TÄTIGKEITSBERICHT DATENSCHUTZ 2024

Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Hamburg

33. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

2024

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

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

Auflage:	400 Exemplare
Bild Titelseite:	Adobe Stock / IKON Images
Layout:	Gebr. Klingenberg & Rompel in Hamburg GmbH
Druck:	Druckerei Siepmann GmbH

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

---

vorgelegt im April 2025
Thomas Fuchs
(Redaktionsschluss: 31. Dezember 2024)

INHALTSVERZEICHNIS

Vorwort

„Bußgelder sind oft notwendig, aber sie ersetzen nicht den ergebnisorientierten Dialog mit den Verantwortlichen“, so endete das Vorwort des letztjährigen Tätigkeitsberichts. Dies bleibt unsere Haltung, und trotzdem haben wir im Jahr 2024 mit 20 rechtskräftig abgeschlossenen Bußgeldverfahren bei einer Bußgeldhöhe von über 1,2 Millionen Euro die höchste Verfahrenszahl seit 2020 erreicht. Interessant dabei: Viele Fälle sind Ausdruck eines schlechten Datenmanagements. Daten werden viel länger gespeichert als notwendig, Datenlisten werden schlecht entsorgt, oft weniger aus bösem Willen als aus Unachtsamkeit oder fahrlässigem Unwissen. Dabei sind gut strukturierte digitale Prozesse nicht nur eine Frage des Datenschutzes, sondern ein Merkmal zukunftsfähiger Unternehmensführung.

Denn das Wissen darüber, zu welchem Zweck welche Daten gespeichert und weiterverarbeitet werden, ist zentral. Gerade für Unternehmen mit digitalen Geschäftsmodellen ist eine professionelle Datennutzung unumgänglich: Wie will man einen (rechtmäßigen) Datenschatz heben, wenn man sich seiner unternehmerisch gar nicht richtig bewusst ist?

Dies gilt erst recht, seit Anwendungen der künstlichen Intelligenz (KI) hinzukommen. Wir haben in diesem Tätigkeitsbericht erstmals ein ganzes Kapitel der KI gewidmet, die inzwischen immanenter Teil der Digitalisierung ist. Entsprechend nehmen die Implementierungen sprunghaft zu. Dadurch steigt bei uns die Zahl der Prüfungen und Beratungen vor allem im öffentlichen Bereich und natürlich auch die Zahl der zu beantwortenden Fragen. Positiv ist festzuhalten: Die Zusammenarbeit mit den Behörden und öffentlichen Unternehmen in Hamburg in diesem Bereich ist eng und konstruktiv. Wir begleiten

die Einführung von KI-Systemen mit technologischem Verständnis und achten zugleich auf angemessenen Datenschutz sowie klare Rechtsgrundlagen.

Diese neue Aufgabe übernehmen wir zusätzlich zu einem weiterhin wachsenden Beschwerdeaufkommen. Mit über 2600 Beschwerden wurde die Vorjahreszahl erneut überschritten. Dasselbe gilt auch für die Zahl der gemeldeten Datenschutzverletzungen, die mit 955 einen neuen Höchststand erreicht haben. Wir haben unsere Ressourcen und Abläufe bei diesen sogenannten Data Breaches optimiert, um noch schneller reagieren zu können, vor allem mit dem Ziel, die umgehende Schließung der Sicherheitslücken und die zügige Information der Betroffenen durch die Unternehmen sicherzustellen.

Trotz dieser hohen strukturellen Verfahrenslast treiben wir gezielt strategische Themen voran: Mit anlasslosen Prüfungen in ausgewählten Schwerpunktbereichen, die auch zu den eingangs erwähnten Bußgeldern führten; durch die aktive Mitgestaltung europäischer Datenschutzstandards, vor allem im Kontext der großen sozialen Netzwerke; die direkte Kommunikation mit den Bürger:innen in unserem Familienprojekt #DigitaleVorbilder; und nicht zuletzt durch den Aufbau unseres Kompetenzzentrums für KI und Datenschutz. Dies alles bisher ohne zusätzliche Haushaltsmittel. Deswegen möchte ich zum Schluss ausdrücklich die Leistung der Mitarbeiter:innen des HmbBfDI herausstellen, die das ermöglicht: Danke an alle Kolleg:innen für ihren Einsatz und ihr Engagement!

Thomas Fuchs

EINLEITUNG I.

Einleitung

Zentralisierung als Konsequenz der Digitalisierung? Wie die Umsetzung der europäischen Digitalgesetze in Deutschland den Föderalismus aushöhlt – und was jetzt getan werden muss.

Die EU hat geliefert. Die Digitalstrategie von 2020 wurde in der letzten Legislatur konsequent ins Werk gesetzt: Data Governance Act (DGA), Digital Services Act (DSA), Digital Markets Act (DMA), AI Act (Verordnung über Künstliche Intelligenz, KI-VO) und Data Act (DA).

Nun werden diese Rechtsakte, teilweise sukzessive, wirksam. Auch wenn sie als Verordnungen unmittelbar geltendes Recht sind, bedarf es nationaler Durchführungsgesetze, vor allem zur Klärung der administrativen Zuständigkeiten und Prozesse. Damit nimmt das Unionsrecht auf die unterschiedlich gewachsenen Strukturen der Mitgliedstaaten Rücksicht und gibt zugleich einen Rahmen vor, innerhalb dessen die national jeweils passenden Aufsichtsbehörden zu benennen sind.

Das stellt die deutsche föderale Struktur vor Herausforderungen, die aber nicht neu sind und seit Jahrzehnten gelöst werden. Unsere Verfassung gibt dabei Leitplanken vor: Die Länder führen die Gesetze des Bundes durch eigene Verwaltung aus, dies gilt auch für das Unionsrecht. Wirtschaftsverwaltung ist Länderkompetenz.

Vor diesem Hintergrund sind die bisher in der Öffentlichkeit wenig beachteten Vorstellungen des Bundes zur Durchführung der europäischen Digitalrechtsakte bemerkenswert. Hierzu liegen nun beschlossene Gesetze und insbesondere Referentenentwürfe vor, die es durch das vorzeitige Ende der Ampel-Regierung nicht mehr ins Gesetzgebungsverfahren geschafft haben. Dies gibt die Chance, die ansonsten isoliert diskutierten Vorschläge einmal im Zusammenhang zu betrachten.

Um das Ergebnis vorwegzunehmen: Die Umsetzung führt zu einer Entmachtung der Länder. Geplant sind weitreichende Kompetenzverlagerungen zum Bund – nicht nur im Bereich der Digitalwirt-

schaft, sondern auch bei der Aufsicht über die Verwaltungsdigitalisierung. Ein komplexes und umfangreiches Unterfangen, bei dem es der Bund sich aber einfach machen will: Hürden des Grundgesetzes und des Unionsrechts werden ignoriert, zudem macht man sich anscheinend wenig Vorstellungen über bislang nicht vorhandene Expertise und entsprechend fehlendes Personal. Zentralisierung ohne Blick für bestehende Strukturen führt in einem Föderalstaat aber nicht zu Vereinfachung, sondern zur Verdoppelung von Verwaltungsstrukturen und damit zu mehr Bürokratie. In Europa begibt sich Deutschland auf einen Sonderweg, indem es vorhandene Aufsichtsbehörden zugunsten einer neuen Superbehörde an den Rand drängt.

Das Digitale Dienste Gesetz: Durchführung des DSA

Seinen Anfang nahm diese Entwicklung mit dem Digital Services Act. Dieser verpflichtet vor allem digitale Plattformen u.a. dazu, transparent und entschlossener gegen schädliche Inhalte im Netz, hier insbesondere „Hass und Hetze", jugendgefährdende Inhalte, Fake News, etc. vorzugehen.

Das Durchführungsgesetz benannte die Bundesnetzagentur (BNetzA) zur zentralen Anlaufstelle. Damals hat diese Wahl noch etwas überrascht, denn deren Kompetenz beschränkte sich auf analoge Netze – Post, Telekommunikation, Energie und Bahn. Die Idee einer Infrastrukturbehörde für das „Digitale Netz" war metaphorisch griffig – aber tatsächlich ging es überwiegend um Fragen des Medienrechts und den Umgang mit Beschwerden von Bürger:innen. Die vorgesehene Koordination von existierenden Institutionen mit Regulierungserfahrung wie den Landesmedienanstalten und der BfDI war deshalb auch fachlich notwendig. Die vom Unionsrecht geforderte Unabhängigkeit musste die weisungsabhängige BNetzA durch eine unabhängige Position des Koordinators innerhalb der Behörde konstruieren. Die Stelle ist noch unbesetzt, ebenso wie ein großer Teil der vorgesehenen Planstellen.

Damit legte der Bundesgesetzgeber den Grundstein für sein Zielbild einer zentralen Digitalagentur für die Wirtschaft – und schaffte zugleich komplexe Doppelstrukturen. Neben der neuen zentralen Beschwerdestelle bei der BNetzA bleiben z.B. die Landesmedienanstalten weiterhin für Beschwerden zuständig. Die BfDI bekam eine neue Sonderzuständigkeit für Online-Werbung nach dem DSA – gleichzeitig bleiben die Landesdatenschutzbehörden nach wie vor zuständig für den Datenschutz bei Online-Werbung.

Durchführungsgesetz zur KI-VO

Dieser problematische Weg wird bei der Umsetzung der KI-VO weitergegangen. Mit den Datenschutzaufsichtsbehörden gibt es bereits erfahrene Regulierer, die sich ohnehin mit KI-Systemen auseinandersetzen – wie auch dieser Tätigkeitsbericht mit einem umfassenden Kapitel zeigt. Dennoch sieht der Referentenentwurf des Bundes vor, diese Aufgaben der damit bisher nicht befassten BNetzA zu übertragen. Wieder muss die Expertise erst entwickelt werden, erneut müssen Gremienkonstrukte mit partieller Unabhängigkeit die Weisungsgebundenheit der BNetzA kompensieren.

Darüber hinaus geht der Entwurf „all-in" und überträgt der BNetzA auch die Überwachung über den KI-Einsatz in Landesverwaltungen. Wenn KI-Systeme z.B. in Universitäten oder in Schulen der Länder entwickelt oder eingesetzt werden, soll eine Bundesbehörde hierüber Aufsicht führen.

Dies würde auch für den Sektor der Inneren Sicherheit gelten, also vor allem für den Polizeibereich. Hier ignoriert der Entwurf nicht nur die Eigenstaatlichkeit der Länder, sondern auch explizite Festlegungen der KI-VO. Demnach soll die bewährte rechtstaatliche Kontrolle von IT-Systemen der Polizei und Strafverfolgung auf KI ausgeweitet werden und bei den bereits zuständigen unabhängigen Datenschutzaufsichtsbehörden verbleiben.

Bezeichnend ist die Begründung im Entwurf: Die Datenschutzbehörden seien nicht innovativ genug. Nun könnte man zu dieser behaupteten Prämisse und dem Verhältnis von Innovation und Grundrechtsschutz einen eigenen Artikel schreiben, aber jedenfalls wenn es um die Innere Sicherheit geht, ist das Argument ein Kategorienfehler. Hier geht es nicht um Innovation, sondern um Grundrechtsschutz und Rechtsstaatlichkeit.

Durchführung des Data Act

Der nächste Schritt dieser Zentralisierung ist nun die Durchführung des Data Act. Darin geht es um die Nutzung und das Teilen von Daten durch Unternehmen und Behörden. Der Entwurf schlägt vor, dass auch hier die BNetzA primär zuständig sein soll. Dass der Data Act bei der Verarbeitung personenbezogener Daten in diesem Kontext vorsieht, die bestehende Datenschutzaufsicht zu nutzen und gerade keine neuen Strukturen zu schaffen, wird übergangen. Stattdessen wird als alleinige Ansprechpartnerin der BNetzA die BfDI benannt, die bisher praktisch keine Zuständigkeit für die Wirtschaft hat.

Wozu führt das? Erneut entsteht eine Doppelstruktur bei Beschwerden und die Eigenstaatlichkeit der Länder wird weiter beschnitten, da auch bei der Datennutzung durch Landesbehörden eine Bundesbehörde entscheiden würde. Dies beträfe etwa die Zusammenarbeit von Behörden und Unternehmen im Bereich der Verkehrsmobilität oder Fragen der Datennutzung im Gesundheitsbereich. Ein konkretes Beispiel: Eine universitäre Forschungseinrichtung, die Daten von Pharmaherstellern zur Bekämpfung einer gesundheitlichen Notlage nutzt, müsste künftig sowohl mit ihrer Landesdatenschutzbehörde als auch mit der BNetzA und der BfDI sprechen – je nachdem, auf welcher Rechtsgrundlage sie welche Daten verarbeitet. Statt Vereinfachung entsteht mehr Komplexität.

Die Länder sind gefragt: Was ist ihr Bild vom Föderalismus in der Digitalisierung?

Es ist deutlich geworden, dass der Bund auf die Zentralisierung der Digitalaufsicht drängt. Die im Grundgesetz verankerte Kompetenzaufteilung zwischen Bund und Ländern wird hierfür schrittweise ausgehöhlt. Festlegungen des EU-Gesetzgebers werden ignoriert.

Die entscheidende politische Frage ist, ob die Länder das mitmachen wollen. Im Ergebnis verlören sie beträchtlich an Mitgestaltungsmöglichkeiten und würden ihre eigenen Landesverwaltungen der Aufsicht einer einzigen Bundesbehörde unterwerfen. Wenn die Länder bereit sind, diese Verantwortung abzugeben, wofür es z.B. fiskalische Gründe geben kann, wäre das natürlich zu akzeptieren. Aber mir scheint die Frage bisher nicht im Sinne einer strategischen Gesamtschau beantwortet zu werden: Weil Bundesgesetze diese Kompetenzordnung scheibchenweise bearbeiten und die Reaktionen der Länder bisher rein reaktiv in späten Stadien der Bundesratsbefassung erfolgen, fehlt es an der Grundsatzdebatte über die Zukunft der föderalen Ordnung im Digitalen. Der Zeitpunkt dafür ist jetzt!

Einheitliche Digitalaufsicht: Ein föderaler 3-Punkte-Plan

Zentralisierung ist weder für die Bürger:innen noch für die Verwaltung und jedenfalls nicht für den Mittelstand und die kleinen Unternehmen am Ende eine gute Lösung. Statt von einer (jedenfalls für lange Zeit erstmal) im Aufbau befindlichen Bundesbehörde abhängig zu sein, längere Entscheidungswege und Doppelstrukturen zu riskieren, braucht es ein Umdenken. Hierfür ist es zentral, dass der Bund (nur) die Aufgaben wahrnimmt, die bundesweit erfüllt werden müssen: z.B. Kontaktstelle zur EU, Zertifizierung nationaler KI-Produkte etc. Die regionale Marktüberwachung, Beratung der öffentlichen Stellen, Beschwerdebearbeitung sowie der Kontakt zu Unternehmen und Bürger:innen müssen weiterhin dort stattfinden, wo sie vor Ort gebraucht werden.

Das eigentliche inhaltliche Ziel ist doch ein gemeinsames: Rechtssicherheit durch einheitliche Auslegung und weniger Bürokratie durch einfachere Verfahren mit klaren Zuständigkeiten. Hierzu benötigen wir in der Tat eine verbindlichere, übergreifende Zusammenarbeit der Aufsichtsbehörden.

Dafür steht dieser 3-Punkte-Plan zur Modernisierung der föderalen Zusammenarbeit in der Digitalaufsicht:

1. **Ein Ansprechpartner für Unternehmen und Forschende**
   - Zentrale Zuständigkeit einer Aufsichtsbehörde bei länderübergreifenden Sachverhalten, z.B. bei Forschungsprojekten oder bei Konzernen mit mehreren Standorten

2. **Effiziente Arbeitsteilung durch Ausweitung des Einer-für Alle (EfA) – Prinzips**
   - Anwendung des EfA-Prinzips auf die Datenschutzbehörden
   - Ergebnis der Prüfung eines bundesweit eingesetzten Verfahrens durch eine Behörde bindet die anderen Behörden

3. **Eine starke Stimme, die einheitlich entscheidet**
   - Die Datenschutzkonferenz (DSK) durch Institutionalisierung zum gemeinsamen Entscheidungsgremium von Bund und Ländern formen
   - Rechtssicherheit durch Mehrheitsentscheidungen in der DSK schaffen, die BfDI und Landesdatenschutzbehörden binden

Der 3-Punkte-Plan bietet einen Weg zur digitalen Transformation, der die föderalen Stärken nutzt statt aufgibt: Feste Zuständigkeiten schaffen die nötige Orientierung in der Digitalwirtschaft, während die Expertise der Länder genutzt wird. Das Einer-für-Alle-Prinzip ermöglicht bundesweit einheitliche Standards. Verbindliche Mehrheitsentscheidungen schaffen Rechtssicherheit. Dies könnte noch ergänzt werden durch verbindliche Fristen für die Durchfüh-

rung von Standardprüfungen und die Beantwortung von Datennutzungsanfragen, wie im Gesundheitsdatennutzungsgesetz angelegt.

Die hierfür notwendige Anpassung des Bundesdatenschutzgesetzes in der kommenden Legislaturperiode ist der nächste Schritt. Entscheidend ist aber der politische Wille der Länder, ihre Kompetenzen zu nutzen. Denn nur so schaffen wir, was eine neue Zentralbehörde alleine nicht leisten kann: Die Verbindung von bewährten Strukturen und innovativen Prozessen – für eine dynamische und rechtssichere Digitalwirtschaft.

PRÜFUNGEN II.

Prüfungen

1. Kontrolle der Antiterror- und Rechtsextremismusdateien beim Verfassungsschutz

Der HmbBfDI hat beim Landesamt für Verfassungsschutz Hamburg (LfV) im Berichtszeitraum eine Vor-Ort-Prüfung der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) durchgeführt. Es wurde stichprobenhaft die Speicherung von einzelnen Personen auf Plausibilität und Schlüssigkeit in den Dateien überprüft. Bei beiden Dateien konnten keine Mängel erkannt werden, die Prüfung führte somit nicht zu Beanstandungen.

Anlass für die vom HmbBfDI durchgeführte Prüfung waren die gesetzlichen Vorgaben, die vorschreiben, dass mindestens alle zwei Jahre eine Überprüfung des Datenbestands durch die Datenschutzaufsicht zu erfolgen hat. Damit ist der Gesetzgeber wiederum den Vorgaben des Bundesverfassungsgerichts gefolgt (vgl. BVerfG, Urt. v. 24.4.2013 – Az. 1 BVR 1215/07). Das Verfassungsgericht hatte bezüglich dieser Dateien festgestellt, dass der Individualrechtsschutz der dort gespeicherten Personen nur schwach ausgestaltet sei, was eine Kompensation im Wege der aufsichtsrechtlichen Kontrolle erforderlich mache. Der institutionalisierten Kontrolle in angemessenen Abständen komme daher eine besondere Bedeutung zu (BVerfG a.a.O, Rn. 217). Bei der nunmehr durchgeführten Prüfung handelt es sich bereits um die vierte Prüfung der fraglichen Dateien beim LfV durch den HmbBfDI (vgl. zu vorherigen Prüfungen: Tätigkeitsbericht Datenschutz 2022, S. 32; 2020, S. 60 und 2016/2017 S. 26)

Sowohl bei der ATD als auch der RED handelt es sich um gemeinsame, standardisierte und zentrale Dateien, die jeweils von verschieden Sicherheitsbehörden des Bundes sowie der Landeskriminalämter und der Verfassungsschutzbehörden der Länder, die zentral beim Bundeskriminalamt geführt werden. 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 (RED-G)). 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, liegt bei der Behörde, die die Daten eingegeben hat (vgl. § 9 Abs. 1 Satz 1 RED-G bzw. § 8 Abs. 1 Satz 1 ATDG).

Der HmbBfDI hat sich in diesem Turnus insbesondere auf die Einhaltung der Speichervoraussetzungen bei einzelnen Betroffenen konzentriert. Ausgewählt wurden die zu prüfenden Individuen z.B. nach Dauer der Speicherung oder/und nach Datum des letzten Erkenntnisgewinns. Die Speicherung aller geprüften Betroffenen in den Dateien war jeweils nachvollziehbar und schlüssig. Die gesetzlichen Voraussetzungen der Speicherungen lagen vor. Verstöße gegen Bestimmungen des Datenschutzes konnte nicht festgestellt werden. Aufgrund des Geheimhaltungsgrads sind detaillierte Ausführungen über den Inhalt der Dateien im Rahmen dieses Tätigkeitsberichts leider nicht möglich.

Ähnlich wie der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) gelangt der HmbBfDI im Rahmen seiner Prüfung aber erneut zu dem Schluss, dass andere Kommunikationswege und Kooperationsformen in der Praxis mehr Relevanz bei der Arbeit der Sicherheitsbehörden aufweisen dürften als die ATD und die RED (ebenso BfDI 31. Tätigkeitsbericht zum Datenschutz, 2022 S. 93).

2. Videoüberwachung Hachmannplatz (beim Hauptbahnhof)

Seit August 2024 wird der Hachmannplatz vor dem Hamburger Hauptbahnhof von der Polizei Hamburg videoüberwacht. Der HmbBfDI hat sich vor Inbetriebnahme der Kameras vor Ort einen Überblick über die Maßnahme verschafft und die Einhaltung der gesetzlichen Voraussetzungen überprüft.

Bereits im Jahr 2023 setzte die Polizei Hamburg den HmbBfDI davon in Kenntnis, dass die Installation und Inbetriebnahme einer Videoüberwachungsanlage am Hachmannplatz geplant sei. Der Hachmannplatz befindet sich im Stadtteil St. Georg an der Nordseite des Hamburger Hauptbahnhofs. Während für die öffentliche Sicherheit im Hauptbahnhof die Bundespolizei zuständig ist, liegt die gefahrenabwehrrechtliche Zuständigkeit für den Hachmannplatz dagegen bei der Landespolizei Hamburg. Diese installierte im Berichtszeitraum dort insgesamt 27 – teils schwenk-, neig- sowie zoombare – Kameras an verschiedenen Standorten.

