art 58 Abs. 2 lit. i	22
Widerruf von Zertifizierungen	Art 58 Abs. 2 lit. h	0

1.4 Europäische Verfahren

Wenn eine Beschwerde o.ä. eingegangen ist, kann die als europäisches Verfahren in das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission eingegeben werden, wenn davon ausgegangen werden kann, dass auch Bürgerinnen und Bürger anderer EU-Staaten von dem vermeintlichen Datenschutzverstoß betroffen sind. Federführend ist dann die Aufsichtsbehörde, in deren Zuständigkeitsbereich der Verantwortliche seine europäische Hauptniederlassung hat, alle anderen Aufsichtsbehörden können sich im Verfahren als betroffen melden.

Europäisches Verfahren	Anzahl 2020
Verfahren mit Betroffenheit	10
Verfahren mit Federführung	2
Weitere Verfahren gem. Kap VII DSGVO (Art. 60 ff)	Werden statistisch nicht erfasst.

1.5 Stellungnahmen in Gesetzgebungsverfahren

Der HmbBfDI ist am Abstimmungsverfahren von Senatsdrucksachen zu beliefern, soweit Belange des Datenschutzes berührt werden (‚Richtlinie zur Beteiligung der/des HmbBfDI' in der Fassung vom 24. Juli 2019). Im Berichtszeitraum wurde der HmbBfDI an 61 sogenannter Drucksachenabstimmungen beteiligt, von denen 34 Gesetzgebungs- und Rechtsetzungsvorhaben (einschl. dem Abschluss von Staatsverträgen) zum Inhalt hatten.

2. Aufgabenverteilung (Stand: 1.1.2021)

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

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

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

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

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

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

Vorzimmer, Geschäftsstelle
Heidi Niemann

Sachbearbeitung Registratur
Frau Vukšić

Sachbearbeitung Registratur, Auskünfte nach Art. 15 DSGVO
Ipek Sari

Datenschutzkompetenzförderung und Medienbildung, Öffentlichkeitsarbeit
Alina Feustel

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

Grundsatzfragen Sanktionen und Aktenführung, Einzelfallbearbeitung
Cornelia Goecke

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

Grundsatzfragen Art. 58 DSGVO, Einzelfallbearbeitung
Steffen Sundermann

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

Pass-, Ausweis- und Meldewesen, Personenstandswesen, Statistik, Archivwesen, öffentliches Bau- und Wohnwesen
Uta Kranold

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

Gesundheits- und Sozialwesen, Forschung
Arne Brest

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

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

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

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

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

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

Soziale Netzwerke (insbes. Facebook, XING, Twitter), themenübergreifende Fallbearbeitung
Simon Hoffmann

Smart Devices (insbes. Voice Assistants), Entwicklung von Prüftools, technische Fortentwicklung des Internetauftritts der Behörde
Roland Schilling

Suchmaschinen (insb. Google)
Dr. Jutta Hazay

Europaangelegenheiten, Akkreditierung und Zertifizierung
Frau Jacobson

Themenübergreifende Fallbearbeitung
Amina Merkel

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

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

Technisch-organisatorische Beratung und Prüfung
Jutta Nadler

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

Internationaler Datenverkehr, Grundsatzfragen Wirtschaft, Landwirtschaft, Gewerkschaften
Dr. Jens Ambrock

Vereine, Sport, Steuerberater und Wirtschaftsprüfer, Stiftungen
Heike Wolters

Beschäftigtendatenschutz, Kreditwirtschaft, Gastronomie
Oksan Karakus

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

Gewerbliche Dienstleistungen, Industrie, Rechtsanwälte (ohne Notare), private Sicherheitsdienste und Detekteien, Markt-Meinungsforschung
Pauline Mattern

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

Auskunfteien, Versand- und Onlinehandel, Inkasso, Kultur, Bildung (ohne Schulen und Hochschulen)
Behrang Raji

Themenübergreifende Fallbearbeitung
Viola Büchl

Themenübergreifende Fallbearbeitung
Eggert Thode

E

F

G

Z

Auflage: 800 Exemplare
Foto Titelseite: Thomas Krenz
Layout & Druck: Druckerei Siepmann GmbH, Hamburg

Herausgegeber:
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Straße 22
20459 Hamburg

Tel.: 040/428 54 40 40 (Geschäftsstelle)
Fax: 040/428 54 40 00
Web: datenschutz-hamburg.de
E-Mail: mailbox@datenschutz.hamburg.de

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Hamburg