Nach umfangreicher datenschutzrechtlicher Prüfung kommt der HmbBfDI zu dem Ergebnis, dass die Voraussetzungen für eine Videoüberwachung des Hachmannplatz durch die Polizei Hamburg gegeben sind:

Grundsätzlich greift eine anlasslose Videoüberwachung wie diese in die Grundrechte aller Betroffenen ein. Bei den Betroffenen einer anlasslosen Videoüberwachung handelt es sich ganz überwiegend um Passanten und Besucher, von denen keine Gefahr ausgeht und die keinen Anlass für die Videoüberwachung gegeben haben. Der Einsatz von Videokameras durch die Polizei zum Zwecke ihrer gesetzlichen Aufgabenerfüllung bedarf einer Eingriffsermächtigung in Form einer gesetzlichen Grundlage. Im Bereich Hachmannplatz stützt die Polizei die Datenverarbeitung in Form einer präventiven Videoüberwachung

auf Grundlage von § 18 Abs. 3 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG). Danach 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 begangen worden sind und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung derartiger Straftaten zu rechnen ist (sogenannte offene präventive Videoüberwachung). Es muss sich bei dem überwachten Gebiet also im Vergleich zu anderen Teilen der Stadt um einen sog. Schwerpunkt der Straßenkriminalität handeln. Zudem muss die Polizei eine negative Prognose für die weitere Entwicklung der Kriminalitätslage erstellen. Die Videoüberwachung von Gebäuden, Gebäudeteilen und Flächen, die zwar öffentlich zugänglich sind, aber nicht zu den öffentlichen Straßen, Wege und Plätzen gehören (sog. Private Zones) ist davon nicht erfasst. Die Polizei Hamburg muss daher durch eine entsprechende Ausrichtung der Kamera oder eine Verpixelung sicherstellen, dass insbesondere keine Hauseingänge und Fenster von Wohngebäuden oder Geschäftsräumen überwacht werden. Durch das Überwachen von z.B. Eingangsbereichen ist der Übergang zum Privatbereich der gefilmten Personen betroffen. Auf diese Weise könnten 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.

Der HmbBfDI ist im Rahmen seiner Prüfung aufgrund der vorgelegten Fallzahlen und Lageanalysen 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 i.S.d. § 18 Abs. 3 PolDVG.

Im Rahmen der am 25.7.2024 ebenfalls erfolgten Vorort-Prüfung sowohl im Polizeikommissariat 11 als auch bei den konkreten Kamera-

standorten hat sich der HmbBfDI zudem einen Überblick über die Maßnahme verschafft. Dabei ging es insbesondere darum zu prüfen, ob die Videoüberwachung auch tatsächlich auf öffentlich zugängliche Orte i.S.d. Norm beschränkt wurde z.B. durch Filter und/oder Ausrichtung. Von einer ausreichenden Unkenntlichmachung konnte sich der HmbBfDI stichprobenhaft überzeugen. Es konnte dabei auch festgestellt werden, dass im Rahmen der Zoom- bzw. Schwenkbetätigung die vorgenannten Private Zones nicht von der Videoüberwachung erfasst wurden. Ausreißer oder Fehlprogrammierungen waren nicht feststellbar. Auch konnte vor Ort festgestellt werden, dass auf die Videoüberwachung seitens der Polizei Hamburg für die Bürger:innen angemessen hingewiesen wurde und die Verantwortlichkeit der Polizei Hamburg hinreichend erkennbar ist.

Nachbesserungsbedarf wird auch weiterhin bei der Umsetzung von technisch-organisatorischen Maßnahmen im Rahmen der Ausgestaltung der gesetzlichen Protokollierungspflicht gesehen. Die Polizei Hamburg hatte bereits im Rahmen von vorherigen Projekten den Einsatz eines ein neues Video-Managementsystem (VMS) Ende 2024 angekündigt, welches u.a. auch für die polizeilichen Videoüberwachungssysteme eine revisionssichere Protokollierung vornehmen soll. Bedauerlicherweise musste der Produktivbetrieb erneut verschoben werden.

3. Prüfung von personengebundenen Hinweisen bei der Polizei

Im Berichtszeitraum hat der HmbBfDI seine bereits im Jahr 2023 begonnene Prüfung von sog. personenbezogenen Hinweisen (PHW) bei der Polizei Hamburg abschließen können. Neben einzelnen Mängeln führten die vom HmbBfDI durchgeführten stichprobenhaften Überprüfungen von einzelnen Personen auch zur Identifikation eines grundsätzlichen Problems bei der Vergabe des PHW „Betäubungsmittelkonsument“ durch die Polizei Hamburg. Als Reaktion auf die Prüfung hat die Polizei bereits umfassende Maßnahmen eingeleitet.

Im Jahr 2024 setzte der HmbBfDI seine 2023 begonnene Prüfung einzelner konkreter Speicherungen von Personen im Polizeilichen Auskunftssystem (POLAS) der Polizei Hamburg fort. POLAS dient der Gefahrenabwehr, einschließlich der vorbeugenden Bekämpfung von Straftaten, und der Aufklärung von Straftaten durch den örtlichen Kriminalaktennachweis, durch örtliche Hinweise und Suchvermerke, den Nachweis von festgenommenen Personen und Fallinformationen. POLAS ermöglicht u.a. den Zugang zu den Kriminalakten und den schnellen Zugriff auf personenbezogene Sofortauskünfte. Voraussetzung für die Speicherung einer Person in POLAS ist, dass gegen diese ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist und dabei wegen der Art, Ausführung oder Schwere der Tat die Besorgnis der Begehung weiterer Straftaten besteht (vgl. § 36 Abs. 2 Gesetz über die Datenverarbeitung der Polizei (PolDVG)).

Aufgrund der Masse der Speicherung von Personen in der polizeilichen Datenbank POLAS, wurde als Ansatzpunkt für eine Stichprobe die Kontrolle von ausgewählten PHW gewählt. PHWs sind Hinweise auf Besonderheiten einer natürlichen Person, wie z.B. „Gewalttätig" oder „Bewaffnet", die bei Abruf einer Person im bundesländerübergreifenden Informationssystem der Polizei (INPOL) und/oder in POLAS gut sichtbar und hervorgehoben angezeigt werden. Diese Warnhinweise sollen ausschließlich dem Schutz des Betroffenen und/oder der Eigensicherung von Polizeibediensteten zur Einschätzung der Gefahrensituation dienen. Der Sinn liegt nicht lediglich in einem Hinweis auf gegebenenfalls vorliegende Vorstrafen. Dabei sind die PHW allen Beamt:innen zugänglich, die Zugriff auf POLAS bzw. INPOL haben.

Aufgrund der besonderen Sensibilität der Daten, der potenziell stigmatisierenden Wirkung und letztlich auch der Gefahr einer zweckentfremdeten Vergabe durch die Polizei wurde vom Bundeskriminalamt (BKA) für die Vergabe der PHW ein bundeseinheitlicher Leitfaden vorgegeben, um eine einheitliche Einschätzung von Gefahrensituationen für die Betroffenen und die einschreitenden Polizeibediensteten zu gewährleisten. Dieser Leitfaden beinhaltet eine Auflistung der

Kategorien von PHW und zu jedem PHW die Vergabekriterien (sog. Zugangskriterien). Ziel der Prüfung des HmbBfDI war es, die Erfüllung der gesetzlichen Voraussetzungen (vgl. § 34 Abs. 6 PolDVG) und der erwähnten Zugangskriterien für die Eintragung der PHW zu überprüfen. Der HmbBfDI hat sich in einem ersten Schritt entschieden, dies anhand der vergebenen PHW „Psychische und Verhaltensstörung", „Gewalttätig" und „Betäubungsmittelkonsument" zu kontrollieren. Durch die Polizei Hamburg wurde für den HmbBfDI zunächst eine Liste derjenigen Personen erstellt, die in POLAS mit den genannten drei PHW hinterlegt sind. Aus diesen ca. 8.700 Einträgen wurde zunächst eine Stichprobe von rund 1% gebildet. Dabei handelte es sich um 89 Personen mit insgesamt 145 PHW-Einträgen.

In einem Vor-Ort-Termin am 23.4.2024 wurde zunächst in die Datensätze von 33 Personen Einsicht genommen. Aufgrund mehrfacher PHW konnten damit insgesamt 54 PHW-Einträge auf Ihre Rechtmäßigkeit hin überprüft werden. Im Hinblick auf 34 der geprüften 54 Einträge bestanden aus Sicht des HmbBfDI keine Bedenken an der Erfüllung der o.g. Rechtmäßigkeitsvoraussetzungen. Insbesondere die Einträge zum PHW „Gewalttätig" erwiesen sich insoweit als unproblematisch. Für die PHW „Gewalttätig" sind die Voraussetzungen, dass die Person bei der Begehung einer Straftat erhebliche Gewalt gegen Personen oder Sachen, insbesondere bei Widerstandshandlungen, eingesetzt hat, oder bei zukünftigen Straftaten, erhebliche Gewalt gegen Personen oder Sachen einsetzen wird. Diese Voraussetzungen konnte in allen vom HmbBfDI kontrollierten Fällen von der Polizei nachgewiesen werden.

Bei acht Einträgen (zu sechs Personen) reichten aber die digital verfügbaren Unterlagen im Ergebnis nicht aus, um die Prüfung durch den HmbBfDI vor Ort abschließen zu können. Dies betraf überwiegend das PHW „psychische und Verhaltensstörung". Für den PHW „psychische und Verhaltensstörung" ist erforderlich, dass eine ärztliche Feststellung der psychischen Erkrankung in schriftlicher Form vorliegt und aus dieser Erkrankung eine Gefahr für den Betroffenen selbst oder andere, insbesondere Polizeibedienstete besteht. In

einigen Fällen konnte die für die Eintragung notwendige ärztliche Einschätzung aber in Form von Gutachten oder Gerichtsentscheidungen direkt digital eingesehen werden. In der überwiegenden Zahl der Fälle war in ausreichendem Maße dokumentiert (Aktenzeichen oder Kurzvermerk zur Art des Dokuments), wo die entsprechenden Informationen in Papierform auffindbar sind.

Als problembehaftet erwiesen sich allerdings weit überwiegend die überprüften Speicherungen des PHW „Betäubungsmittelkonsument". Zwar enthielten alle Fälle Hinweise auf einen Betäubungsmittelkonsum und/oder Handel. Dies ist für die Vergabe des PHW nach dem BKA-Leitfaden aber nicht ausreichend. Vielmehr muss aus dem Konsum eine nicht unerhebliche Gesundheitsgefahr für ihn selbst oder für andere, insbesondere Polizeibedienstete, folgen. Dies bedeutet, dass ein PHW z.B. zulässig ist, wenn es u.a. darum geht, dass Polizeibedienstete davor geschützt werden sollen, bei Durchsuchungen auf verunreinigte Konsumutensilien, vor allem Spritzen, zu treffen und sich dabei zu verletzen und einem Ansteckungsrisiko ausgesetzt zu sein. Hingegen ist ein Eintrag unzulässig, wenn bei der Person lediglich Betäubungsmittel gefunden wurden, die geschluckt oder geraucht werden. Die erforderliche, aus dem Konsum resultierende Gefährlichkeit war weder erkennbar noch schien dies überhaupt bei der Vergabe Beachtung gefunden zu haben. In elf Fällen wurde daher durch den HmbBfDI die Löschung der PHW angeregt, hilfsweise die Erläuterung der Rechtmäßigkeit erbeten.

Im Ergebnis wurde in 14 der 19 vom HmbBfDI normierten Fälle eine Löschung der PHW von der Polizei vorgenommen und in drei Fällen kurzfristig nachvollziehbar nachdokumentiert.

In einem Anschlusstermin im Polizeipräsidium am 25.9.2024 wurde durch den HmbBfDI bei weiteren 60 Personen Einsicht in die Datensätze genommen. Ziel des Termins war es nunmehr zum einen, auch solche Speicherungen des Eintrags „psychische und Verhaltensstörung" zu prüfen, die an Personen vergeben wurden, die nicht auch gleichzeitig den PHW „Gewalttätig" zugeordnet haben. Für

diese Gruppe ist die Eintragung besonders stigmatisierend und der notwendige Gewaltbezug der psychischen Störung ggf. nicht so offensichtlich wie bei Personen mit Doppeleintragung. Dabei wurden im Nachgang von der Polizei drei der acht überprüften Datensätze gelöscht, aufgrund fehlenden Aktenrückhaltes. Der Prüfungsschwerpunkt im zweiten Durchgang wurde aber insbesondere auf die Eintragung „Betäubungsmittelkonsument" gelegt, nachdem die erste Stichprobe im April 2024 hier auf eine womöglich fehlerhafte Eintragungspraxis (Vergabe für reinen Konsum ohne Gefährdung) hindeutete. Ansatz der Prüfung war zunächst, durch die Bildung von Stichproben aus verschiedenen Jahrgängen eine Eingrenzung des Problembereichs zu erreichen. Nach übereinstimmender Bewertung ist dies nicht gelungen. Vielmehr zeigte sich, dass über alle Jahrgänge hinweg und unabhängig von der Quelle der Einträge erhebliche Defizite festzustellen waren. Lediglich ganz vereinzelt ließen es die polizeilichen Dokumentationen zu, einem vorhandenen Drogenkonsum auch in Beziehung zu einer – nach dem Leitfaden des BKA – erforderlichen Eigengefährdung oder Fremdgefährdung für eingesetzte Beamt:innen zu setzen. Dies erschien allerdings eher zufällig.

Die eingesehenen Fälle verstärkten vielmehr den Eindruck, dass der PHW „Betäubungsmittelkonsum" von ganz überwiegenden Teilen der eintragenden Personen als Kennzeichnung für reine Konsumenten missverstanden wird oder fehlerhaft auch für BTM-Händler vergeben wird. Beide Stichproben deuteten damit auf ein grundsätzliches Problem bei der Polizei Hamburg hin, welches nach Ansicht des HmbBfDI über die erforderliche Berichtigung von (geprüften) Einzelfällen hinausging und vielmehr ein generelleres Handeln der Polizei in zwei zeitliche Richtungen erforderlich machte: So wurde mit hoher Dringlichkeit für die Zukunft durch technische und organisatorische Maßnahmen ein höherer Qualitätsgrad bei der Eintragung des PHW „Betäubungsmittelkonsument" gefordert. Insbesondere ist dafür zu sensibilisieren, dass dieser PHW entgegen der irreführenden Bezeichnung als „Betäubungsmittelkonsument" eben mehr als den reinen Konsum von Betäubungsmitteln voraussetzt, nämlich eine Eigen- oder Fremdgefährdung in Zusammenhang mit dem Konsum.

Notwendig erscheint nach dem bisherigen Gesamteindruck auch ein Ansetzen schon in der Ausbildung, aber auch in (Nach-)Schulung, um ein Problembewusstsein in der Breite der Datenbank-Anwender:innen zu schaffen. Denkbar wären auch technische Maßnahmen in Form von eindeutigen Hinweisen, Ausfüllhilfen oder Ankreuzmöglichkeiten (Drogenkonsum sowie hierdurch verursachte Eigen- und Fremdgefährdung). Zudem ist die Polizei aber auch gehalten, umfassende Datenbestände aus der Vergangenheit zu sichten. Im Hinblick auf die Masse der Einträge stellt dies eine besondere Herausforderung dar.

Im Dezember 2024 teilte die Polizei mit, erste Schritte ergriffen zu haben. Erste Maßnahmen zur Sensibilisierung des Vollzugs in Form von Gesprächen und Informationsemails sind danach erfolgt. Ein Informationsschreiben, welches insbesondere detaillierte Vorgaben zur Pflichtbegründung bei der Vergabe der PHW macht, ist in Vorbereitung. Zudem werde darauf hingewirkt, in den bestehenden Aus- und Fortbildungseinheiten zu POLAS deutlicher auf die Besonderheiten zur PHW-Vergabe hinzuweisen.

Besonders erfreulich ist aber, dass die Polizei Hamburg mitgeteilt hat, im Hinblick auf 1.300 Eintragungen zum PHW „Betäubungsmittelkonsument“ eine Löschung vorzubereiten. Dies betrifft Einträge vor dem Jahr 2017. Weitere noch bestehende ca. 1.300 PHW „Betäubungsmittelkonsument“ müssen noch einzeln auf das Vorliegen der Voraussetzungen überprüft werden. Zudem hat die Polizei insgesamt ca. 50 Datensätze mangels Aktenrückhalts gelöscht.

4. Mitarbeiterexzesse im Gesundheitsbereich

Immer wieder einmal erhält der HmbBfDI Hinweise oder Beschwerden dazu, dass einzelne Mitarbeiter:innen von Gesundheitseinrichtungen zu privaten Zwecken Zugriff auf Daten von in der Einrichtung behandelten Personen nehmen. Einen solchen Fall hatte der HmbBfDI in 2023 an die Staatsanwaltschaft Hamburg abgegeben und Strafantrag gemäß § 42 Abs. 3 BDSG gestellt. Im Berichtsjahr hat die Staatsanwaltschaft den HmbBfDI darüber informiert, dass der Erlass eines Strafbefehls beantragt wurde.

Zusätzlich zu den nach der Datenschutz-Grundverordnung (DSGVO) vorgegebenen Sanktionsmöglichkeiten ist in Art. 84 DSGVO vorgesehen, dass die Mitgliedstaaten weitere Sanktionen für Verstöße gegen die DSGVO einführen. Der deutsche Gesetzgeber hat das in Form des § 42 Bundesdatenschutzgesetz (BDSG) getan. Danach wird die gewerbsmäßige Offenlegung von großen Beständen personenbezogener Daten unter Strafe gestellt (Abs. 1). Gleiches gilt für die unbefugte Verarbeitung nicht allgemein zugänglicher personenbezogener Daten bzw. deren Erschleichen mit Bereicherungs- oder Schädigungsabsicht (Abs. 2). Eine solche Schädigungsabsicht in Form einer Rufschädigung, Bloßstellung oder Ehrverletzung sah der HmbBfDI in einem Fall, in dem eine in einem Krankenhaus in Hamburg beschäftigte Person Daten von Patient:innen – Namen sowie Informationen zu Erkrankungen/Diagnosen – in einem chinesischen sozialen Netzwerk veröffentlicht und im Text dazu herabsetzende, auf die Diagnosen bezogene Angaben gemacht hatte. Die Informationen zu den Patient:innen stammten dabei aus dem Krankenhausinformationssystem. Der HmbBfDI sah daher Anhaltspunkte für das Vorliegen einer Straftat nach § 42 Abs. 2 BDSG und sich gemäß § 41 Abs. 1 Gesetz über Ordnungswidrigkeiten veranlasst, den Vorgang an die Staatsanwaltschaft abzugeben. Da die Tat nur auf Antrag verfolgt wird und u.a. die Aufsichtsbehörde nach § 42 Abs. 3 BDSG

antragsberechtigt ist, hat er einen entsprechenden Strafantrag gestellt. Das hat die Staatsanwaltschaft dazu veranlasst, den Erlass eines Strafbefehls zu beantragen.

In den Fällen, in denen Beschäftigte entgegen der Weisungen und Interessen ihrer Arbeitgeber sensible Gesundheitsdaten verarbeiten, stellt sich regelmäßig die Frage, ob dies den Arbeitgebern zugerechnet werden kann. Das ist grundsätzlich dann nicht der Fall, wenn – wie eindeutig bei der Veröffentlichung von Patien:innendaten auf einer Social-Media-Plattform – eine beschäftigte Person mit der Datenverarbeitung eigene Zwecke verfolgt, die nicht den ihr zugewiesenen Aufgaben entspricht, und nicht ausnahmsweise von einer Billigung durch die Geschäftsleitung ausgegangen werden kann. In einem weiteren Vorgang ging es darum, zu signalisieren, dass ein bestimmtes Verhalten von Mitarbeiter:innen nicht toleriert wird. In jener Sache ist der HmbBfDI aufgrund eines Hinweises auf eine während der Arbeitszeit aus den Räumlichkeiten eines Krankenhauses streamende, dort beschäftigte Person an die Klinik herangetreten. Hier konnte zwar kein Datenschutzverstoß, z.B. durch die Offenlegung von Daten von Patient:innen, festgestellt werden. Das Krankenhaus hat den Vorgang aber zum Anlass genommen, in die Hausordnung noch einmal ausdrücklich ein Verbot von Streamings während der Arbeitszeit aufzunehmen.

5. Diebstahl von Festplatten aus zwei Arztpraxen

Ein Täter ist in zwei Arztpraxen eingedrungen und hat Festplatten mit Patientendaten entwendet. Der HmbBfDI hat dafür gesorgt, dass die Betroffenen umfassend über den Vorfall informiert wurden.

Zwei zum selben Träger gehörende Arztpraxen sind Opfer eines Diebstahls geworden. Ein Täter hat außerhalb der Geschäftszeiten die Praxisräume unberechtigt betreten und gezielt die Festplatten ausgebaut und entwendet, auf denen sich die Daten der

Patient:innen befanden. Der Fall ist mittlerweile aufgeklärt und die Speichermedien sind zurückgegeben worden. Die Untersuchung der Hintergründe des Vorfalls oblag dabei der Polizei. Ist eine mögliche Datenschutzverletzung zugleich eine Straftat, ist die Strafverfolgung vorrangig zu betreiben. Hier greift das Verbot der Doppelbestrafung, sodass dieselbe Tathandlung nur einmal sanktioniert werden kann. Die möglichen Ordnungswidrigkeitstatbestände der DSGVO treten dann hinter den Tatbeständen des Strafgesetzbuchs zurück, solange ein polizeiliches bzw. staatsanwaltschaftliches Ermittlungsverfahren läuft.

Gleichwohl bestehen auch in diesen Fällen Meldepflichten gegenüber dem HmbBfDI im Rahmen des Art. 33 DSGVO. Sind infolge eines Sicherheitsbruchs personenbezogene Daten durch Unberechtigte eingesehen oder entwendet worden, ist dies der Datenschutzbehörde binnen 72 Stunden mitzuteilen, wenn ein Risiko für die Rechte und Freiheiten der Betroffenen besteht. Der HmbBfDI hat dafür ein Meldeformular auf seiner Internetseite eingerichtet. Eine solche Meldung hat der Betreiber der Arztpraxen auch rechtzeitig vorgenommen. Da die Motivation des Täters zunächst völlig unklar war, er jedoch gezielt die Datenspeicher entfernt hat, musste von einem Missbrauchsrisiko ausgegangen werden.

Neben der Aufsichtsbehörde sind auch die Betroffenen zu informieren, wenn nicht nur ein einfaches, sondern ein hohes Risiko besteht. Das Risiko bemisst sich in der Gesamtschau aus dem möglichen Schaden und dessen Eintrittswahrscheinlichkeit. Aufgrund der hohen kriminellen Energie war von unredlichen Absichten auszugehen. Der Umfang der erbeuteten, sehr sensiblen Daten führte ebenfalls zu dem Schluss einer hohen Wahrscheinlichkeit invasiver Datenschutzverletzungen. In der Rückschau des ausermittelten Falls ist nicht mehr davon auszugehen, dass es zu Datenmissbrauch gekommen ist. Zum Zeitpunkt der Meldepflicht war dies jedoch noch unklar. Die Arztpraxen stellten proaktiv Transparenz her durch Anfertigung eines Informationsschreibens, das den Patient:innen beim nächsten Besuch ausgehändigt wurde.

Dem HmbBfDI reichte diese sukzessive Information jedoch nicht aus. Es kann nicht davon ausgegangen werden, dass die Mehrzahl der Patient:innen sich kurzfristig in den Praxen persönlich vorstellt, zumal in den Einrichtungen auch spezialisiertes fachärztliches Personal tätig ist. Er hat daher nachdrücklich auf eine öffentliche Information hingewirkt. In der Folge haben die beiden Praxen ausführliche und adressatengerechte Informationstexte an zentraler Stelle ihrer Internetseiten veröffentlicht.

Dem HmbBfDI genügte diese an die Allgemeinheit gerichtete Transparenz. Im konkreten Fall konnte von einer individuellen Kontaktaufnahme mit allen Patient:innen, deren Daten betroffen waren, abgesehen werden. Art. 34 Abs. 3 lit. c) DSGVO erlaubt die zentralisierte, öffentliche Information, wenn Einzelbenachrichtigungen einen unverhältnismäßigen Aufwand darstellen würden. Diese Ausnahme legt der HmbBfDI eng aus, hat sie aber hier akzeptiert. Ein gewichtiges Argument war dabei die sechsstellige Anzahl an Patient:innen, für die in der Regel keine elektronische Kontaktmöglichkeit vorgelegen hat. Der HmbBfDI hat zudem die Tatsache, dass es sich um Arztpraxen handelte, in die Abwägung einbezogen. Wäre beispielsweise ein Unternehmen betroffen gewesen, dessen Geschäftszweck die intensive Verarbeitung personenbezogener Daten ist, wäre die ggf. postalische Einzelbenachrichtigung notwendig gewesen. Dasselbe würde in der Regel für Großunternehmen gelten, von denen ein erhöhter Grad an Professionalität und Compliance zu erwarten ist.

6. Prüfung des Onlinedienstes „Hinweise auf Verstöße im Rahmen der Geldwäscheaufsicht mitteilen (Whistleblower-System)“

Die Umsetzung des Onlinezugangsgesetzes (OZG) in der FHH wird durch den HmbBfDI begleitet. Einzelne Onlinedienste umfassen dabei abweichend von den übrigen Verfahren umfangreichere Systeme, wie der Onlinedienst zur Meldung von Verstößen gegen Vorschriften des Geldwäschegesetzes.

Durch Geldwäsche werden organisierte Kriminalität und Terrorismus finanziert. Berufsgruppen wie Immobilienmakler, Versicherungsvermittler, Kunstvermittler, Buchmacher und Lohnsteuerhilfevereine sind gefährdet, für Geldwäsche und Terrorismusfinanzierung missbraucht zu werden. Das Geldwäschegesetz (GwG) sieht in § 53 GwG vor, dass die Aufsichtsbehörden für diese Berufsgruppen ein Meldesystem zur Annahme von Hinweisen durch hinweisgebende Personen („Whistleblower“) zu Verstößen gegen die Vorgaben des Geldwäschegesetzes errichten, wobei das System die Abgabe von Hinweisen über einen geschützten Kommunikationsweg ermöglichen soll und Hinweise auch anonym abgegeben werden können.

Die FHH hat für diese Vorgabe einen Onlinedienst auf Basis einer Drittanbieterlösung geschaffen, den nach dem Einer-für-Alle-Prinzip (EfA) auch andere Behörden anderer Bundesländer nutzen können. Über diesen Dienst können hinweisgebende Personen Meldungen über Verstöße gegen das Geldwäschegesetz für die jeweilige Berufsgruppe abgeben und der Dienst leitet diese an die jeweils zuständige Stelle weiter. Wenn ein Hinweis über diesen Onlinedienst abgegeben wird, können bundesweit die zuständigen Aufsichtsbehörden für Geldwäscheaufsicht erreicht werden, die sich dem Onlinedienst angeschlossen haben. Dieser Onlinedienst übernimmt dabei nicht nur die Schnittstellenfunktion zu einem nachgelagerten Fachverfahren wie bei vielen vom HmbBfDI geprüften OZG-Onlinediensten, son-

dern beinhaltet selbst eine Fachverfahrenskomponente in Form einer Webanwendung mit eigenen Funktionen für Datenhaltung, -sichtung und -bearbeitung. Verantwortlicher für diesen Dienst ist die jeweils zuständige Stelle, d.h. die Fachbehörde mit der Aufgabe der Geldwäscheaufsicht. Die Behörde für Wirtschaft und Innovation (BWI) betreibt den Onlinedienst im Auftrag und ist aber auch selbst als Aufsichtsbehörde für die Einhaltung der Bestimmungen des Geldwäschegesetzes eine der zuständigen Stellen in der FHH und datenschutzrechtlich Verantwortliche.

Meldungen von hinweisgebenden Personen über Verstöße gegen das Geldwäschegesetz enthalten besonders sensible Daten über den Hinweisgebenden selbst und über die Person, der mögliche Gesetzesverstöße angelastet werden.

Die Datenschutzdokumentation wurde vom HmbBfDI sorgfältig geprüft. Aufgrund der Komplexität des Verfahrens forderte der HmbBfDI insbesondere Klarstellungen in Hinblick auf die Rolle der Behörde für Wirtschaft und Innovation (BWI) als Auftragsverarbeiter und als Verantwortliche.

Aufgrund der Regelungen des OZG-Änderungsgesetzes, das am 24.7.2024 in Kraft getreten ist, wird die datenschutzrechtliche Verantwortlichkeit bei Onlinediensten nunmehr in § 8a OZG gesetzlich geregelt. In dieser Hinsicht sind die vorgelegte Datenschutzdokumentation und Auftragsverarbeitungsverträge zu diesem Onlinedienst anzupassen. Hinsichtlich der dargelegten technischen und organisatorischen Maßnahmen wurden ebenfalls Nachschärfungen gefordert, da die Angaben dazu teilweise unvollständig oder nicht ausreichend konkret waren. So wurde eine Nachbesserung zur Gewährleistung der Anonymität der Hinweisgebenden gefordert, um eine Rückverfolgbarkeit der Hinweisgebenden z.B. durch deren Arbeitgeber auszuschließen. Des Weiteren wurden Nachbesserungen hinsichtlich der Authentifizierungsmaßnahmen für Hinweisbearbeiter der zuständigen Aufsichtsbehörden angeregt. Zudem wurde ein plausibles Verschlüsselungskonzept nachgefordert, da dies

nicht in konsistenter Form vorgelegt wurde. Weitere Hinweise und Anregungen des HmbBfDI bezogen sich u.a. auf die Mandantentrennung zwischen den zuständigen Aufsichtsbehörden sowie Speicherdauern und Löschfristen zu abgegebenen Meldungen durch hinweisgebende Personen.

Eine inhaltliche Rückmeldung auf die Hinweise des HmbBfDI steht noch aus. Der HmbBfDI wird sich auch im Jahr 2025 mit dem Onlinedienst befassen.

7. Prüfung von Bewerbermanagementsoftware (BMS) in Unternehmen

Mit der zunehmenden Verbreitung von Bewerbungsmanagementsoftware wachsen auch die Risiken für Bewerber:innen und spätere Mitarbeitende, insbesondere im Hinblick auf Datenschutz, Transparenz und Fairness. Der HmbBfDI hat daher im Berichtsjahr 2024 mit der Prüfung solcher Systeme begonnen, mit dem Ziel, dass beim Einsatz dieser Technologien die Grundsätze der DSGVO gewahrt bleiben.

Vor dem Hintergrund gemeldeter Datenpannen und Beschwerden im Zusammenhang mit Bewerbungsmanagementsystemen stellte sich heraus, dass bei der Frage nach einem datenschutzkonformen Einsatz in der Praxis die tatsächlichen Funktionsweisen und Module eine große Rolle spielen. Der HmbBfDI hat deshalb in 2024 damit begonnen, führende Softwarehersteller von Bewerbungsmanagementsoftware mit Sitz in Hamburg zu kontaktieren. Ziel hierbei war es, die genauen Einsatzmöglichkeiten und Funktionsweisen der Software zu verstehen. Datenschutzrechtlich interessant ist die Stellung eines Softwareherstellers deswegen, weil dieser oftmals nicht als „Verantwortlicher“ i.S.d. Art. 4 Nr. 7 DSGVO anzusehen ist, solange dieser die Software nicht mit Echtdaten betreibt. Die DSGVO definiert den Verantwortlichen als die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und

Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO). In der Praxis bedeutet dies, dass oftmals erst der Anwender der Software als Verantwortlicher gilt. Der Softwarehersteller hingegen ist in der Regel nicht der Verantwortliche, solange er weder Zweck noch Mittel der Datenverarbeitung letztverantwortlich festlegt, was z.B. der Fall wäre, wenn er die Software bei den eigenen Mitarbeitern einsetzen würde. In der späteren Vertragsgestaltung tritt der Hersteller oftmals als Auftragsverarbeiter gem. Art. 28 DSGVO gegenüber seinen Kunden auf und stellt auf diese Weise die Software als „Software as a Service" zur Verfügung.

Erfreulicherweise fanden sich Hamburger Unternehmen führender Bewerbungsmanagementsoftware, die bereit waren, ihre Softwarelösungen zu erläutern. Bei einer detaillierten Präsentation einer dieser Softwarelösungen wurden verschiedene kritische Aspekte erörtert wie die Methoden der Datenverarbeitung und -speicherung, Möglichkeiten zur automatisierten Datenauswertung sowie Implementierung technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO. Aber auch Aspekte wie die Informationspflichten und Verantwortlichkeiten wurden diskutiert.

Der Informationsaustausch diente ausdrücklich nicht einer formellen datenschutzrechtlichen Prüfung, sondern dem Verständnis der Softwarefunktionalitäten und potenzieller Risiken. Ziel war es, in potenziellen Beschwerdeverfahren gezieltere Untersuchungen zu ermöglichen, um potenzielle Schwachstellen sofort zu erkennen oder auf datenschutzfreundliche Einstellungen hinweisen zu können. Ebenfalls wurde auf diese Weise ein Fragenkatalog entwickelt, der auch genutzt werden soll, um zukünftige Verfahren zu optimieren.

Für das kommende Jahr ist im nächsten Schritt geplant, die Untersuchung auf Unternehmen auszuweiten, die diese Bewerbungsmanagementsoftware einsetzen. Hierbei sind auch anlasslose Prüfungen denkbar. Insbesondere im Zeitalter von KI-Anwendungen und einer Vielzahl digitaler Einsatzfelder soll auf diese Weise die weiterhin anwachsende Verarbeitung von Bewerberdaten überprüft werden.

8. Gastbestellungen im Onlinehandel

Im Regelfall muss im Onlinehandel die Möglichkeit zur Gastbestellung eingeräumt werden. Ausnahmen hiervon sind aber möglich, wenn dem Grundsatz der Datenminimierung auch auf andere Weise Rechnung getragen wird.

Die Datenschutzkonferenz (DSK), die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, hat mit Beschluss vom 24. März 2022 Hinweise zum datenschutzkonformen Onlinehandel mittels Gastzugang veröffentlicht. Danach müssen Verantwortliche im Onlinehandel ihren Kund:innen grundsätzlich einen Gastzugang für Bestellungen bereitstellen, unabhängig davon, ob sie auch die Möglichkeit eines registrierten Nutzungszugangs (fortlaufendes Kund:innenkonto) anbieten. Dieser Gastzugang ermöglicht es den Kund:innen, Bestellungen ohne Registrierung und ohne die Erstellung eines fortlaufenden Kontos vorzunehmen. Unter bestimmten Umständen sind allerdings Ausnahmen von diesem Grundsatz vorgesehen. In solchen Fällen muss jedoch dem Grundsatz der Datenminimierung Rechnung getragen werden, beispielsweise durch automatische Löschung inaktiver Konten.

Der HmbBfDI prüfte im Berichtszeitraum die Praxis eines großen Hamburger Versandhändlers. Es ging dabei um die Frage, ob es zulässig ist, Bestellungen ausschließlich über ein Kundenkonto zu ermöglichen und keinen Gastzugang anzubieten. Nach eingehender Prüfung entsprechender Unterlagen und Geschäftsdaten des Unternehmens gelangte der HmbBfDI zu dem Ergebnis, dass die Pflicht zur Bereitstellung eines Gastzugangs in diesem Fall nicht besteht.

Dem Ergebnis liegen folgende Gründe zugrunde, die sich aus den im DSK-Beschluss genannten Ausnahmemöglichkeiten ergeben:

1. Der Händler stellt einen Marktplatz für eine hohe Zahl angeschlossener Dritthändler bereit und hat ein berechtigtes Interesse daran, dass Bestellungen und nachgelagerte Kommunikations- und Bearbeitungsvorgänge (Gewährleistung, Garantie, Rücksendung) zentral verwaltet bzw. unmittelbar mit den Händlern geführt werden. Dies umfasst die Bereitstellung von Informationen und Self-Service-Funktionen im Kund:innenkonto, um Effizienzvorteile zu erzielen und die Kund:innen auf diese Informationen und Funktionen verweisen zu können. Der Händler hat im konkreten Fall ausführlich dargelegt, dass ein solcher Marktplatz nur mithilfe solcher Funktionen wirtschaftlich betrieben werden kann. Würden sämtliche Kundenanfragen durch den Kundendienst selbst verwaltet werden, einschließlich der Identifizierung der Kund:innen, der Prüfung des Vorgangs und die Weiterleitung an die jeweils zuständigen Händler, würde ein unwirtschaftlich hoher Zeit- und Ressourcenaufwand entstehen.

2. Bei der Erstellung eines Kund:innenkontos wird im Vergleich zu einer Gastbestellung lediglich das Passwort als zusätzliches Datum erhoben. Die Erhebung aller weiteren Angaben ist sowohl bei einer Gastbestellung als auch bei der Kontoerstellung datenschutzrechtlich unbedenklich, da sie für die Geschäftsabwicklung erforderlich sind oder im berechtigten Interesse des Unternehmens liegen. Das Unternehmen ist berechtigt, Informationen zu Bestellungen aufzubewahren, um die Kundenrechte (Gewährleistung, Garantie, Rücksendung) prüfen und erfüllen zu können. Zudem unterliegt das Unternehmen gesetzlichen Aufbewahrungsfristen aus dem Handels- und Gesellschaftsrecht, um die über den Marktplatz getätigten Geschäfte nachweisen zu können.

3. Um dem Grundsatz der Datenminimierung hierbei Rechnung zu tragen, bietet der Händler zwei Optionen: Zum einen können die Kund:innen ihr Kund:innenkonto nach Abwicklung der Bestellung manuell löschen zu lassen. Zum anderen erfolgt bei

längerer Inaktivität eine automatische Löschung des Kund:innenkontos. Durch diese Maßnahmen wird sichergestellt, dass die vom Händler verarbeiteten Daten letztendlich dem Umfang einer Gastbestellung entsprechen.

Das Landgericht Hamburg bestätigte in einem Urteil vom 22. Februar 2024 (Az. 327 O 250/22) diese Position des HmbBfDI, dass unter bestimmten Umständen die Pflicht zur Bereitstellung eines Gastzugangs entfallen kann. Obwohl das Gericht nicht an den Beschluss der DSK gebunden war, wurde dieser als „Soft Law" berücksichtigt. In seiner Entscheidung betonte das Landgericht Hamburg, dass das Prinzip der Datenminimierung nicht zwingend einen Gastzugang erfordert, sondern auch durch andere Maßnahmen gewährleistet werden kann. Das Gericht stellte fest, dass die Pflicht zur Einrichtung eines Kund:innenkontos für eine Bestellung nicht gegen das Gebot der Datenminimierung verstößt, wenn die notwendigen Daten nur für die Abwicklung des Vertrages erhoben und diese nach Ablauf der Aufbewahrungsfristen gelöscht werden oder Kund:innenkonten nach einer bestimmten Inaktivitätsperiode automatisch gelöscht werden. Diese Maßnahmen stellen sicher, dass die Datenverarbeitung im Einklang mit den datenschutzrechtlichen Vorgaben steht, insbesondere mit dem Grundsatz der Datenminimierung (Art. 5 Abs. 1. lit. c) DSGVO).

9. Transparenzanforderungen für den Versand von Bestandskundenwerbung per E-Mail

Die Verarbeitung von E-Mail-Adressdaten zum Zwecke der Direktwerbung an Bestandskunden für ähnliche Produkte sowie das diesbezügliche Widerspruchsrecht muss den Kunden:innen von den werbetreibenden Unternehmen bereits bei Erhebung der personenbezogenen Daten transparent dargelegt werden.

Im Rahmen seiner Aufsichts- und Kontrolltätigkeiten wurde der HmbBfDI im Juli 2024 durch eine Beschwerde auf die Ausgestaltung der Bestellmaske für die Registrierung oder Bestellung als Gast

im Online-Shop eines europaweit agierenden großen Online-Mode-Händlers aufmerksam gemacht.

Zu diesem Zeitpunkt lautete die Formulierung neben dem Feld, welches von den Kund:innen auf dem Online-Shop in dem Bestellformular nach der Eingabe ihres Vor- und Nachnamens, E-Mail-Adresse sowie Passworts angekreuzt werden kann, wie folgt:

> ☐ Ich möchte per E-Mail von dem Unternehmen über aktuelle Trends, Angebote und Gutscheine informiert werden.
> Jederzeit kostenlos abbestellen.
>
> [Button zur Verifizierung]
> [Button zur Registrierung]
>
> Wie bei jedem Online-Shop erhältst du von uns alle relevanten Bestellinformationen per E-Mail. Dazu gehören Auftragsbestätigung, Lieferbestätigung, Rücksendeinformationen, Empfehlungen).
> Du kannst die Empfehlungen jederzeit kostenlos abbestellen.
> [Verlinkung zur Datenschutzerklärung]

Obwohl die Kund:innen des Online-Mode-Händlers während des Bestellvorgangs beim Ausfüllen der Anmeldeinformationen das obere Feld nicht angekreuzt hatten, erhielten sie im Nachgang zu ihrer Bestellung regelmäßig Werbe-E-Mails mit Produktempfehlungen von dem Unternehmen über die Absender-E-Mail-Adresse newsletter@unternehmens-domäne.com.

Hierbei stellt sich die Schwierigkeit, dass die Verarbeitung personenbezogener Daten zu Zwecken der Direktwerbung per E-Mail gemäß Art. 6 Abs. 1 lit. a DSGVO i.V.m. § 7 Abs. 2 Ziff. 2 UWG grundsätzlich einer vorherigen Einwilligung der Werbeempfänger bedarf.

Lediglich die Verarbeitung von E-Mail-Adressen, die von den Unternehmen bei ihren Kund:innen im Rahmen einer Geschäftsbeziehung

erhoben wurden, kann auch über berechtigte Interessen der werbetreibenden Unternehmen nach Art. 6 Abs. 1 lit. f DSGVO legitimiert werden. Unter der Einhaltung der Vorgaben des § 7 Abs. 3 Ziff. 1 bis 4 UWG darf an solche Bestandkunden auch ohne ausdrückliche vorherige Einwilligung E-Mail-Werbung für ähnliche Produkte des Unternehmens versendet werden.

Der hier beschriebene Online-Mode-Händler versendet sowohl Newsletter per E-Mail auf Einwilligungsbasis (bei Ankreuzen des oberen Feldes) als auch unabhängig davon Produktempfehlungen.

In beiden Fällen ist es allerdings erforderlich, dass diese Verarbeitung ihrer personenbezogenen Daten den Kund:innen bereits bei der Erhebung ihrer Daten dargelegt wird. Die Unternehmen müssen ihre Kund:innen informieren, wie ihre Daten verarbeitet werden (Art. 5 Abs. 1 lit. a i.V.m. Art. 12 Abs. 1 DSGVO, Art. 13 Absatz 1 lit. c) DSGVO) und über ihr Widerspruchsrecht aufklären (Art. 21 Abs. 4 DSGVO, § 7 Abs. 3 Ziff. 4 UWG).

Die Ausgestaltung der Hinweise auf der Bestellmaske sowie die für den Versand der Produktempfehlungen verwendete Absender E-Mail-Adresse „newsletter@unternehmens-domäne.com“ waren aus Sicht des HmbBfDI nicht hinreichend geeignet, um den Kund:innen die Verarbeitung ihrer E-Mail-Adresse für den Versand von Bestandskundenwerbung für ähnliche Produkte nach einer Bestellung – unabhängig von einer Einwilligung in den Erhalt eines Newsletters – sowie die diesbezügliche Möglichkeit zum Widerspruch transparent zu machen. Hierauf wurde das Unternehmen hingewiesen.

Es hat daraufhin vollumfänglich und zeitnah kooperiert und den Hinweistext in den Bestellmasken für die Registrierung und die Bestellung als Gast europaweit wie folgt angepasst:

☐ Ich möchte zukünftig von dem Unternehmen über aktuelle Trends, Angebote und Rabatte gemäß der Datenschutzerklärung [Verlinkung zur Datenschutzerklärung auf den entsprechenden Abschnitt zum Newsletters-Erhalt] erhalten. Du kannst Deine Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen, indem Du eine Nachricht an kundenservice@unternehmens-domäne.de schickst oder die Abmeldeoption am Ende jedes Newsletters nutzt.

[Button zur Verifizierung]
[Button zur Registrierung]

Unabhängig davon, ob Du einen Newsletter abonniert hast, erhältst Du regelmäßig Produktempfehlungen für ähnliche Artikel und Dienstleistungen, die auf Deinen früheren Einkäufen basieren. Du kannst den Produktempfehlungen jederzeit kostenlos, mit Wirkung für die Zukunft, am Ende jeder Produktempfehlungs-E-Mail widersprechen oder eine Nachricht an kundenservice@unternehmens-domäne.de senden. Datenschutzerklärung [Verlinkung zur Datenschutzerklärung auf den entsprechenden Abschnitt zu Produktempfehlungen per E-Mail]

Des weiteren wurde eine neue separate Absender-E-Mail-Adresse für den Versand der Produktempfehlungen eingerichtet, um den Kund:innen die Differenzierung zwischen Produktempfehlungen und einem einwilligungspflichtigen Newsletter sowie die jeweiligen Abmeldefunktionen zu verdeutlichen.

Der HmbBfDI begrüßt, dass mit der nunmehr gewählten Gestaltung eine transparentere Information der Kund:innen erreicht wird, die auch anderen Unternehmen der Branche empfohlen werden kann.

10. Versand werblicher E-Mails an geschäftliche E-Mail-Adressen

Die Verwendung von E-Mail-Adressen natürlicher Personen zur werblichen Ansprache (Kalt-Akquise), ist auch im geschäftlichen Kontext nur datenschutzrechtlich zulässig, wenn der angeschriebene Kontakt zuvor ausdrücklich darin eingewilligt hat.

Die Verwendung von E-Mail-Adressen natürlicher Personen zur werblichen Ansprache (Kalt-Akquise), ist auch im geschäftlichen Kontext nur datenschutzrechtlich zulässig, wenn der angeschriebene Kontakt zuvor ausdrücklich darin eingewilligt hat.

Den HmbBfDI erreichen eine Vielzahl von Beschwerden zu unerwünschter E-Mail-Werbung. Im vergangenen Jahr war dabei insbesondere eine Zunahme von Beschwerden über unerwünschte werbliche E-Mails an geschäftliche E-Mail-Adressen mit Personenbezug (z.B. Vorname.Nachname@Unternehmen.de) festzustellen.

Der Werbebezug ergab sich in der Regel daraus, dass für Produkte oder Dienstleistungen eines Unternehmens geworben wurde. Mit dieser Werbung sollten in der Regel gezielt Personen angesprochen werden, die ausweislich ihrer beruflichen Position mutmaßlich über Entscheidungsbefugnisse über den Bezug oder Einsatz der beworbenen Produkte oder Dienstleistungen in ihrem Unternehmen verfügen.

In datenschutzrechtlicher Hinsicht sind hierbei mehrere Aspekte problematisch, insbesondere die Herkunft dieser Daten und die Rechtsgrundlage für die Nutzung zur werblichen Ansprache per E-Mail.

Nach den Erkenntnissen des HmbBfDI stammen die E-Mail-Adressen sowie die korrespondierenden Daten (häufig Name, Vorname, Arbeitgeber, berufliche Position) oftmals aus öffentlich verfügbaren

Quellen wie der Internetpräsenz des Unternehmens und beruflichen sozialen Netzwerken. Teilweise erfolgt aber auch eine Anreicherung vorhandener Daten mit Hilfe von hierauf spezialisierten Unternehmen. Hierbei kommt es sowohl zu plattformweitem Scraping (d.h. automatisiertes Durchsuchen und Abgreifen von Daten in großem Umfang) auf den sozialen Netzwerken als auch zum Einsatz von Programmen, welche aus dem öffentlich verfügbaren Vor- und Nachnamen sowie dem Unternehmensnamen auf Grundlage von möglichen Kombinationen und Abkürzungen (z.B. Vorname.Nachname@, V.Nachname@, Vorname.N@, V.N.@) automatisiert eine hohe Zahl zutreffender, aber nicht öffentlich verfügbarer E-Mail-Adressen generieren können.

Da es sich bei diesen E-Mail-Adressen aufgrund der Identifizierbarkeit der jeweiligen Personen um personenbezogene Daten (Art. 4 Nr. 1 DSGVO) handelt, unterfällt deren Verarbeitung (Art. 4 Nr. 2 DSGVO) den Vorschriften der DSGVO. Als Folge darf jegliche Verarbeitung dieser Daten, sowohl also die Erhebung bzw. Erzeugung und Speicherung der E-Mail-Adressen sowie etwaiger weiterer personenbezogener Daten der adressierten Personen als auch deren Nutzung zur werblichen Ansprache der Betroffenen, nur auf einer entsprechenden Rechtsgrundlage erfolgen (Art. 5 Abs. 1 lit. a), Art. 6 Abs. 1 DSGVO). Darüber hinaus sind die Informationspflichten aus Art. 13, 14 DSGVO zu beachten, so dass den Betroffenen im Rahmen dieser Verarbeitung u.a. die Herkunft ihrer personenbezogenen Daten und deren Verarbeitungszwecke darzulegen ist.

Für die Werbung mittels elektronischer Post (hierzu zählt insbesondere die E-Mail, aber auch sonstige Formen wie digitale Posteingänge, Nachrichten auf sozialen Netzwerken oder Messenger) kommen nur zwei Rechtsgrundlagen in Betracht: einerseits die Werbung auf Grundlage einer vorherigen, ausdrücklichen Einwilligung des Betroffenen (Art. 6 Abs. 1 Satz 1 lit. a), Art. 7 DSGVO i. V. m. § 7 Abs. 2 Nr. 2 DSGVO), andererseits die Bestandskundenwerbung für ähnliche Produkte auf Grundlage von Art. 6 Abs. 1 Satz 1 lit. f) DSGVO i. V. m. § 7 Abs. 3 UWG unter den dort genannten Voraussetzungen.

In den dem HmbBfDI vorliegenden Fällen lag keine der beiden genannten Rechtsgrundlagen vor. Seitens der werbenden Unternehmen ist als Rechtfertigung überwiegend damit argumentiert worden, dass von einem mutmaßlichen Interesse der adressierten Personen ausgegangen worden sei, welches die rechtmäßige Versendung der werblichen E-Mails ermöglichen würde. Eine werbliche Ansprache mittels elektronischer Post auf Grundlage eines mutmaßlichen Interesses der etwaigen Werbeempfänger ist allerdings gesetzlich nicht zulässig. Das mutmaßliche Interesse ist lediglich für den in § 7 Abs. 2 Nr. 1 UWG beschriebenen Ausnahmefall der telefonischen Werbung (sog. Cold Calls) gegenüber Unternehmen als Voraussetzung genannt. Eine Übertragung dieser Ausnahme als Grundlage für den Versand werblicher E-Mails an geschäftliche (personenbezogene) E-Mail-Adressen ist nicht möglich.

Der HmbBfDI stellt bei entsprechenden Beschwerden in diesen Fällen aufgrund der Verarbeitung personenbezogener Daten ohne Rechtsgrundlage Verstöße fest. Unternehmen ist daher dringend anzuraten, von der Verwendung personenbezogener E-Mail-Adressen zur werblichen Ansprache abzusehen, sofern keine entsprechend dokumentierte Einwilligung vorliegt, und stattdessen die rechtlich zulässigen Wege zur Kontaktaufnahme zu nutzen.

11. Diversity in der Filmbranche – Erhebung von hochsensiblen Daten

Seit 2020 sind in der Filmförderung Diversitätskriterien verpflichtend zu berücksichtigen. Hierfür wurden sog. „Diversity-Checklisten" für Filmproduktionen eingeführt. Naturgemäß enthalten diese Datensätze eine Vielzahl hochsensibler Daten der betroffenen Personen. Seit 2024 ergänzt die Online-Plattform OMNI Inclusion Data die Checkliste und liefert konkretere Angaben zur Diversität der deutschen Film- und Medienbranche. Erstmals stammen diese Antworten von Cast und Crew selbst, nicht von den Produktionen. Der HmbBfDI begleitete die Entwicklung der Plattform und gab Empfehlungen zur datenschutzkonformen Gestaltung, um den Schutz hochsensibler personenbezogener Daten sicherzustellen.

OMNI Inclusion Data basiert auf internationalen Vorbildern, insbesondere aus Australien und Großbritannien. In Australien gibt es bereits seit 2020 „The Everyone Project", das Diversitätsdaten für die dortige Medien- und Filmbranche erhebt. In Großbritannien existiert das Projekt „Diamond", das schon länger aktiv ist und wichtige Erkenntnisse lieferte, beispielsweise zur Unterrepräsentation von Menschen mit Behinderung in der Filmbranche. Die MOIN Filmförderung führte Gespräche mit Vorbildern aus diesen Ländern sowie Kanada, um verschiedene Plattformen und deren Wirksamkeit kennenzulernen. Die Technologie von „The Everyone Project" diente dabei als Grundlage für die Entwicklung des deutschen OMNI-Tools, wobei das Backend speziell für die deutsche Branche angepasst wurde.

Im Gegensatz zur Checklist, die von Produktionsfirmen ausgefüllt wird, ermöglicht OMNI den Cast- und Crew-Mitgliedern selbst, Informationen zu diversitätsrelevanten Merkmalen beizusteuern. Diese umfassen Aspekte wie Geschlecht, Hautfarbe, Fluchtgeschichte, Behinderung, Bildung und Bildungshintergrund sowie Diskriminierungserfahrungen.

Ende 2023 wurde OMNI dem HmbBfDI vorgestellt. Aufgrund der beschriebenen, besonders sensiblen Datenkategorien im Fokus gab der HmbBfDI Empfehlungen zur datenschutzkonformen Gestaltung, Anonymisierung, Datenzugriff und Datensparsamkeit sowie zu potenziellen Rechtsgrundlagen. Im Februar 2024 startete die Pilotphase von OMNI, mit einem geplanten vollständigen Launch für 2025.

Bei einer Vorstellung im September 2024 konnten weitere datenschutzrechtliche Problemfelder identifiziert werden. So wurde festgestellt, dass die Datenschutzdokumentation, insbesondere im Zusammenhang mit der Pilotstudie, noch nicht vollständig vorlag, und die Einwilligungserklärung in ihrer Transparenz und Nachvollziehbarkeit optimiert werden musste. Auch die Verarbeitung von sensiblen Daten, die zunächst personenbezogen erhoben und erst später anonymisiert wurden, wurde optimiert. Insbesondere wurden hier Verbesserungen der technischen und auch organisatorischen Maßnahmen i.S.d. Art. 32 DSGVO festgestellt. Dieses Vorgehen ermöglichte es dem HmbBfDI, gezielte Verbesserungsvorschläge zu machen, und half dem Verantwortlichen, die Schwachstellen zu identifizieren.

Die MOIN Filmförderung setzte die Empfehlungen zügig um und leitete umfassende Verbesserungsmaßnahmen ein. So wurden die Speicherfristen klar definiert und ein strukturiertes Löschkonzept etabliert. Kontaktdaten der Mitwirkenden werden nun konsequent nach Abschluss des Erhebungszeitraums einer Produktion gelöscht. Gleichzeitig bleiben Umfragedaten für überjährige Auswertungen erhalten, können jedoch auf Wunsch der Teilnehmenden jederzeit gelöscht werden, was den Datenschutzanforderungen in besonderem Maße Rechnung trägt.

In einem weiteren Austausch wurden zusätzliche Schritte zur Stärkung des Datenschutzes vereinbart. So sollten die Daten nun bereits zum frühestmöglichen, durch den Zweck der Umfrage zulässigen Zeitpunkt anonymisiert und zuvor pseudonymisiert verarbeitet werden. Um die Freiwilligkeit der Einwilligungen sicherzu-

stellen, wurden verschiedene Maßnahmen eingeführt, darunter die vertragliche Verpflichtung der Produktionsgesellschaften, die Freiwilligkeit konsequent zu gewährleisten. Ebenfalls sollte aus diesem Anlass das diesbezügliche Informationsschreiben angepasst werden, um vollständige Transparenz und eine vollumfängliche Information der Teilnehmenden zu ermöglichen.

Insgesamt wird deutlich, dass das Vorhaben ein bedeutendes Ziel im Bereich Diversität und Inklusion in der Filmbranche verfolgt und gleichzeitig eine Vielzahl datenschutzrechtlicher Fallstricke aufwies. Durch die konstruktive Hinzuziehung des HmbBfDI konnten potenzielle datenschutzrechtliche Herausforderungen frühzeitig erkannt und mehrfach und erfolgreich angepasst werden.

Gleichzeitig empfiehlt der HmbBfDI eine regelmäßige Überprüfung der datenschutzrechtlichen Vorgaben, um den hohen Anforderungen an den Schutz sensibler, besonderer Kategorien personenbezogener Daten gerecht zu werden.

12. Unangekündigte Vor-Ort-Prüfungen

Der HmbBfDI führte im Berichtszeitraum vermehrt unangekündigte Vor-Ort-Prüfungen durch. Sie verfolgten in den meisten Fällen den Zweck, einen Datenschutzverstoß zügig abzustellen. In manchen Fällen dienten sie auch der Beweissicherung.

Im Berichtszeitraum führte der HmbBfDI verstärkt unangekündigte Vor-Ort-Kontrollen durch. Ziel dieser Maßnahmen war es, entweder akute Datenschutzverstöße unverzüglich abzustellen oder notwendige Beweise zu sichern. Dabei wurde stets darauf geachtet, dass die Eingriffe in die Rechte der Verantwortlichen verhältnismäßig waren und die eingesetzten Mittel in einem angemessenen Verhältnis zu dem angestrebten Zweck standen. Positiv hervorzuheben ist, dass die Verantwortlichen sich bei den durchgeführten Vor-Ort-

Prüfungen durchweg kooperativ zeigten und teils gemeinsam mit dem HmbBfDI rasch Lösungen erarbeiteten.

Nachfolgend werden exemplarisch einige der durchgeführten Prüfungen dargestellt:

1. Der HmbBfDI wurde durch einen anonymen Hinweis darüber informiert, dass durch das Schaufenster einer Apotheke sensible Informationen wie Rezepte samt Namen, Adressen und Medikationsdaten ebenso wie Mitarbeiter:innenlisten mit Telefonnummern von der Straße aus einsehbar waren. Ein Mitarbeiter des HmbBfDI überprüfte dies unverzüglich vor Ort. Der Datenschutzverstoß konnte innerhalb von zwei Stunden abgestellt werden: Das betroffene Fenster wurde mit einer Milchglasfolie beklebt. Nachträglich übersandte Fotos dokumentierten die sofortige Umsetzung.
2. Durch einen weiteren anonymen Hinweis wurde der HmbBfDI darauf aufmerksam, dass bei einem Unternehmen der beruflichen Rehabilitation eine Aktenvernichtungstonne unverschlossen, unbefestigt und leicht zugänglich in einem unbeaufsichtigten Hinterhof abgestellt war. Durch eine Vor-Ort-Kontrolle konnten Beweise für eine später ausgesprochene Verwarnung gesichert und vor allem der Datenschutzverstoß unmittelbar abgestellt werden, indem die Aktenvernichtungstonne abgeschlossen und in einen verschlossenen Raum umgestellt wurde.
3. In einem weiteren Fall fertigte ein Hotelbetrieb datenschutzrechtswidrig von sämtlichen Hotelgästen Ausweiskopien. Der durchgeführten unangekündigten Vor-Ort-Kontrolle ging eine schriftliche Auseinandersetzung über die Rechtmäßigkeit dieser Datenverarbeitungspraxis voraus. Für den HmbBfDI ergaben sich Hinweise darauf, dass das Unternehmen seine Datenverarbeitungspraxis nicht angepasst haben könnte. Die der Nachkontrolle dienende unangekündigte Vor-Ort-Prüfung ergab indes, dass sich der Betriebszweck des Unternehmens geändert hatte, sodass die Prüfung obsolet wurde.

4. Zuletzt prüfte der HmbBfDI mehrere Tankstellen bezüglich der eingesetzten Videoüberwachungsanlagen auf die Einhaltung der Transparenzpflichten aus Art. 13 DSGVO. Einige der Prüfungen dauern noch an.

Die beschriebenen Fälle stellen nur eine Auswahl der im Berichtszeitraum durchgeführten unangekündigten Vor-Ort-Prüfungen dar. Sie zeigen, wie durch gezielte und unvermittelte Kontrollen Datenschutzverstöße erkannt und zum Teil unmittelbar behoben werden können. Diese Form der Prüfung ergänzt die regulären, angekündigten Kontrollen und wird weiterhin punktuell eingesetzt werden, vor allem, um Hinweisen auf dringlich abzustellende Datenschutzverstöße nachzugehen.

BERICHTE III.

Berichte

1. Novellierung von Sicherheitsgesetzen bei Polizei und Landesamt für Verfassungsschutz

Die Behörde für Inneres und Sport (BIS) hat im Berichtszeitraum sowohl einen Entwurf zur Änderung des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) als auch zum Hamburgischen Verfassungsschutzgesetz (HmbVerfSchG) vorgelegt. Der HmbBfDI hat die Entwürfe – bei äußerst kurzen Beteiligungsfristen – im Rahmen seiner Zuständigkeit geprüft. Einige der vom HmbBfDI geltend gemachten datenschutzrechtlichen Bedenken wurden dabei aufgegriffen. Es ist besonders erfreulich, dass die Digitalisierung nunmehr nicht nur in der polizeilichen Praxis voranschreitet, sondern auch Eingang in das PolDVG findet.

Im Sommer 2024 erreichten den HmbBfDI im Rahmen von formell eingeleiteten behördlichen Drucksachenabstimmungen sowohl der Entwurf der BIS für eine Änderung des PolDVG, als auch der Entwurf für eine Änderung des HmbVerfSchG. Es ist kritisch festzuhalten, dass der HmbBfDI nicht bereits im Rahmen einer Vorabstimmung bei beiden Gesetzen beteiligt wurde. Von einer frühzeitigen Einbeziehung der datenschutzrechtlichen Aufsichtsbehörde in Gesetzgebungsverfahren, welche überwiegend datenschutzrechtlich höchst sensible Aspekte behandelt, hätten beide Seiten profitiert. Insbesondere bei der Drucksachenabstimmung zum PolDVG wurde dem HmbBfDI eine äußerst kurze Frist von elf Werktagen zur Stellungnahme eingeräumt. Angesichts der Bedeutung sowie Komplexität der Materie erscheint dies unangemessen.

1.1 Änderungen PolDVG

Mit den im Juli 2024 in die behördliche Drucksachenabstimmung eingebrachten Änderungen des PolDVG sollten laut BIS insbesondere die Vorgaben des Bundesverfassungsgerichts (BVerfG) aus dem Beschluss vom 27.5.2020 (1 BvR 1873/13, 1 BvR 2618/13 – Bestandsdatenauskunft II), dem Beschluss vom 9.12.2022

(1 BvR1345/21) und dem Urteil vom 16.2.2023 (1 BvR 1547/19, 1 BvR 2643/20) umgesetzt werden.

Die Vorgaben aus Letzterem waren aus Hamburger Sicht besonders spannend. Das höchste deutsche Gericht hatte in dieser Entscheidung § 49 Abs. 1 Alt. 1 PolDVG für verfassungswidrig erklärt. Der HmbBfDI hatte als Sachkundiger Dritter gem. § 27a BVerfGG sowohl schriftlich als auch im Rahmen der mündlichen Verhandlung vor dem BVerfG zu der Vereinbarkeit mit dem Grundgesetz datenschutzrechtlich Stellung genommen (vgl. Tätigkeitsbericht 2022, Kapitel III 1).

Der nun zunächst im Rahmen der Behördenabstimmung vorgelegte Entwurf entsprach zunächst nicht in ausreichendem Maße den Vorgaben des Gerichts. Erfreulicherweise wurden jedoch die vom HmbBfDI im Rahmen der Behördenabstimmung vorgetragenen datenschutzrechtlichen Bedenken teilweise aufgegriffen: Die Eingriffsschwelle wurde erhöht. Der Verweis auf § 100a Strafprozessordnung (StPO) (schwere Straftaten) wurde auf § 100b StPO (besonders schwere Straftaten) umgestellt und eine Definition zu „Vorfeldstraftaten" eingefügt. Die Vorschrift wird nunmehr rechtstaatlichen Anforderung besser gerecht. Im Hinblick auf die Rechtsprechung des BVerfG zum § 49 PolDVG a.F. bestehen aber weiterhin verfassungsrechtliche Unsicherheiten im Hinblick auf den Wesentlichkeitsvorbehalt, da Rechte- und Rollenkonzept sowie Kategorisierungs- und Kennzeichnungskonzept weiterhin ohne nähere Vorgaben des Gesetzgebers durch die Polizei selbst zu erstellen sind. Ferner bleibt der Umfang der Veröffentlichungspflicht für die diesbezüglichen Verwaltungsvorschriften unklar.

Kritisch geäußert hatte der HmbBfDI sich u.a. auch im Hinblick auf die konkrete Ausgestaltung der Einführung eines sog. Pre-Recordings beim Einsatz von Bodycams (§ 18 Abs. 6 Satz 2 PolDVG-E). Als Pre-Recording wird ein technisches Verfahren bezeichnet, in welchem eine Kamera das gesamte Geschehen aufzeichnet und diese Sequenzen in bestimmten Abständen immer wieder überspielt, ohne diese zu speichern, außer die Löschung wird manuell von einer

Person ausgesetzt. Die Einführung einer solchen dauerhaft und anlasslosen vorläufigen Aufzeichnung, die nicht einmal an die Durchführung einer polizeilichen Maßnahme gekoppelt ist, wurde vom HmbBfDI als datenschutzrechtlich bedenklich bewertet. Abgeholfen wurde dem jedoch nicht. Der zudem vorgetragenen Kritik im Hinblick auf die Dauer des Pre-Recordings (ursprünglich Löschung nach 90 Sekunden) wurde insoweit Rechnung getragen, als dass die Dauer des Pre-Recordings in der Drs. 22/16042 auf 60 Sekunden herabgesetzt wurde. Bedauerlicherweise wurde die Kritik bezüglich eines fehlenden Kernbereichsschutzes auch bei Erhebung/Aufnahme im Pre-Recording nicht umgesetzt. Möglich sind Fälle, in denen Bodycams auf größere Entfernung genutzt werden und hierbei Gespräche erfasst werden, insbesondere von unbeteiligten Dritten, aber auch der Polizeibeamt:innen selbst. Auf die vom HmbBfDI vorgebrachte Kritik hin wurde aber zumindest für den Einsatz von Bodycams in Wohnungen auf der Verwertungsebene eine Kernbereichsregelung eingefügt (§ 18 Abs. 7 PolDVG-E).

Zweifel bestehen auch nach der Behördenabstimmung noch im Hinblick auf die Ausgestaltung des Einsatzes von unbemannten Luftfahrtsystemen nach § 18 Abs. 8 PolDVG-E. Die Norm wirkt als technik-offener Auffangtatbestand für die Videoüberwachung im Gefahrenabwehrbereich. Aus der gesetzlichen Begründung folgt trotz der Technikoffenheit der Regelung, dass mit dieser Norm vor allem die Verarbeitung von personenbezogenen Daten durch den Einsatz von Drohnen geregelt werden soll. Beim Einsatz von Drohnen ist – im Vergleich zu herkömmlichen technischen Mitteln zur Videoüberwachung – von einer erhöhten Eingriffsintensität auszugehen, die daraus resultiert, dass Betroffene die Tatsache, dass Aufzeichnungen erfolgen, sehr viel schlechter wahrnehmen können. Diese erhöhte Eingriffsintensität sollte sich nach Auffassung des HmbBfDI auch in der Norm niederschlagen. Insbesondere sollte sichergestellt werden, dass neben dem Einsatz der Drohne auch die verantwortliche Stelle erkennbar ist und auf beides hingewiesen wird. Letzteres wurde zumindest in die gesetzliche Begründung aufgenommen. Es erscheint datenschutzrechtlich aber weiterhin bedenklich, eine so

eingriffsintensive Maßnahme auf den generalklauselartig formulierten § 18 Abs. 8 PolDVG-E zu stützen.

Die Umsetzung der Rechtsprechung zur hypothetischen Datenneuerhebung in § 34 PolDVG-E wurde vom HmbBfDI – ebenso von Experten im Rahmen der Anhörung im Innenausschuss am 28.11.2024 – als verfehlt beurteilt. Sie ist sprachlich teils nicht gelungen und das Verhältnis zu anderen Vorschriften ist nicht eindeutig erkennbar. Insbesondere die pauschale Verwendung des datenschutzrechtlichen Oberbegriffs der „Verarbeitung" für verschiedene Phasen der Verarbeitung von personenbezogenen Daten anstatt der Verwendung von eindeutigen Unterbegriffen (vgl. § 2 Abs. 8 PolDVG) trägt nicht zur Klarheit der Norm bei. Der HmbBfDI hat in seiner Stellungnahme Vorschläge gemacht, um die Verständlichkeit der Regelung deutlich zu verbessern Der am 15.1.2025 von zwei Fraktionen in die Bürgerschaft eingebrachte und angenommene Änderungsantrag (Bü.-Drs. 22/17442) greift auch diese Vorschläge des HmbBfDI ausdrücklich auf.

Abschließend hat der HmbBfDI deutlich darauf hingewiesen, dass die im Rahmen der Behördenabstimmung vorgelegte Überarbeitung des PolDVG dringend notwendige Regelungen und Ergänzungen zur Bewältigung der zunehmenden Digitalisierung der Gesellschaft und damit auch der Polizeiarbeit vermissen lässt. Schon jetzt werden zur Aufgabenerfüllung durch die Polizei Hamburg intelligente Videoüberwachungssysteme eingesetzt (vgl. Tätigkeitsbericht 2023, Kapitel III 1 Intelligente Videoüberwachung Hansaplatz). Im Jahr 2024 ist neu dazugekommen, dass die Polizei Hamburg diese Systeme nun auch mit den Daten von Hamburger Bürger:innen trainieren will (vgl. Kapitel IV 9). Bisher wurden die Systeme ausschließlich vortrainiert erworben. Diese neue Dimension des Eingriffs spiegelte sich nicht in den vorhandenen gesetzlichen Grundlagen wider. Mit Blick auf diese Entwicklungen erschien es daher misslich, dass die Anpassung des Gesetzes nicht genutzt wurde, um gesetzgeberische Leitlinien für diese Entwicklung vorzugeben. Der HmbBfDI hat im Rahmen der Behördenabstimmung auch zunächst nicht umgesetzte Anregungen

für eine/derartige Normen gegeben. Durch den am 15.1.2025 angenommenen Änderungsantrag (Bü.-Drs. 22/17442) wird nun ebenfalls das Trainieren und Testen von IT-Systemen erstmalig und ausdrücklich in § 37a PolDVG auf ein rechtliches Fundament gestellt. Dies ist eine dringend notwendige Reaktion auf den digitalen Fortschritt auch im Sicherheitsbereich und erhöht die Rechtssicherheit sowohl für den Anwender als auch die Betroffenen.

1.2 Änderungen HmbVerfSchG

Mit dem im Juni 2024 im Rahmen der 1. Behördenabstimmung vorgelegten Gesetzesentwurf zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzrechts beabsichtigt die BIS die Anpassung dieses Gesetzes an geändertes Bundesrecht, insbesondere an das Bundesverfassungsschutzgesetz (BVerfSchG) und die Fortentwicklung des HmbVerfSchG nach den Vorgaben der verfassungsgerichtlichen Rechtsprechung. Im Fokus standen dabei vor allem die Urteile des BVerfG vom 26.4.2022 (1 BvR 1619/17) zum Bayrischen Verfassungsschutzgesetz und vom 28.9.2022 (1 BvR 2354/13) zur Übermittlung von Informationen durch Nachrichtendienste. Der HmbBfDI wurde im Rahmen von zwei Behördenabstimmungen beteiligt. Dabei wurden in dem Gesetzentwurf, der Gegenstand der zweiten Abstimmung war, bereits viele Bedenken und Anmerkungen des HmbBfDI aus der ersten Behördenabstimmung aufgegriffen. Dabei sind insbesondere die auf Anregung des HmbBfDI erfolgte Überarbeitung der Regelung zur Protokollierung und die dadurch erfolgte Verbesserung der datenschutzrechtlichen Überprüfbarkeit positiv zu bewerten.

Allerdings wurden Anmerkungen und Anregungen des HmbBfDI im Zusammenhang mit den sog. Übermittlungsvorschriften nicht gestaltend aufgriffen. Die Übermittlung von Informationen von Nachrichtendiensten an andere öffentliche Stellen ist verfassungsrechtlich aber besonders brisant. Die weitreichenden Überwachungsbefugnisse der Nachrichtendienste sind verfassungsrechtlich nur dann gerechtfertigt, wenn die aus der Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen

Anschlussbefugnissen (wie z.B. die Polizei) übermittelt werden dürfen (sog. Trennungsgebot). Eine Übermittlung durch eine Verfassungsschutzbehörde setzt stets voraus, dass die Übermittlung dem Schutz eines besonders gewichtigen Rechtsguts dient. Die Übermittlung an eine Gefahrenabwehrbehörde erfordert darüber hinaus, dass für dieses Rechtsgut eine hinreichend konkretisierte Gefahr besteht (BVerfG, Urt. v. 26.4.2022 – 1 BvR 1619/17, 3. Leitsatz). Im vorgelegten Entwurf wurde bei der Offenlegung von personenbezogenen Daten gegenüber der Polizei und allen anderen öffentlichen Stellen insoweit differenziert, als dass nur bei ersterem die konkretisierte Gefahr verlangt wurde (vgl. §§ 26, 27 HmbVerfSchG-E). Damit wurde im Entwurf eine starre Trennlinie zwischen Polizei und anderen öffentliche Stellen gezogen. Dies ist problematisch, wenn die empfangenden Stellen ebenfalls über eigene operative Anschlussbefugnisse verfügen wie beispielsweise einer Gewerbeuntersagung oder Ausweisung. Nach den Ausführungen des BVerfG müssten insoweit ähnlich hohe Anforderungen gelten wie bei der Übermittlung an die Polizei. Nach der starren Regelung im HmbVerfSchG-E gilt eine einfache Unterscheidung zwischen Polizei und allen anderen Stellen der Verwaltung, ohne dass Besonderheiten bei den Stellen der Verwaltung Berücksichtigung finden. Zwar wurden die Bedenken des HmbBfDI im Hinblick auf § 27 HmbVerfSchG-E als „gewichtig“ angesehen, aus Harmonisierungsgründen wird dennoch dem Bund gefolgt. Die Vorschrift entspricht in Ausgestaltung und Begründung fast vollständig § 20 BVerfSchG.

Dies ist umso bedauerlicher, da nach Fertigung der Stellungnahmen des HmbBfDI die Entscheidung des BVerfG zum reformierten hessischen Verfassungsschutzgesetz ergangen ist (BVerfG, Beschl. v. 17.7.2024 – 1 BvR 2133/22; veröffentlicht am 17.9.2024). Diese Entscheidung stützt die Ausführungen des HmbBfDI und hat – wie auch von den Experten im Innenausschuss am 10.10.2024 aufgegriffen – gravierende Auswirkungen auf den vorgelegten Entwurf, die jedoch bedauerlicherweise nicht aufgegriffen wurden.

2. Hinweisschreiben an den Polizeipräsidenten – Datenschutzverstoß im Ermittlungsverfahren

Im Berichtszeitraum hat ein datenschutzrechtlicher Vorfall dazu geführt, dass der HmbBfDI sich mit einem Hinweisschreiben direkt an den Hamburger Polizeipräsidenten wenden musste. Zwar ist der Sachverhalt als Einzelfall zu bewerten. Gleichwohl veranschaulicht er deutlich, welche Folgen der unbedachte Umgang mit personenbezogenen Daten für die Betroffenen haben kann und wie wichtig deswegen die wiederholte Schulung und Sensibilisierung von Mitarbeiter:innen ist.

Am 22.1.2024 wurde der HmbBfDI vom Hoteldirektor eines Beherbergungsunternehmens mit Sitz in Hamburg darüber in Kenntnis gesetzt, dass eine Beamtin des Landeskriminalamts der sich per E-Mail an das Hotel gewandt hatte. Unter Bezugnahme auf ein polizeiliches Aktenzeichen fordert die Beamtin die Empfänger der E-Mail auf, die vollständigen Personalien und Kontaktdaten einer dort angestellten Person zu übermitteln, da gegen diese ein Ermittlungsverfahren laufe. Neben der namentlichen Nennung der/des Tatverdächtigen führte sie zudem das in Frage kommende Delikt und den Namen des mutmaßlichen Opfers auf. Besonders brisant ist dabei, dass es sich bei dem Opfer ebenfalls um eine angestellte Person im selben Unternehmen handelt.

Die dabei genutzte Empfänger-E-Mail-Adresse wurde von der Beamtin dem allgemein zugänglichen und vorwiegend für Reservierungsanfragen gedachten Internetauftritt des Hotels entnommen. Eine vorherige Kontaktaufnahme mit dem Hotel per Telefon oder auf anderem Weg war nicht erfolgt. Der Hoteldirektor teilte dem HmbBfDI mit, dass auf dieses allgemeine Reservierungs-E-Mailpostfach alle Mitarbeiter:innen der Reservierung und der Rezeption Zugriff hätten, um auf Kundenanliegen schnell reagieren zu können. Nach Angaben des Hotels waren das zum entscheidenden Zeitpunkt zwölf Personen, alles Angestellte des Hotels und damit Kolleg:innen

sowohl der beschuldigten Person als auch des mutmaßlichen Opfers. Durch die Übersendung der E-Mail an dieses allgemeine Postfach hätten daher nahezu alle Mitarbeiter:innen des Hotels Kenntnis von dem Inhalt erhalten. Nach Angaben des Hotels handelt es sich dabei zum fraglichen Zeitpunkt um rund 65 Mitarbeiter: innen.

Der Verstoß ist im Hinblick auf den hier zugrunde liegenden Eingriff in Grundrechte der beiden betroffenen Personen erheblich. Die Weiterverbreitung von Daten zu Tatvorwürfen an einen unnötig großen Empfängerkreis stellt einen schwerwiegenden Eingriff in Persönlichkeitsrechte des Beschuldigten dar. Hinzu tritt im vorliegenden Fall auch noch die Verbreitung der personenbezogenen Daten des mutmaßlichen Opfers, deren Schutzwürdigkeit nicht in Zweifel stehen dürfte. Vertieft wird der Verstoß vorliegend noch dadurch, dass es sich bei den Empfängern der Daten um einen Großteil der Kolleg:innen sowohl der beschuldigten Person als auch des mutmaßlichen Opfers handelt. Durch diese Nähebeziehung verstärkt sich die Eingriffstiefe.

Die Polizei Hamburg hat sich gegenüber dem HmbBfDI zunächst auf § 163 StPO als Ermächtigungsgrundlage berufen. Diese Norm rechtfertigt aber nicht die Übermittlung von personenbezogenen Daten zu Ermittlungszwecken an unspezifizierte, offensichtlich nicht auf bestimmte Personen begrenzte E-Mailkonten. Der HmbBfDI stimmt der Polizei Hamburg darin zu, dass zum Zwecke der Sachverhaltsaufklärung Ermittlungen auch durch (formlose) Auskunftsersuchen nach § 163 StPO erfolgen dürfen. Art und Umfang der Maßnahme sind jedoch im vorliegenden Fall nicht mehr von dieser Generalklausel gedeckt, weil die Datenübermittlung unverhältnismäßig ist. Es war jedenfalls für die Sachverhaltsaufklärung nicht erforderlich, die personenbezogenen Daten des Tatverdächtigen und des mutmaßlichen Opfers an ein E-Mail-Postfach eines Hotels zu senden, das nicht personengebunden ist, sondern der allgemeinen Kontaktaufnahme dient. Aus mehreren gleich geeigneten Maßnahmen ist stets diejenige zu wählen, die den Einzelnen und die Allgemeinheit voraussichtlich am wenigsten beeinträchtigt. Es wäre der Polizei

ohne weitere Schwierigkeiten und ohne für die weiteren Ermittlungen zeitlich relevante Verzögerungen möglich gewesen, zu diesem Zweck zunächst telefonisch oder elektronisch ohne Personenbezug nach einem für diese Angelegenheiten zuständigen Beschäftigten oder einer internen Stelle zu fragen. Bei einem auf der Homepage angegebenen Postfach eines Beherbergungsbetriebs ist regelmäßig nicht von einem streng begrenzten Kreis zugriffsberechtigter Personen auszugehen. Im Hinblick auf die Größe des Hotels und den mit den Öffnungszeiten verbundenen großen Arbeitnehmerpool drängte es sich auf, dass mehrere Personen berechtigt sind, auf Reservierungsanfragen zuzugreifen. Gerade Personen, die in der Lage wären, Auskunft zu Personaldaten zu geben, dürften eher nicht zu dem zugriffsberechtigten Personenkreis gehören. Zur Erreichung des Zwecks – Erforschung des konkreten Sachverhalts – wäre es lediglich nötig gewesen, mit einer Person in Kontakt zu treten, die dazu befugt ist, Einsicht in die Personalakten des Verdächtigten zu bekommen.

Dieser Verstoß gegen Vorschriften des Datenschutzschutzrechts war zum Zeitpunkt der Kenntnis des HmbBfDI bereits abgeschlossen und leider nicht mehr zu beseitigen. Die Polizei Hamburg konnte gegenüber dem HmbBfDI allerdings darlegen, dass diese Vorgehensweise nicht der üblichen Praxis der Polizei Hamburg entspricht und eine mit der Staatsanwaltschaft abgestimmte Vorgehensweise die Zeugenbefragung mittels Mailverkehr und das Übermitteln entsprechender „sensibler" Daten für nicht zulässig bestimmt. Obwohl es sich auch nach der Erfahrung des HmbBfDI um einen Einzelfall handelte, hat sich der HmbBfDI als datenschutzrechtliche Aufsichtsbehörde der Polizei Hamburg aufgrund der Schwere des Verstoßes entschieden, den Hamburgischen Polizeipräsidenten mit einem Schreiben auf diesen Vorfall hinzuweisen. Neben der Veranschaulichung der Erheblichkeit des Verstoßes, wurde die datenschutzrechtliche Sensibilisierung der Mitarbeiter:innen durch entsprechende Schulungen und eine Aufarbeitung der Problematik angemahnt sowie die unverzügliche Aktualisierung der mit der Staatsanwaltschaft abgestimmten Vorgehensweise gefordert.

Der Polizeipräsident sicherte zukünftige Maßnahmen zu und berichtete insbesondere von einer bereits aufgrund des Vorfalls vorgenommenen Sensibilisierung und Adressierung der Mitarbeiter:innen des LKA.

3. Sicherheitslücken in der Telefon-Software der Justizvollzugsanstalten

Über verschiedene Sicherheitslücken in den in den Hamburger JVA eingesetzten Systemen für Telefonie und Videotelefonie war es potentiell über einen langen Zeitraum möglich, Daten von Insass:innen ohne jede Berechtigungsprüfung abzurufen. Nach Bekanntwerden wurden diese Lücken unverzüglich geschlossen. Ein tatsächlicher Datenfluss erscheint nach den bisher vorliegenden Kenntnissen insgesamt unwahrscheinlich. Der Fall zeigt, dass insbesondere in sensiblen Verarbeitungsbereichen eine ständige Beobachtung auch lange etablierter Systeme zwingend erforderlich ist.

Den HmbBfDI erreichte am 24.6.2024 der Hinweis einer IT-Sicherheitsexpertin auf mögliche Mängel in der Sicherheit der Verarbeitung personenbezogener Daten (Art. 32 DSGVO) bei einer bundesweit in Justizvollzugsanstalten eingesetzten Telefoniesoftware für die Insass:innen. Die Vorwürfe lauteten im Wesentlichen, dass über die Ausnutzung verschiedener Lücken Daten von Insass:innen von Justizvollzugsanstalten für Dritte ohne weitere Absicherung frei im Internet verfügbar gewesen waren.

Daraufhin nahm der HmbBfDI umgehend mit der Behörde für Justiz und Verbraucherschutz (BJV) Kontakt auf, um den Vorwürfen nachzugehen. Es stellte sich im Rahmen der Aufklärung heraus, dass der IT-Dienstleister der BJV die Meldung ebenfalls erhalten hatte und bereits erste Prüfungen vorgenommen hatte. Dabei haben sich zahlreiche Vorwürfe im Kern bestätigt. Namen, Vornamen, Haftnummern und Daten zum Telefonierverhalten waren ungesichert über

eine Schnittstelle im Netz abrufbar. Am 27.6.2024 erreichten den HmbBfDI innerhalb der vorgeschriebenen 72-Stunden-Frist dementsprechend auch Meldungen von Verletzungen des Schutzes personenbezogener Daten („Data Breach Meldungen", Art. 33 DSGVO). Nicht bestätigt hatte sich jedoch der Vorwurf, dass auch Aufzeichnungen von Telefongesprächen abrufbar gewesen waren.

Die BJV ging auch selbst von einer Verletzung des Schutzes personenbezogener Daten aus und traf Maßnahmen, um die Betroffenen hierüber zu informieren (Art. 34 DSGVO). Die Insass:innen wurden über den Vorfall durch Infoblätter in den JVA ab dem 28.6.2024 (mit Updates in der Folge) informiert. Die Information von den teils ebenfalls betroffenen Gesprächspartner:innen am Telefon erfolgte über eine Website.

Der HmbBfDI wirkte sodann auf eine vollständige Dokumentation des Vorfalls im Sinne von Art. 33 Abs. 5 DSGVO hin. Zu sichten waren neben der umfangreichen Dokumentation durch die IT-Sicherheitsexpertin zudem umfassende Unterlagen zur Ausschreibung der Telefonie-Systeme, zur Datenschutzdokumentation und mehrere Stellungnahmen der am Systembetrieb beteiligten Stellen.

Die Aufklärung der technischen Ursachen für den Vorfall ist weitestgehend abgeschlossen. Dem Vorfall lagen zwei unterschiedliche technische Probleme zugrunde, deren Auswirkungen auf den Schutz personenbezogener Daten der Insass:innen nach Art und Umfang sehr unterschiedlich waren (1. und 2.).

Zudem ließ sich der HmbBfDI die umfassenden Abhilfemaßnahmen zum Abstellen des Verstoßes und zur Verhinderung ähnlicher Vorfälle in der Zukunft darstellen (3.). Diese sind abschließend als nunmehr technisch ausreichend zu beurteilen:

1. **Ungesichterte GraphQL Schnittstelle**
   Es wurde festgestellt, dass in den Insass:innen-Telefonsystemen der Justizvollzugsanstalten der Stadt Hamburg wahrscheinlich

am 8.10.2022 eine sog. GraphQL-Schnittstelle installiert worden war. Dies war nicht beabsichtigt gewesen. Diese Schnittstelle erfüllt für den Betrieb der Software über keinerlei relevante Funktionen. Tatsächlich war dieses Update mit der Schnittstelle nur für bestimmte, andere Einrichtungen, die vom selben Dienstleister betreut werden, bestimmt. Dies wurde aber bis zum 24.6.2024 nicht bemerkt.

Dieses Update betraf grundsätzlich alle Justizvollzugsanstalten der FHH. Durch einen glücklichen Zufall kann aber bei der JVA Glasmoor weitgehend ausgeschlossen werden, dass es hierdurch zu einem Datenabfluss kam: Die Schnittstelle war zwar aktiviert, aber funktionsuntüchtig. Jeder Zugriff hätte zu einem dokumentierten Absturz geführt. Die Schnittstelle war nur erreichbar, wenn die dafür erforderlichen URLs (Domain-Namen) bekannt waren. Diese URLs sind – im Gegensatz zu normalen Domains – in keinem Verzeichnis wie der Denic o.ä. enthalten und daher auch nicht ohne weitere Kenntnisse durchsuchbar. Die Informationen sind nicht offensichtlich erkennbar, obwohl diese fehlende Erkennbarkeit nie bewusst als „Sicherungsmaßnahme“ angesehen wurde. Die URLs folgten allerdings einem recht vorhersehbaren Aufbau. Da die Einrichtung dieser Schnittstelle nie beabsichtigt war, fand auch keine Prüfung von Zugriffsrechten statt. Jedermann konnte hier potentiell ohne weitere Authentifizierung Abfragen vornehmen.

Betroffen von dem Vorfall waren personenbezogener Daten aller Personen, die in diesem Zeitraum Insass:innen der Hamburger JVA waren. Die Speicherung erfolgt zudem auch noch bis zu 365 Tage nach der Entlassung. Eine genaue Zahl der Betroffenen ließ sich im Nachgang – insbesondere aufgrund des langen Zeitraums – nicht mehr rekonstruieren. Potentiell war der Zugriff möglich auf Stammdatensätze der Insass:innen (u.a. Name, Vorname, Haftnummer und weitere Daten zum Telefonverhalten) sowie auf Telefonprotokolle (u.a. Anrufziel, Zeitpunkt, Dauer und Angaben zur Aufzeichnung des Gesprächs). Die Hinweisgeberin

listete Zugriffsmöglichkeiten auf ca. 3.300 Personendatensätze sowie 470.000 protokollierte Telefonanrufe. Diese erhebliche Größenordnung des Vorfalls wird seitens des HmbBfDI als plausibel eingeschätzt.

In der Flur- und Haftraumtelefonie der Hamburgischen JVA waren personenbezogene Daten von Gefangenen im Zeitraum vom 8.10.2022 bis zum Abend des 24.6.2024 entgegen der Regelungen des § 37 HmbJVollzDSG (i.V.m. Art. 29 JI-RL), § 40 HmbJVollzDSG i.Vm. § 64 BDSG nicht durch ein dem Stand der Technik entsprechendes Rechte- und Rollenkonzept vor dem Zugriff beliebiger Dritter geschützt (s. insb. § 64 Abs. 3 Nr. 4 BDSG: Benutzerkontrolle). Jedenfalls in einem dokumentierten Fall sind diese Daten dadurch auch in den Zugriffsbereich einer Dritten, unbefugten Person gelangt: der besagten IT-Sicherheitsexpertin.

Der unbemerkte Zugriff auf die Daten durch weitere Personen kann im Hinblick auf den langen Zeitraum und das Fehlen von Protokollierungen für die unbeabsichtigt betriebene Schnittstelle selbst nicht mit letzter Sicherheit ausgeschlossen werden. Für die relative Unwahrscheinlichkeit eines systematischen Ausnutzens der Lücke wird jedoch insoweit plausibel vorgetragen, dass dies zumindest in der JVA Glasmoor nachweisbar hätte sein müssen, da der Zugriff dort zum Absturz geführt hätte. Hierzu lagen dem Dienstleister zumindest Protokolle bis zum 15.6.2023 zurück vor. Abstürze dieser Art hätte es bis zum Zugriffsversuch der IT-Sicherheitsexpertin nicht gegeben. Isolierte Zugriffe auf die Schnittstellen der anderen JVA schließt dies aber nicht mit Sicherheit aus.

Die Schnittstelle wurde nach Auswertung der Meldung der IT-Sicherheitsexpertin durch den IT-Dienstleister noch im Laufe des 24.6.2024 zunächst abgeschaltet und die Abschaltung am Folgetag noch einmal überprüft.

2. Zugriffsmöglichkeiten durch Konfiguration einer Bezahlsoftware und der Software VideoVisit

Für die Insass:innen der Hamburger JVA besteht die Möglichkeit, über eine Website durch dritte Personen von außen Geld auf das Telefonkonto laden zu lassen. Zudem stellen einige Einrichtungen seit der Corona-Pandemie über die Software VideoVisit eine Möglichkeit digitaler Besuche zur Verfügung, um Einschränkungen der Besuchsregelungen durch die damaligen Kontaktbeschränkungen zu minimieren. Eine Kombination von Abfragemöglichkeiten in diesen beiden Systemen hat es im Einzelfall ermöglicht, dass Personen an die personenbezogenen Daten von Insass:innen gelangen konnten. Bis Redaktionsschluss blieb unklar, über welchen genauen Zeitraum hinweg diese Möglichkeit bestand.

Um Einzahlungen auf das Telefonkonto von Insass:innen zu ermöglichen, wird deren Telefonkontonummer benötigt. Durch sehr häufiges, technikgestütztes Ausprobieren war es in der Einzahlschnittstelle möglich, diese Kontonummern zu erhalten. Letztlich wurde automatisiert durch ein Skript vielfach und zufällig ausprobiert, ob zufällige Zahlenfolgen als Kontonummer existieren. Denn um die Funktion des Systems zu gewährleisten, muss das System einem Nutzer regelmäßig zurückmelden, ob eine eingegebene Nummer existiert (und somit für diese ein Betrag eingezahlt werden kann) oder eben nicht. Hierdurch lässt sich die Existenz von ausprobierten Häftlingsnummern bestätigen. Aus dieser Nummer sind für Dritte zunächst keine weiteren Rückschlüsse auf die Person zu ziehen.

Problematisch wurde das Erraten von Telefonkontonummern in Zusammenhang mit denjenigen Einrichtungen, die zusätzlich „VideoVisit“ nutzen. Dies sind die Sozialtherapeutische Anstalt (Sotha) und die JVA Fuhlsbüttel. Erst über die zusätzliche Nutzung von VideoVisit war es mithilfe der erlangten Kontonummern über die dortige Login-Seite möglich, Name und Vorname der Insassen zu erhalten.

Die IT-Sicherheitsexpertin erlangte über dieses Verfahren zunächst wohl 157 Telefonkontonummern. Damit konnte in 23 Fällen der Zugriff auf weitere personenbezogene Daten (Name, Vorname) der Insass:innen erlangt werden.

In der Bezahlschnittstelle/im System VideoVisit der JVA Fuhlsbüttel und der Sotha waren personenbezogene Daten von Gefangenen seit einem zu Redaktionsschluss noch nicht abschließend bestimmten Zeitpunkt bis zum Abend des 24.6.2024 entgegen der Regelungen des § 37 HmbJVollzDSG (i.V.m. Art. 29 JI-RL), § 40 HmbJVollzDSG i.Vm. § 64 BDSG nicht durch eine dem Stand der Technik entsprechende Benutzerprüfung vor dem Zugriff beliebiger Dritter geschützt (s. insb. § 64 Abs. 3 Nr. 4 BDSG: Benutzerkontrolle). Im Bezahlsystem konnte beliebig oft eine Kontonummer eingegeben und dadurch erraten werden. Dadurch war die reine Autorisierung eines Zugriffs auf Name und Vorname in VideoVisit durch Eingabe ebendieser Kontonummer kein hinreichend sicheres Nutzerauthentifizierungsverfahren mehr.

Die Datenbankabfragen des Einzahlungssystems wurden aus Sicherheitsgründen am 26.06.2024 zunächst als Sofortmaßnahme so umgestellt, dass bis zum Vorliegen eines Sicherheits-Updates jede Zahlungsanfrage nur zu einer Fehlermeldung führt.

Zumindest ein Zugriffsversuch einer unbefugten dritten Person (der Zugriff der IT-Sicherheitsexpertin) unter Ausnutzung dieser Sicherheitsmängel ist dokumentiert. Mit gewisser Sicherheit lässt sich hier nach Angaben des IT-Dienstleisters sagen, dass dieser Angriffsweg jedenfalls im Zeitraum von Januar 2024 bis zur Aufdeckung der Lücke nicht genutzt wurde. Die System-Log hätten einen solchen Brute-Force-Angriff sonst erkennen lassen. Ältere Daten hierzu lagen nicht vor.

3. Technische Anpassungen zur Abstellung und Verhinderung der Sicherheitsvorfälle

In Reaktion auf die Verletzung der Sicherheit personenbezogener Daten nahmen die BJV und der IT-Dienstleister nach Anhörung durch den HmbBfDI umfassende Änderungen vor. Die Graph-QL-Schnittstelle (vgl. 1) ist für den Normalbetrieb der Telefoniesoftware in den Einrichtungen nicht erforderlich und wird in diesen daher nach der Abschaltung nicht wieder implementiert werden. Bei dem Dienstleister wurde die Entwicklungsrichtlinie geändert, um ähnliche Vorfälle in Zusammenhang mit fehlerhaft eingespielten Updates in Zukunft zu verhindern. Es habe sich dort herausgestellt, dass ein Negativ-Test auf mögliche Lücken viel schwieriger zu bewerkstelligen sei als ein Positivtest auf die ordnungsgemäße Funktion von Änderungen und vollständige Abnahmetests: Für die Übertragung von Änderungen in produktiv genutzten Systemen sei deswegen ein Vier-Augen-Prinzip etabliert worden, wobei der Schwerpunkt für die zweite Person insbesondere auf mögliche Angriffe von außen gelegt worden sei. Auch in der bisherigen Entwicklungsrichtlinie war enthalten, dass die Sicherheitstests grundsätzlich durch die Kunden spezifiziert werden. Hierzu sollen die Kunden in Zukunft gerade bei größeren Updates noch einmal aktiv angehalten werden.

Anders als bei der GraphQL-Schnittstelle schied eine vollständige Abschaltung der Einzahlungsschnittstelle oder Videotelefonie (2.) auf Dauer aus, weil die ausgenutzten Funktionen für einen Betrieb grundsätzlich benötigt werden. Auch eine Absicherung bspw. mit Login-Namen und Passwort kam nicht ohne Weiteres in Frage. Der offene Zugriff auf die Einzahlungsschnittstelle ist grundsätzlich erforderlich. Als langfristige Maßnahme wurde daher ein sog. Rate-Limit integriert. Das Ausprobieren von beliebigen Kontonummern über die Schnittstelle wird nun erschwert, weil eine sich steigernde Wartezeit für eine erneute Abfrage in das System integriert wurde. Die Seite wurde im Anschluss wieder aktiviert, nachdem eine Überprüfung durch extern beauftragte Penetrations-Tester erfolgte. Es erfolgt zudem eine

Minimierung der Daten auf die für die Funktion erforderlichen Informationen bei Abfrage einer gültigen Kontonummer. Das Risiko kann so ohne Funktionsverlust jedenfalls reduziert werden. Die Kontonummern der Nutzer seien zudem ausgetauscht worden.

Insgesamt verdeutlicht dieser Data-Breach-Vorfall noch einmal, dass auch bei lange etablierten IT-Systemen eine regelmäßige Beobachtung und Testung zwingend notwendig ist. Dies gilt umso mehr bei Systemen, die sensible Daten enthalten. Softwareprodukte entwickeln sich oft dauerhaft weiter. Die damit einhergehenden Veränderungen können neue Schwachstellen eröffnen. Der Fall des Einbaus einer Schnittstelle, die tatsächlich gar nicht benötigt wird, aber dennoch neue Angriffsszenarien ermöglicht, stellt hier einen besonders dramatischen Fehler im Updatemanagement dar. Denkbar sind ähnliche Problematiken aber natürlich auch bei tatsächlich beabsichtigten Änderungen, die im Zusammenspiel mit bisherigen Gegebenheiten neue Angriffe ermöglichen können. So liegt es hier nahe, dass die fehlenden Beschränkungen in der Einzahlungsschnittstelle und in der Videotelefonie-Software schon bei Auslieferung der Produkte vorlagen. Eine Bestätigung hierfür lag bei Redaktionsschluss noch nicht vor. Dies wirkte sich erst dann negativ aus, als beide Systeme parallel eingesetzt worden sind. Beide Fehler blieben über lange Zeiträume unentdeckt. Dass es hier aller Wahrscheinlichkeit nach nicht zu nachweisbaren, größeren Datenabflüssen kam, ist letztlich nicht dem systematischen Schutz, sondern dem Zufall zu verdanken.

4. Bezahlkarte für Asylsuchende

Der HmbBfDI hat die Einführung der Bezahlkarte für Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG) in der FHH aufmerksam verfolgt und zu zentralen datenschutzrechtlichen Fragen Stellung genommen. Dadurch konnte insbesondere erreicht werden, dass Leistungsbehörden von datenschutzwidrigen Vorhaben wie der Einsicht in den Kontostand von leistungsberechtigten Personen und der Übermittlung von Ausländerzentralregister-Nummern an Kreditunternehmen Abstand genommen haben.

Zum 15. Februar 2024 wurde in der FHH die sog. SocialCard eingeführt. Dabei handelt es sich um eine Bezahlkarte in Form einer VISA-Guthabenkarte, die dazu dient, Leistungen nach dem AsylbLG zu erbringen. Eine SocialCard erhalten leistungsberechtigte Personen (in erster Linie Asylsuchende und deren Familienangehörige) zur Erfüllung ihres Anspruchs auf Gewährleistung eines menschenwürdigen Existenzminimums. Dabei müssen für die Einrichtung und Durchführung der Bezahlkarte personenbezogene Daten dieses Personenkreises verarbeitet werden. Ein wesentlicher Unterschied zur vormaligen Bargeldausgabe besteht darin, dass die FHH für die Auszahlung der Leistungen mittels Bezahlkarte auf privatwirtschaftlich organisierte Dienstleister zurückgreifen muss. Das Unternehmen Publk GmbH ist gemeinsam mit der Secupay AG der Vertragspartner der FHH für die notwendigen Bankleistungen.

In ihrer Kernfunktion ersetzt die Bezahlkarte damit die bis dato bei einer Behörde oder Kassenstelle stattfindende Bargeldausgabe. Zwar kann mit der SocialCard an Geldautomaten oder an der Supermarktkasse auch Bargeld abgehoben werden, allerdings ist der Abhebungsrahmen auf 50 Euro pro Monat begrenzt. Ansonsten kann mit der SocialCard nur in Geschäften bezahlt werden, die eine Kreditkartenzahlung ermöglichen. Überweisungen sind nicht zugelassen. Laut der Gesetzesbegründung verfolgt die Bezahlkarte damit das

Ziel, Geldzahlungen an Schleuser zu unterbinden (siehe BT-Drs. 20/11006, Seite 101 f.). Nach Schilderung der in der FHH für die Leistungsgewährung zuständigen Behörden soll sich mit der Bezahlkarte der Aufwand sowohl für die Verwaltung als auch für leistungsberechtigte Personen nachhaltig verringern, weil lediglich eine einmalige Einrichtung der Karte erforderlich ist und die – häufig mit langen Warteschlangen verbundene – monatliche Bargeldausgabe entfällt. Auch müsse keine größere Menge an Bargeld mehr in den Behörden vorgehalten werden, wodurch die entsprechenden Sicherheitsmaßnahmen obsolet würden.

Bei dem Entwicklungsprozess der SocialCard wurde der HmbBfDI nicht beteiligt. Erst durch eine Schriftliche Kleine Anfrage vom 29. August 2023 (Bü.-Drs. 22/12723) ist der HmbBfDI auf die unter Federführung der Kasse.Hamburg umgesetzte SocialCard aufmerksam geworden. Da das Vorhaben erkennbar mit einer weitergehenden automatisierten Verarbeitung von personenbezogenen Daten – im Vergleich zur vormals analogen Vorgehensweise – einhergeht, hat der HmbBfDI um Einbeziehung in die wesentlichen datenschutzrechtlichen Fragestellungen gebeten.

Nachdem die geplante Ausgestaltung der Bezahlkarte dem HmbBfDI auf Anfrage dargelegt worden ist, zeigten sich grundlegende Berührungspunkte mit dem Datenschutzrecht. In den anschließenden Dialog der Sach- und Rechtsfragen haben sich auch die behördlichen Datenschutzbeauftragten der Finanzbehörde, Sozialbehörde und der BIS eingebracht. Als in besonderem Maße erörterungsbedürftig erwiesen sich dabei die Frage der Rechtsgrundlage für die behördliche Datenverarbeitung, die technisch denkbare Möglichkeit zur Einsichtnahme in den Kontostand für die Leistungsbehörde sowie die Übermittlung der Ausländerzentralregister-Nummer (AZR-Nummer) an die eingebundenen Unternehmen. Das AsylbLG enthält keine spezialgesetzlichen Vorschriften zur Verarbeitung von personenbezogenen Daten, weshalb allein auf die Generalklausel zur Datenverarbeitung für öffentliche Stellen in § 4 HmbDSG als einschlägige Rechtsgrundlage zurückgegriffen werden kann. Nach die-

ser Norm ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle nur dann zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. Folglich dürfen die für die Umsetzung der Bezahlkarte zuständigen Behörden nur diejenigen personenbezogenen Daten verarbeiten, deren Verarbeitung für die Erfüllung der im AsylbLG bestimmten Aufgaben zwingend erforderlich ist. Aus datenschutzrechtlicher Perspektive kommt es also darauf an, welche konkreten Zwecke das AsylbLG vorgibt und welche Verarbeitungsvorgänge zur Erreichung dieser Zwecke unmittelbar benötigt werden. Die Einsichtnahme in den Kontostand zählt nicht dazu, ebenso wie die Übermittlung der AZR-Nummer. Aufgrund dieser datenschutzrechtlichen Grenzen sind diese Vorgehensweisen daher nicht zulässig (näher dazu https://datenschutz-hamburg.de/news/datenschutzrechtliche-grundlagen-einer-bezahlkarte-fuer-asylbewerberinnen).

Diese vom HmbBfDI vertretenen Standpunkte haben auch auf Bundesebene Eingang in die datenschutzrechtliche Auseinandersetzung mit der Bezahlkarte gefunden. Unter maßgeblicher Mitwirkung des HmbBfDI ist ein Positionspapier der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) entstanden und am 19. August 2024 veröffentlicht worden (siehe https://www.datenschutzkonferenz-online.de/media/dskb/2024_08_19_DSK_Beschluss_Bezahlkarte.pdf). Im Rahmen dieser Stellungnahme wurden noch weitere zentrale Aspekte ausformuliert, die aus der Perspektive des Datenschutzrechts bei der Umsetzung einer Bezahlkarte für Leistungen nach dem AsylbLG beachtet werden müssen. Problematisch sind bspw. pauschale räumliche Beschränkungen von Bezahlkarten, wodurch diese Karten nur innerhalb eines eng begrenzten Postleitzahlengebiets genutzt werden können. Zwar unterliegen leistungsberechtigte Personen häufig räumlichen Beschränkungen nach dem Asylgesetz oder dem Aufenthaltsgesetz. Allein dies rechtfertigt aber noch keine generelle Verknüpfung mit der Bereitstellung von existenzsichernden Leistungen, weil rechtskonforme Möglichkei-

ten zum temporären Verlassen des Aufenthaltsbereichs existieren. Es fehlt also an einer hinreichenden Zweckbestimmung im AsylbLG, die eine Datenverarbeitung für eine pauschale Beschränkung tragen könnte. In dem Positionspapier der DSK wird zudem klarstellend darauf hingewiesen, dass die für Behörden geltenden rechtlichen Grenzen in Bezug auf die Verarbeitung von personenbezogenen Daten durch die bei der Leistungsgewährung eingebundenen Unternehmen nicht ausgehöhlt werden dürfen.

Neben der Auseinandersetzung mit den oben genannten Punkten hat sich der HmbBfDI in einer Arbeitsgemeinschaft (AG) bestehend aus insgesamt vier Landesdatenschutzbehörden eingebracht, die vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit initiiert wurde. Diese AG ist in dem gemeinsamen Vergabeverfahren von 14 Bundesländern zur Einführung einer einheitlichen Bezahlkarte beratend hinzugezogen worden. Gegenstand und Ziel der Beratung war es, datenschutzrechtliche Vorgaben bereits im Zuge der Leistungsbeschreibung zu berücksichtigen. Durch die Einbeziehung der AG zu diesem frühen Zeitpunkt des Vorhabens bestand die Möglichkeit, während des Vergabeverfahrens Einfluss zugunsten einer datenschutzkonformen Gestaltung auszuüben. So hat die AG unter anderem auf zu weitgehende Aufgabenübertragungen und damit einhergehende Befugnisse der Dienstleister hingewiesen, die sich nicht mit den Anforderungen nach Art. 32 DSGVO vereinbaren lassen. Auch im Nachgang an die Vergabeentscheidung ist die Arbeitsgemeinschaft bei der Entwicklung eines Musters für die gebotene Datenschutz-Folgenabschätzung einbezogen worden.

Voraussichtlich zum Februar 2025 soll die einheitliche Bezahlkarte in 14 Bundesländern – einschließlich der FHH – ausgegeben werden. Bereits jetzt zeichnet sich ein unabweisbares praktisches Bedürfnis ab, Überweisungen und Lastschriftmandate in gewissem Umfang zuzulassen, um unbedenkliche Zahlungsvorgänge wie etwa Mobilfunkverträge oder Mitgliedschaften in Sportvereinen für leistungsberechtigte Personen zu ermöglichen. Es sind verschiedene Lösungen denkbar, wie Zahlungen freigeschaltet werden können. Der HmbBfDI

wird dabei darauf hinwirken, dass ein Konzept gewählt wird, das sowohl für leistungsberechtigte Personen als auch für Zahlungsempfänger:innen mit einer möglichst geringen Eingriffsintensität verbunden ist.

5. Messenger-Dienste in der Jugendarbeit

Dem Einsatz von Messenger-Diensten kommt gerade in der Kinder- und Jugendarbeit eine besondere praktische Bedeutung zu, so dass der HmbBfDI einen Flyer zum Thema „Messenger-Dienste in der Kinder- und Jugendarbeit" veröffentlichte, um verantwortlichen Stellen aus diesem Bereich klare Rahmenbedingungen für den Einsatz an die Hand zu geben.

Der HmbBfDI veröffentlichte am 24. Juli 2024 einen Flyer zum Umgang mit Messenger-Diensten im Bereich der Jugendarbeit (https://datenschutz-hamburg.de/news/messenger-dienste-in-der-kinder-und-jugendarbeit) und empfiehlt darin eine datensparsame und zurückhaltende Nutzung. Träger bemängeln zumeist, dass sie die Jugendlichen oft nicht mehr richtig erreichen können und dass der Einsatz von Messenger-Diensten zur Koordination ihrer Arbeit immer relevanter wird. Wichtig ist jedoch, dass die Möglichkeiten des Messenger-Dienstes nicht in solchen Bereichen ausgeschöpft werden, in denen dies zu unnötigen Datenverarbeitungen führt, die lediglich eine Erleichterung für den Alltag der Einrichtung bedeuten. Insbesondere muss der persönliche Kontakt zu den Kindern und Jugendlichen erhalten bleiben. Eine Verlagerung der Arbeit in den digitalen Raum unter Nutzung von Messenger-Diensten stellt sich wegen der intransparenten und eingriffsintensiven Verarbeitungspraktiken vieler Messenger-Dienste als problematisch dar.

Der HmbBfDI hielt fest, dass die Verantwortung für den Einsatz bei der verwendenden Einrichtung liegt und dass sich diese vorab Ge-

danken zum Einsatz machen und Nutzungsvorgaben festlegen muss. Am 14. Oktober 2024 stellte der HmbBfDI den Flyer in einer Austauschveranstaltung mit diversen Jugendhilfeträgern vor und diskutierte die Möglichkeiten der Träger.

6. Entwicklungsdokumentation im Kindergarten

Bei der Datenverarbeitung in Kindertagesstätten lässt sich eine Anfertigung und Nutzung von Fotografien betreuter Kinder nicht mit der Pflicht zur Entwicklungsdokumentation rechtfertigen.

Den HmbBfDI erreichen immer wieder Beschwerden über die Anfertigung von Fotos in Kitas. In diesen Fällen haben die Sorgeberechtigten (i.d.R. die Eltern) meist nicht bei Vertragsschluss in eine Fotoanfertigung des betroffenen Kindes eingewilligt. Die verantwortlichen Kitabetreiber tragen häufig pauschal vor, dass die kritisierte Fotoanfertigung auf Grundlage einer verpflichtenden Entwicklungsdokumentation erfolgt ist. Dies findet jedoch keine gesetzliche Stütze.

Die Anfertigung der Fotos der Kinder wird zumeist mit unterschiedlichen Zwecken begründet. Einerseits sollen die Fotos den Eltern einen Einblick in den Alltag des Kitabetriebs erlauben und andererseits soll durch sie ein Teil der gesetzlich vorgeschriebenen Entwicklungsdokumentation abgedeckt werden. In vielen Kitas ist es Praxis, dass die angefertigten Fotos gesammelt und zum Ende der Betreuung – etwa in einer Mappe – an das betroffene Kind übergeben werden, damit dies ein Erinnerungsstück an die Zeit im Kindergarten hat. In anderen Einrichtungen werden die Eltern über eine eigene Verwaltungs-App oder gängige Messenger-Dienste regelmäßig mit Fotos der Kinder versorgt, damit sie über aktuelle Ereignisse in der Einrichtung auf dem Laufenden bleiben. Dies geschieht regelmäßig ohne vorherige Absprache mit den Eltern und diese wundern sich über plötzlich erhaltene Fotos.

Eine Kita hat gem. § 22 Abs. 2 u. 3 i.V.m. § 22a SGB VIII die Entwicklung des betreuten Kindes zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu fördern. § 2 des Hamburger Kinderbetreuungsgesetzes (KibeG) sieht vor, dass Tageseinrichtungen die Erziehung und Bildung des Kindes in der Familie durch alters- und entwicklungsgemäße pädagogische Angebote zu fördern, ergänzen und unterstützen haben. § 6 KibeG spricht gar von einem Anspruch auf Förderung jedes Kindes vom vollendeten ersten Lebensjahr an. Dieser an unterschiedlicher Stelle beschriebene Förderauftrag ist integraler Bestandteil der fachlichen und pädagogischen Arbeit einer Kita und füllt das Betreuungsverhältnis mit Leben. Die pädagogischen Fachkräfte leisten mit ihrer Arbeit einen wichtigen und wesentlichen Beitrag für die Entwicklung des Kindes.

Es liegt nahe, dass die Kitas in diesem Zusammenhang auch die Entwicklung und Förderungsergebnisse dokumentieren wollen. Häufig werden dabei Notizen angefertigt, die später eine Grundlage für das Einzelgespräch mit den Eltern (§ 24 Abs. 1 KibeG) darstellen. In diesen Gesprächen haben die Betreuer:innen über den Entwicklungsstand des Kindes, seine besonderen Interessen und Fähigkeiten sowie geplante Maßnahmen zur gezielten Förderung zu berichten. Aber weder die genannten Regelungen noch eine andere des Kinderbetreuungsgesetzes sehen vor, dass die Entwicklungsdokumentation anhand von Fotoaufnahmen erfolgen soll. Die Entwicklung eines Kindes ist vielmehr primär an die elterliche Erziehungspflicht und das elterliche Erziehungsrecht gebunden. Kitas nehmen hier eine unterstützende Rolle ein. So sieht § 22a Abs. 2 S. 2 SGB VIII sogar vor, dass Eltern an den Entscheidungen in wesentlichen Angelegenheiten der Erziehung, Bildung und Betreuung zu beteiligen sind, was auch kindbezogene Einzelentscheidungen umfasst. Die Kitas haben Erziehungsmaßnahmen der Eltern demnach zu berücksichtigen und zu respektieren. Die Anfertigung und Nutzung von Fotos der Kinder im Rahmen einer Entwicklungsdokumentation sind daher problematisch, wenn die Eltern eine solche Form der Dokumentation strikt ablehnen. Es wäre widersprüchlich eine Fotoanfertigung für eine Entwicklungsdokumentation vor-

zunehmen, die sich insbesondere an die Eltern richten soll, wenn diese eine Fotoanfertigung gar nicht wollen. Als einzig zulässige Rechtsgrundlage für regelmäßige Fotoanfertigungen verbleibt daher die Einwilligung der Sorgeberechtigten.

Wenn Kitas die Eltern bei Vertragsschluss über die vorgesehene Praxis der Fotoanfertigung informieren und dafür eine Einwilligung einholen, werden Überraschungen und Missverständnisse verhindert und die gewünschte Dokumentation kann auf einer rechtmäßigen Grundlage erfolgen. Wenn eine Einwilligung nicht erfolgt, hat eine Fotoanfertigung im Kita-Alltag zu unterbleiben.

7. UKE – neues Krankenhausarbeitsplatzsystem (nextKAS)

Nach Einbindung in die Umstellung des bisherigen Arbeitsplatzsystems im Universitätsklinikum Hamburg-Eppendorf (UKE) auf eine alternative Software in den Jahren 2022 und 2023 hat der HmbBfDI die Beratung im Frühjahr 2024 abgeschlossen, und Hinweise gegeben, welche datenschutzrechtlichen Anforderungen mit Projektende und Inbetriebnahme des neuen Systems im gesamten UKE-Konzern noch erfüllt sein müssen.

Ende 2023 hatte der HmbBfDI angemahnt, dass es einer weitergehenden Berücksichtigung datenschutzrechtlicher Vorgaben in mehreren Bereichen des Projekts zur Einführung des neuen Krankenhausarbeitsplatzsystems (KAS) Clinical G3 / NAVIS bedarf (vgl. 32. TB, Kapitel III 10). Daraufhin hat das UKE nachgeschärft und dazu im Januar/Februar 2024 auch eine ergänzte bzw. überarbeitete Datenschutzdokumentation zur Verfügung gestellt. Diese vermochte die datenschutzrechtliche Bewertung jedoch noch nicht grundlegend zu ändern.

Im März 2024 hat der HmbBfDI mit Blick auf die Projektdynamik die Beratung mit einem zusammenfassenden Schreiben beendet. Die-

ses enthielt Hinweise auf noch offene sowie auf solche Punkte, die unbedingt weiterhin nachgebessert werden müssen. Dazu zählten unter anderem die Ermittlung sämtlicher, mit der Inbetriebnahme von Clinical G3 / NAVIS im gesamten UKE-Konzern einhergehender Risiken und zu deren Bewältigung vorgesehener technischer und organisatorischer Abhilfemaßnahmen, das Rollen- und Berechtigungskonzept und Einzelthemen wie das Löschen und Aufbewahren oder die Umsetzung der Betroffenenrechte.

Der Go-Live des neuen KAS startete im Berichtsjahr dann zunächst in einem Teilbereich des Altonaer Kinderkrankenhauses (AKK), für die weiteren Bereiche der Kinderklinik wurde es verschoben. Die vollständige Ablösung des alten KAS auch in den weiteren Kliniken des UKE-Konzerns hat sich dadurch ebenfalls verzögert und konnte bislang nicht umgesetzt werden.

Die Teileinführung von nextKas war im November 2024 auch Gegenstand der Berichterstattung in einem Online-Nachrichtenmagazin. Mit Blick auf Presseanfragen und eine Beschwerde ist der HmbBfDI ebenfalls im November mit konkreten Fragen zum Einsatz von Clinical G3 / NAVIS im AKK an das UKE herangetreten. Diese Fragen betrafen die Anmeldung zum System und den Zugriff auf Daten von Patient:innen durch Beschäftigte im AKK sowie die Richtigkeit der in diesem Zusammenhang und bei der weiteren Dokumentation im System verarbeiteten Informationen. Die Fragen konnten für den HmbBfDI nachvollziehbar beantwortet werden. Ein Ansatzpunkt für eine weitergehende Prüfung des neuen Systems im AKK hat sich nicht ergeben.

Es bleibt festzustellen, dass der Zeitplan der vollständigen Implementierung von Clinical G3 / NAVIS im gesamten UKE-Konzern weiterhin nicht feststeht und dass noch offen ist, wie es gelingen kann, bis dahin auch die datenschutzrechtlichen Anforderungen vollständig umzusetzen. Das wird der HmbBfDI deshalb weiterhin in den Blick nehmen.

8. Umsetzung des Gesundheitsdatennutzungsgesetzes

Am 26. März 2024 ist das Gesundheitsdatennutzungsgesetz (GDNG) in Kraft getreten. Mit diesem Gesetz sollen Gesundheitsdaten außerhalb des unmittelbaren Versorgungskontextes u.a. zu Forschungszwecken nutzbar gemacht werden. Eine Weitergabe der personenbezogenen Behandlungsdaten an Dritte ist in diesem Zusammenhang grundsätzlich untersagt, kann aber unter bestimmten Voraussetzungen in die Zustimmung der zuständigen Datenschutzaufsichtsbehörde gestellt werden.

Das entsprechende Zustimmungsverfahren ist in Artikel 6 Abs. 3 GDNG geregelt. Darüber hinaus enthält die Norm weitere Ausnahmen vom grundsätzlichen Verbot der Weitergabe von Versorgungsdaten an Dritte zu den in Abs. 1 genannten Zwecken, und zwar die Einwilligung der betroffenen Person(en) sowie andere gesetzliche Vorschriften des Bundesrechts, des Landesrechts oder unmittelbar geltender Rechtsakte der Europäischen Union, die eine Weitergabe dieser Daten erlauben. Zum Verhältnis von Art. 6 Abs. 3 GDNG zu landesrechtlichen Vorschriften stellen sich ebenso Fragen wie zur konkreten Ausgestaltung des Zustimmungsverfahrens oder auch zu den neuen Zuständigkeitsregelungen zur Datenschutzaufsicht bei länderübergreifenden Gesundheitsforschungsvorhaben nach Art. 5 GDNG. Der Klärung dieser für die Forschenden wichtigen Fragen hat sich im Berichtsjahr eine Arbeitsgruppe (AG) der Taskforce Forschungsdaten angenommen. Der HmbBfDI beteiligt sich an dieser AG, auch weil für die Krankenhäuser in Hamburg, die an der stationären Versorgung der Bevölkerung teilnehmen, mit § 12 Hamburgisches Krankenhausgesetz (HmbKHG) bereits vor Geltungsbeginn des GDNG eine Vorschrift existiert hat, die die Weiterverarbeitung von Behandlungsdaten zu wissenschaftlichen Forschungszwecken unter bestimmten Voraussetzungen erlaubt. Insoweit stellt sich die zuvor angesprochene Frage des Verhältnisses der Norm des HmbKHG zum GDNG, deren Klärung der HmbBfDI in der AG anstrebt.

Wie in der Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 24.11.2022 zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung gefordert (sogenannte Petersberger Erklärung, vgl. https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf), enthält das GDNG in § 7 Geheimhaltungspflichten der Datennutzenden. Verstöße gegen diese Pflichten sind gemäß § 9 GDNG unter Strafe gestellt. Dass diese Forderung aufgegriffen wurde, ist zu begrüßen.

9. Elektronische Patientenakte für alle

Am 26. März 2024 ist das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) in Kraft getreten. Kernelement des Gesetzes ist die elektronische Patientenakte (ePA) für alle. Die gesetzlichen Krankenkassen müssen sie ihren Versicherten beginnend ab dem 15. Januar 2025 bereitstellen, wenn diese nicht nach Erhalt einer vorherigen Information der Einführung widersprochen haben.

Die ePA für alle wird ab Mitte Januar in Hamburg und Umland sowie in Franken und in Teilen von Nordrhein-Westfalen getestet, bevor sie bundesweit ausgerollt wird. Bei Hamburg, Franken und Umland handelt es sich um sogenannte Modellregionen für digitale Gesundheit, in denen Anwendungen und Dienste der Telematikinfrastruktur (TI), der zentralen Plattform für digitale Anwendungen im deutschen Gesundheitswesen, erstmalig erprobt und auf ihre Nutzbarkeit geprüft werden (vgl. 32. TB, Kapitel III 9). Die Erfahrungen der Nutzenden in diesen Modellregionen fließen in die Weiterentwicklung der Anwendungen / Dienste ein. Der HmbBfDI hat in 2024 die Erprobung des TI-Messengers in der Modellregion Hamburg und Umland begleitet. In 2025 wird er die Pilotierung und den weiteren Einsatz der ePA für

alle durch Ärzt:innen und andere Leistungserbringer in Hamburg und Umland betrachten.

Bei der ePA für alle handelt es sich um eine von der versicherten Person selbst geführte Akte, auf die in deren Behandlung eingebundene Ärzt:innen und weitere Leistungserbringer mit dem Stecken der Versichertenkarte grundsätzlich Zugriff erhalten. Dort können relevante medizinische Daten, wie z.B. Behandlungsdokumentationen, Therapiepläne, Medikamentenverschreibungen, abgelegt werden.

Im Sommer 2024 haben die Krankenkassen damit begonnen, ihre Mitglieder zur Einführung der ePA für alle zu informieren und u.a. darüber aufzuklären, dass der Bereitstellung widersprochen werden kann, sogenanntes Opt-out-Verfahren. Dazu und zu weiteren Inhalten des Informationsschreibens der Krankenkassen hat der HmbBfDI auf seiner Webseite einen Beitrag veröffentlicht (s. https://datenschutz-hamburg.de/news/aktuelle-post-der-krankenkassen-zur-einfuehrung-der-elektronischen-patientenakte-epa). Darin hat er u.a. darauf hingewiesen, dass Versicherte, die der Einrichtung der ePA für alle vorab nicht widersprochen haben, jederzeit die teilweise oder vollständige Löschung von Daten der ePA verlangen können, § 343 Abs. 1a Nr. 5c Sozialgesetzbuch (SGB) Fünftes Buch (V). Umgekehrt ist es auch solchen Versicherten, die widersprochen haben, zu einem späteren Zeitpunkt noch möglich, die Einrichtung einer ePA zu beantragen, § 343 Abs. 1a Nr. 5b SGB V. Wenn die elektronische Patientenakte bereitgestellt wurde, bestehen darüber hinaus vielschichtige Gestaltungsmöglichkeiten, deren Ausübung allerdings eine intensive Befassung mit der Thematik erfordert.

Es versteht sich von selbst, dass die in der ePA geführten Gesundheitsdaten als sehr sensible Daten einer besonders guten technischen Absicherung bedürfen. Das ePA-Sicherheitskonzept der gematik GmbH, die die Gesamtverantwortung für die TI trägt, ist von einem Forschungsteam des Fraunhofer-Instituts für Sichere Informationstechnologie SIT überprüft und im Oktober 2024 für angemessen befunden worden. Der gematik GmbH wurden in

diesem Zusammenhang technische und organisatorische Verbesserungsvorschläge unterbreitet (s. dazu https://www.sit.fraunhofer.de/de/presse/details/news-article/show/neues-epa-sicherheitskonzept-auf-dem-pruefstand/). Allerdings wurde kurz vor Redaktionsschluss für diesen Tätigkeitsbericht im Rahmen des 38th Chaos Communication Congress' des Chaos Computer Clubs (CCC) demonstriert, dass und wie unberechtigte Personen Zugang zur ePA für alle erlangen können (s. dazu https://www.ccc.de/de/updates/2024/ende-der-epa-experimente). Die Sicherheit der ePA wird daher für die Verantwortlichen auch zukünftig eine große und prioritäre Herausforderung sein.

10. Gesundheitsdaten auf Lohn- und Gehaltsabrechnungen – Zwischen Transparenz und Datenschutz

Arbeitgeber und Dienstherren vermerken sensible Gesundheitsdaten auf Lohn- und Gehaltsabrechnungen. Ist dies ein notwendiger Schritt zur Lohntransparenz oder ein unzulässiger Eingriff in die Privatsphäre der Beschäftigten? Eine datenschutzrechtliche Gratwanderung, die Arbeitnehmer und Beamte gleichermaßen betrifft und grundlegende Fragen zum Umgang mit sensiblen Daten im Arbeitsleben aufwirft.

Der HmbBfDI wird regelmäßig gefragt, ob Gesundheitsdaten auf Lohn- und Gehaltsabrechnungen und Bezügemitteilungen aufgeführt werden dürfen. Aufgrund von zwei konkreten Beschwerden führte der HmbBfDI eine Prüfung der Zulässigkeit dieser Praxis durch.

Die erste Beschwerde betraf die Angabe eines zusätzlichen Urlaubsanspruchs aufgrund einer Schwerbehinderung auf den Gehaltsabrechnungen eines Arbeitnehmers. Er monierte, dass die Angabe der Gesundheitsdaten auf seinen Gehaltsabrechnungen Nachteile bedeuten könnte, wenn diese an Dritte weitergegeben werden müssten. Die zweite Beschwerde richtete sich gegen die Angabe der

krankheitsbedingten Arbeitsunfähigkeit samt Zeitraum auf der Bezügemitteilung einer Beamtin der Freien und Hansestadt Hamburg.

Der HmbBfDI stellte fest, dass weder die Gewerbeordnung (GewO) noch die Entgeltbescheinigungsverordnung (EntgBV) die Angabe zusätzlicher personenbezogener Daten auf Abrechnungen explizit verbieten, da diese Regelwerke lediglich Mindeststandards für den Inhalt festlegen. Die Verarbeitung von Gesundheitsdaten auf Lohn- und Gehaltsabrechnungen und Bezügemitteilungen unterliegt den strengen Anforderungen der DSGVO, insbesondere Artikel 9 DSGVO. Mögliche Rechtsgrundlagen sind Art. 9 Abs. 2 lit. b) DSGVO in Verbindung mit arbeits- und sozialrechtlichen Vorschriften sowie Art. 9 Abs. 2 lit. f) DSGVO i.V.m. § 26 Abs. 3 BDSG; § 10 Abs. 2 i.V.m. Abs. 3 HmbDSG und § 10 Abs. 3 HmbDSG i.V.m. §§ 85 bis 92 des HmbBG und Art. 6 Abs. 1 DSGVO.

Nach diesen Vorschriften dürfen Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies erforderlich ist. Die Prüfung der Erforderlichkeit umfasst dabei nicht nur die Frage, ob die Datenverarbeitung zur Erreichung des Zwecks geeignet und notwendig ist, sondern auch eine Abwägung der widerstreitenden Interessen und Grundrechtspositionen von Arbeitgeber und Beschäftigten. Ziel ist es, einen angemessenen Ausgleich zwischen den berechtigten Interessen des Arbeitgebers an der Datenverarbeitung und dem Schutz der Persönlichkeitsrechte der Beschäftigten herzustellen. Die Abwägung erfolgt im Sinne einer „praktischen Konkordanz“, die darauf abzielt, beide Interessen möglichst weitgehend zu berücksichtigen und in Einklang zu bringen. Dies bedeutet insbesondere, dass mildere Mittel geprüft werden müssen, um die Rechte der betroffenen Person möglichst zu schonen.

Für besondere Kategorien personenbezogener Daten ist eine noch intensivere Interessenabwägung erforderlich. Hier darf kein Grund zur Annahme bestehen, dass ein überwiegendes schutzwürdiges Interesse der betroffenen Person an dem Ausschluss der Verarbeitung vorliegt.

Der HmbBfDI empfiehlt Arbeitgebern und Dienstherren in vergleichbaren Situationen, die Erforderlichkeit der Angabe von Gesundheitsdaten auf Abrechnungen sorgfältig zu prüfen und die Rechte der Betroffenen zu berücksichtigen. Die Verarbeitung muss stets im Einklang mit den datenschutzrechtlichen Grundsätzen, insbesondere der Zweckbindung und Datenminimierung, erfolgen. Zwar sind Verarbeitungsmöglichkeiten denkbar, die dem Datenminimierungsgrundsatz gerechter werden könnten. Allerdings widerspricht eine Aussparung der Gesundheitsdaten dem Transparenzgedanken des § 108 GewO. Ohne diese Angaben wären Arbeitnehmer oder Beamte in ihren Möglichkeiten eingeschränkt, die entsprechenden Informationen zu prüfen und bei Unstimmigkeiten Widerspruch anzumelden.

Zusätzlich ist zu beachten, dass Lohn- und Gehaltsabrechnungen oft von Dritten angefordert werden. Der Gesetzgeber hat dies berücksichtigt und z.B. in § 2 Abs. 2 EntgBV die Möglichkeit zur Schwärzung des Kirchensteuermerkmals eingeräumt. Dies impliziert, dass auch andere sensible Daten grundsätzlich geschwärzt werden dürfen, wenn sie für den jeweiligen Zweck nicht erforderlich sind. In diesem Sinne ist die konkrete Verarbeitungssituation zu berücksichtigen. Grundsätzlich werden die fraglichen Gesundheitsdaten dergestalt verarbeitet, dass sie nur dem Arbeitnehmer bzw. Beamten offenbart werden – also denjenigen Personen, die die Daten betreffen. Andere Personen haben somit keine Möglichkeit der Kenntnisnahme, wenn der Betroffene eine Schwärzung vornimmt.

Im Ergebnis verstößt die Angabe der Gesundheitsdaten auf der Lohn- und Gehaltsabrechnung bzw. Bezügemitteilung aus Gründen der Transparenz, des engen Verarbeitungskontexts und der Möglichkeit des Betroffenen, bei Weitergabe an Dritte diese Daten unkenntlich zu machen, nicht gegen den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) DSGVO und damit nicht gegen die DSGVO.

11. Beschäftigtendaten(schutz)gesetz: Hoffnung oder Enttäuschung – Der geleakte Entwurf und seine Folgen

Der geleakte Entwurf des Beschäftigtendatengesetzes (BeschDG-E) weckte langjährige Hoffnungen und versprach bedeutende Fortschritte im Schutz von Beschäftigtendaten. Das Scheitern der Bundesregierung bedeutet auch das Scheitern des Entwurfs und hinterlässt weiterhin eine Lücke in der dringend benötigten Modernisierung des Beschäftigtendatenschutzes.

Bereits im Tätigkeitsbericht 2023 wurden die Entwicklungen im Bereich des Beschäftigtendatenschutzes und ein geplantes Beschäftigtendatenschutzgesetz thematisiert. Besondere Aufmerksamkeit galt damals dem Urteil des Europäischen Gerichtshofs vom 30. März 2023 (Az. C-34/21), das Zweifel an der Konformität des § 26 Abs. 1 Satz 1 BDSG mit dem EU-Recht aufwarf. Der HmbBfDI hatte als erste Aufsichtsbehörde mit einer Pressemitteilung vom 3. April 2023 zu diesem Urteil Stellung genommen und sowohl Unternehmen als auch den Hamburgischen Gesetzgeber aufgefordert, die verwendeten Rechtsgrundlagen erneut zu prüfen. Gleichzeitig hat er aber betont, dass trotz des EuGH-Urteils Datenverarbeitungsvorgänge im Beschäftigtenkontext nicht ohne Rechtsgrundlage sind. Art. 6 Abs. 1 lit. b DSGVO gilt weiterhin als unmittelbare Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erfüllung eines Arbeitsvertrages. Politische Bestrebungen zur Schaffung eines eigenständigen Gesetzes zum Beschäftigtendatenschutz wurden unterstützt.

Aufbauend auf dieser Vorarbeit beleuchtet der aktuelle Tätigkeitsbericht 2024 nun den jüngst geleakten Entwurf des Beschäftigtendatenschutzgesetzes, der einen bedeutenden Schritt in der Weiterentwicklung des Datenschutzrechts im Arbeitskontext hätte darstellen können.

Auffallend ist zunächst, dass die Ministerien für Arbeit und Soziales und das Bundesministerium des Innern und für Heimat sich für einen Entwurf mit der Bezeichnung „Entwurf eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt", kurz Beschäftigtendatengesetz – BeschDG entschieden haben. Es geht hier also nicht primär um den Beschäftigtendatenschutz, sondern um die Beschäftigtendaten. Ein Grund hierfür könnte darin bestanden haben, dass das Gesetz sich nicht auf den Schutz der Daten der Beschäftigten beschränken, sondern auch Regelungen für deren Nutzung schaffen sollte.

Der Entwurf adressiert mehrere kritische Bereiche: Zunächst werden klare Richtlinien für den Umgang mit Bewerberdaten festgelegt. Der allgemeine Teil beschäftigt sich hierfür mit grundsätzlichen Regelungen für Verarbeitungssituationen im Beschäftigtenkontext. Im besonderen Teil wird Bezug auf einzelne, konkrete Verarbeitungssituationen genommen. Der Entwurf zielt darauf ab, die Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten zu präzisieren, was direkt auf die im Vorjahr diskutierten Probleme mit § 26 Abs. 1 S. 1 BDSG reagiert. Schließlich berücksichtigt der Gesetzesentwurf die zunehmende Nutzung von KI-Technologien und versucht, einen angemessenen Rahmen für deren Einsatz zu schaffen.

Grundsätzlich war die Initiative zur Schaffung eines spezifischen Beschäftigtendatengesetzes zu begrüßen. Bei aller Kritik an den geschaffenen Regelungen, auf welche hier nicht im Einzelnen eingegangen werden soll, sollte der Blick konstruktiv in die Zukunft gerichtet werden, um dieses Vorhaben in der Zukunft möglicherweise irgendwann rechtskonform umzusetzen.

Der geleakte Entwurf hätte ein wichtiger Schritt zur Modernisierung des Beschäftigtendatenschutzes werden können, auch wenn Änderungen hier unabdingbar gewesen wären. Entscheidend wäre gewesen, eine finale Fassung sorgfältig auszuarbeiten, um den He-

rausforderungen der digitalen Arbeitswelt gerecht zu werden und gleichzeitig die Grundrechte der Beschäftigten zu wahren sowie einer übermäßigen Bürokratisierung eines ohnehin schon schwierigen Themenkomplexes vorzubeugen. Wichtig ist ein ausgewogenes Verhältnis zwischen den Interessen der Arbeitgeber und dem Schutz der Privatsphäre der Beschäftigten zu finden. Besonders hervorzuheben war die Bedeutung der menschlichen Überprüfung bei automatisierten Entscheidungsprozessen. Niemand sollte verpflichtet sein, sich ausschließlich automatisierten Entscheidungen zu unterwerfen, wie es Art. 22 DSGVO vorsieht. Die Verarbeitung von Beschäftigtendaten durch Profiling sollte demnach nur zulässig sein, wenn sie nicht bereits nach Art. 22 DSGVO ausgeschlossen ist und die Interessen des Arbeitgebers die der Beschäftigten „erheblich überwiegen". Ob diese zusätzliche Anforderung DSGVO-konform ist, wurde in der Literatur teilweise angezweifelt.

Wäre eine solche Neuregelung nachgebessert und verabschiedet worden, hätten sich Arbeitgeber darauf einstellen müssen, ihr bestehendes Vertragswerk (Arbeitsverträge, Betriebsvereinbarungen etc.) sowie ihre betrieblichen Abläufe sowie Bewerbungsverfahren einer umfassenden datenschutzrechtlichen Überprüfung zu unterziehen. Der Referentenentwurf birgt trotz einiger Schwächen und Widersprüche wertvolle Ansätze und Überlegungen, die für zukünftige Gesetzgebungsprozesse genutzt werden könnten und sollten. Eine Analyse der Struktur und der wesentlichen Regelungen führt dazu, dass der Entwurf eine umfassende Grundlage für Diskussionen und Verbesserungen bieten kann, so dass dessen Scheitern hier als Chance verstanden werden sollte.

12. Positionspapier "Bewerberdatenschutz und Recruiting im Fokus"

Der digitale Wandel in der Arbeitswelt führt zu einem Paradigmenwechsel bei der Personalgewinnung: Klassische Bewerbungsverfahren verlieren an Bedeutung, während proaktive Methoden wie Active Sourcing und Headhunting sowie der verstärkte Einsatz von Social Media zunehmend an Bedeutung gewinnen. Diese Entwicklung stellt Unternehmen vor neue datenschutzrechtliche Herausforderungen. Um Bewerberdaten angemessen zu schützen und den Verantwortlichen klare Grenzen und datenschutzkonforme Möglichkeiten aufzuzeigen, hat der HmbBfDI das Positionspapier „Bewerberdatenschutz und Recruiting im Fokus" am 6.6.2024 veröffentlicht.

Die rasante Entwicklung digitaler Technologien und die damit einhergehende Transformation der Arbeitswelt haben tiefgreifende Auswirkungen auf Bewerbungsprozesse. Unternehmen setzen zunehmend auf innovative Methoden, um geeignetes Personal zu finden und anzusprechen. Diese Veränderungen bringen jedoch neue datenschutzrechtliche Herausforderungen mit sich.

Der HmbBfDI hat auf diese Entwicklung reagiert und am 6.6.2024 ein umfassendes Positionspapier zum Thema Bewerberdatenschutz und Recruiting veröffentlicht, das als Orientierungshilfe für Unternehmen, Personalabteilungen und für Bewerbende dient (abzurufen unter: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240606_Information_Bewerberdatenschutz_und_Recruiting.pdf). Das Papier adressiert die gängigen Fragestellungen, die sich aus dem Spannungsfeld zwischen modernen Methoden zur Personalgewinnung und dem Schutz personenbezogener Daten ergeben.

Bewerbungsunterlagen enthalten eine Vielzahl sensibler Daten. Ein sorgfältiger und diskreter Umgang mit diesen Informationen ist von

höchster Bedeutung. Seit Jahren verzeichnet der HmbBfDI zahlreiche Beschwerden und Beratungsanfragen zu Bewerbungsverfahren. Insbesondere der zunehmende Einsatz proaktiver Methoden wie Active Sourcing und Headhunting, die verstärkte Nutzung von Social Media und Internetrecherchen sowie der Einsatz automatisierter Verfahren und künstlicher Intelligenz bei der Bewerbungssichtung werfen komplexe datenschutzrechtliche Fragen auf, die im Positionspapier behandelt werden.

Um den Einstieg in die Thematik zu erleichtern, wird zunächst ein umfassender Überblick über aktuelle rechtliche Entwicklungen gegeben, insbesondere das EuGH-Urteil vom 30.3.2023 (Az. C-34/21) und dessen Auswirkungen auf den Beschäftigtendatenschutz in Deutschland (siehe hierzu auch die Pressemitteilung des HmbBfDI vom 03.04.2023). Bei der Verarbeitung von Bewerber:innendaten gelten die Prinzipien der DSGVO, insbesondere die Rechtmäßigkeit, Zweckbindung und Datenminimierung, wobei die Erforderlichkeit der Datenverarbeitung im Kontext des Beschäftigungsverhältnisses zentral ist. In der Praxis zeigt sich ein erhöhter Beratungsbedarf bezüglich der Informationspflichten nach Art. 13 und 14 DSGVO, da diese oft vernachlässigt werden oder Bewerber:innen sich unzureichend informiert fühlen.

Zudem werden wichtige Begriffe wie beispielsweise „Recruiting“ oder „Active Sourcing“ klar definiert, um eine einheitliche Verwendung zu gewährleisten. Im Bereich der Personalgewinnung war es notwendig, Definitionen zu finden, um den zahlreichen Anglizismen gerecht zu werden, da diese Begriffe oft unterschiedlich interpretiert und verwendet werden und eine einheitliche Kommunikation und Verständigung zwischen Unternehmen und Bewerbern sichergestellt werden muss. Aus diesem Grunde hat der HmbBfDI seine eigenen Definitionen der wichtigsten Begriffe im Recruiting in dem Papier zur Verfügung gestellt.

Daneben enthält das Papier konkrete Handlungsempfehlungen für die vier Hauptphasen des Recruitingprozesses: Erstkontakte, Be-

werbungsverfahren, Anstellungsverhältnis und dessen Beendigung. Jede Phase wird detailliert hinsichtlich der datenschutzrechtlichen Anforderungen beleuchtet.

Auch die Aufnahme in Talentpools, die nur mit einer Einwilligung möglich ist, sowie Background-Checks, die sich am Fragerecht im Bewerbungsgespräch orientieren, werden praxisnah beleuchtet und vom HmbBfDI bewertet. Hierbei waren z.B. die Reichweite der Einwilligung, konkrete Speicherdauer in unterschiedlichen Konstellationen und unterschiedliche Verantwortlichkeiten zu berücksichtigen.

Ein weiterer Fokus des Positionspapiers liegt auf dem Einsatz von Künstlicher Intelligenz im Recruiting, insbesondere bei der Nutzung von Lebenslaufparsern und Emotionsanalysen. Lebenslaufparser werden unter bestimmten Bedingungen als zulässig erachtet, während Emotionsanalysen grundsätzlich als unzulässig eingestuft werden.

Das Positionspapier wurde in Fachkreisen positiv aufgenommen und als praxisnaher Leitfaden geschätzt, der konkrete Handlungsempfehlungen für die Umsetzung des Datenschutzes im Bewerbungsverfahren bietet.

Seit der Veröffentlichung des Positionspapiers wurden zahlreiche Anfragen gestellt, die sich auf die darin behandelten Problemkreise bezogen. Diese Anfragen ermöglichten einen konstruktiven Austausch und eine detaillierte Konkretisierung der einzelnen Punkte. Die Beispiele zeigen, dass die Veröffentlichung zu konkreten Verbesserungen im Einzelfall beigetragen hat.

13. Betrugswelle auf Buchungsportalen von Hotels

Im Jahr 2024 konnte der HmbBfDI eine Zunahme von Betrugsfällen im Zusammenhang mit Hotelbuchungen über Online-Plattformen feststellen. Diese Vorfälle werfen nicht nur Fragen zur IT-Sicherheit auf, sondern Stellen alle Beteiligten vor datenschutzrechtliche Probleme. Die Betrüger nutzen gestohlene oder manipulierte Daten, um täuschend echte oder tatsächlich echte Nachrichten aus der Infrastruktur der Hotels zu versenden und Zahlungsinformationen der Hotelgäste zu erbeuten. Der folgende Bericht beleuchtet die datenschutzrechtlichen Aspekte dieser Fälle und gibt Empfehlungen zur Prävention

Die Betrugsmaschen basieren häufig auf Phishing-Angriffen, bei denen Kriminelle Zugang zu Buchungsdaten erlangen. Die Ursachen und Schwachstellen dieser Angriffe sind dabei oftmals genauso vielseitig wie unklar. Daten werden z.B. durch Schadsoftware auf Hotel-Extranets oder durch Phishing-E-Mails an Hotelmitarbeitende kompromittiert. Die Täter nutzen die erlangten Informationen, um sich als Unterkunftsanbieter auszugeben und Gäste zur Eingabe sensibler Daten auf gefälschten Webseiten zu bewegen. Besonders perfide ist, dass die Nachrichten oft direkt über legitime Plattformen wie Booking.com oder Expedia versendet werden und echte Buchungsdetails enthalten, was das Erkennen des Betrugs erschwert. Den HmbBfDI erreichen diesbezüglich sowohl Databeach Meldungen der Hamburger Hotels i.S.d. Art. 33 Abs. 1 DSGVO sowie Beschwerden der Betroffenen i.S.d. Art. 77 DSGVO. Plattformbetreiber müssen als Verantwortliche für die Verarbeitung der Kundendaten sicherstellen, dass ihre Systeme vor unbefugtem Zugriff geschützt sind (Art. 32 DSGVO). Die Buchungsplattformen betonen, dass keine Sicherheitslücke in ihrem System vorläge. Somit ist die Identifizierung der Sicherheitslücken und die Frage nach der Sicherstellung der Datensicherheit zentraler Bestandteil der anhaltenden Ermittlungen des HmbBfDI.

Betrugsmaschen im Zusammenhang mit Hotelbuchungen umfassen eine Vielzahl von Methoden, die gezielt darauf abzielen, sensible Daten oder Zahlungen von Gästen zu erlangen. Eine der gängigsten Techniken sind Phishing-Nachrichten, bei denen sich Betrüger als Hotels ausgeben und Gäste kontaktieren, die kürzlich eine Buchung vorgenommen haben. In diesen Nachrichten fordern sie die Verifizierung von Zahlungsdaten über Links, die auf täuschend echt wirkende, aber gefälschte Webseiten führen. Diese Seiten nutzen oft echte Buchungsdetails, um glaubwürdig zu erscheinen und das Vertrauen der Opfer zu gewinnen. Eine weitere Methode besteht in der Manipulation von Hotelkonten. Kriminelle verschaffen sich durch Phishing Zugriff auf die Konten von Unterkunftsanbietern auf Buchungsplattformen. Mit diesen kompromittierten Zugängen kontaktieren sie Gäste direkt über die Plattform und stellen gefälschte Zahlungsanforderungen.

Eine neue Dimension des Betrugs eröffnet der Einsatz generativer KI-Tools. Diese Technologien ermöglichen es den Tätern, täuschend echte E-Mails und Nachrichten zu erstellen, was die Erkennung solcher Betrugsversuche erheblich erschwert. Die Kombination aus technischen Angriffen und psychologischen Manipulationen macht diese Betrugsmaschen besonders effektiv und stellt sowohl Gäste als auch Plattformbetreiber vor große Herausforderungen. Im Rahmen der Ermittlungen hat der HmbBfDI ebenfalls Kontakt mit der niederländischen Aufsichtsbehörde aufgenommen, weil diese zuständig für eine große Buchungsplattform ist. In diesem Zusammenhang wurde uns mitgeteilt, dass im Jahr 2024 ein Anstieg der durchgeführten Betrugsversuche von ca. 900 % verzeichnet werden konnte, was vermutlich auf den gezielten Einsatz von KI Tools bzw. Sprachmodellen zurückzuführen ist.

Für Hotels gilt weiterhin, dass ein bekannt gewordener Betrugsversuch ein meldepflichtiger Vorgang i.S.d. Art. 33 DSGVO darstellt. Hotelgäste hingegen sollten bei zukünftigen Buchungen darauf achten, nach Abschluss ihrer Buchung keine Kreditkarten- oder sons-

tigen Zahlungsinformationen preiszugeben. Sollten Fragen im Zusammenhang mit der Buchung auftreten, sollten diese Fragen am Informationsschalter des Hotels oder telefonisch geklärt werden, da zum jetzigen Zeitpunkt nicht davon ausgegangen werden kann, dass die Angriffe aufhören oder auf eine einzelne Schwachstelle zurückzuführen sind. Weiterhin empfiehlt der HmbBfDI Gästen bei der Buchung „Zahlung in der Unterkunft" auszuwählen, um diesen Problemen vorzubeugen. Hotels werden niemals durch Nachrichten in einer Buchungsplattform zur erneuten Zahlung unter Verwendung eines „Links" auffordern. Auch die Angabe von Bankdaten zur Überweisung sollten in Nachrichten stets ignoriert werden.

Die Ermittlungen in dieser Angelegenheit halten an. Sowohl die Buchungsplattformen als auch die Hotels arbeiten mit den Aufsichtsbehörden zusammen, um potenzielle Schwachstellen zu identifizieren und zu beheben. Es ist jedoch zu erwarten, dass sich die Angriffsmethoden weiterentwickeln und nicht auf einzelne Sicherheitslücken beschränken werden. Der HmbBfDI plant daher, Hamburger Hotelbetreiber kontinuierlich durch Sensibilisierungsmaßnahmen zu unterstützen, um gemeinsam technische und organisatorische Lösungen zu entwickeln welche den Schutz der personenbezogenen Daten der Hotelgäste gewährleisten. Diesbezüglich ist der HmbBfDI eine Kooperation mit der Datenschutzaufsichtsbehörde der Niederlande eingegangen. Diese Zusammenarbeit hat sich als äußerst gewinnbringend erwiesen, da sie den Austausch von wertvollen Erkenntnissen und Best Practices ermöglicht hat, die direkt in die Entwicklung wirksamer Schutzmaßnahmen eingeflossen sind.

14. DSK-Papier zur wissenschaftlichen Forschung

Am 11. September 2024 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein Positionspapier zum Begriff „wissenschaftliche Forschungszwecke" beschlossen. Damit soll Verantwortlichen Hilfestellung gegeben werden bei der Beurteilung, ob eine Datenverarbeitung tatsächlich zu wissenschaftlichen Forschungszwecken erfolgt und insoweit privilegierende Regelungen der Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) oder des Landesrechts zur Anwendung gebracht werden können.

Einzelne Regelungen der DSGVO, des BDSG oder des Landesrechts bevorteilen Datenverarbeitungen zu wissenschaftlichen Forschungszwecken und sehen in diesem Zusammenhang Ausnahmen oder Einschränkungen von grundsätzlichen datenschutzrechtlichen Anforderungen vor. So wird insbesondere der Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 lit. b) DSGVO gelockert. Das heißt, eine Weiterverarbeitung für wissenschaftliche Forschungszwecke gilt unter bestimmten, in Art. 89 DSGVO genannten, Voraussetzungen nicht als unvereinbar mit den ursprünglichen Zwecken der Verarbeitung. Eine Verarbeitung von sensiblen Daten im Sinne von Art. 9 Abs. 1 DSGVO kann gemäß § 27 BDSG zu wissenschaftlichen Forschungszwecken auch ohne Einwilligung der betroffenen Person erfolgen, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung erheblich überwiegen. Schließlich kann die Einstufung einer Datenverarbeitung als eine solche zu wissenschaftlichen Forschungszwecken auch zu einer Beschränkung von Informationspflichten oder von Pflichten der verantwortlichen Stellen im Zusammenhang mit Betroffenenrechten, z.B. dem Auskunfts- oder dem Widerspruchsrecht, führen.

Solche Ausnahmen und Einschränkungen des Grundrechts auf Datenschutz nach Art. 8 Grundrechtecharta (GRCh) zugunsten der Forschungsfreiheit nach Art. 13 GRCh sind – unter Wahrung des Verhältnismäßigkeitsgrundsatzes – nur dann gerechtfertigt, wenn sie den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen entsprechen oder dem Schutz der Rechte und Freiheiten anderer dienen. Mit Blick darauf geht die DSK von den folgenden fünf Kriterien aus, die erfüllt sein müssen, um die zuvor beschriebene Privilegierung zu rechtfertigen: methodisches und systematisches Vorgehen, Erkenntnisgewinn, Nachprüfbarkeit, Unabhängigkeit und Selbständigkeit sowie Gemeinwohlinteresse.

Dabei ist zu berücksichtigen, dass Erwägungsgrund 159 DSGVO eine weite Auslegung der Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken vorsieht, so dass auch die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung dazu zählen kann (vgl. Positionspapier unter https://datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf).

Dem Positionspapier kommt im Zusammenhang mit neuen gesetzlichen Regelungen wie dem Gesundheitsdatennutzungsgesetz, das die Nutzbarmachung von Versorgungsdaten u.a. zu Forschungszwecken zum Gegenstand hat (vgl. 33. TB, Kapitel III 9), eine besondere Bedeutung zu.

15. Nationaler und internationaler Austausch zu technischen Prüfungen

Ein wichtiger Aufgabenbereich des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ist die technische Prüfung von Webanwendungen und Smartphone-Applikationen im Bereich Cookies und Tracking. Zu diesem Bereich erhielt er auch im laufenden Berichtsjahr zahlreiche Beschwerden und Beratungsanfragen.

Aufgrund der Komplexität und Dynamik der zu prüfenden Technik ist hierbei die Zusammenarbeit mit anderen Aufsichtsbehörden und Institutionen von besonderer Bedeutung, um die erforderlichen Kompetenzen zu erwerben und zu erweitern. An diesem Austausch beteiligt sich der HmbBfDI auf verschiedenen Ebenen:

1. Der HmbBfDI nimmt regelmäßig an Workshops teil, die vom europäischen Datenschutzausschuss (EDSA) organisiert werden. Zuletzt wurden im September 2024 wissenschaftliche Ausarbeitungen zu den Themen Dark Patterns in Cookiebannern und Trackinganalysen von Android-APIs vorgestellt, die einen tiefen Einblick in komplexe technische Sachverhalte vermitteln. Die HandsOn-Session mit der Projektverantwortlichen der PiRogue Tool Suite (https://www.pts-project.org) gab die Gelegenheit, speziell für Smartphoneaudits entwickelte Prüfmethoden und Analysewerkzeuge zu erproben.

2. Auf nationaler Ebene arbeitet der HmbBfDI mit anderen Landesdatenschutzbehörden sowie der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) in Form von Workshops zusammen. Schwerpunkte im Jahr 2024 waren technische Prüfverfahren von IoT-Geräten, Webseiten und Smartphoneapplikationen. Zudem fand im Oktober 2024 ein intensiver Austausch zu Prüflaboren statt, der für den geplan-

ten Betrieb eines solchen Labors beim HmbBfDI wichtige Erkenntnisse und Erfahrungswerte lieferte.

3. Eine besonders enge Kooperation besteht mit dem Landesbeauftragten für den Datenschutz Niedersachsen. Seit dem Jahr 2023 fanden mehrere Treffen auf Arbeitsebene statt. Neben dem allgemeinen Erfahrungsaustausch spielte dabei der kritische Vergleich von Prüfungs- und Auswertungsmethodiken eine wichtige Rolle. Im Idealfall sollte die technische Prüfung einer bestimmten Website zum gleichen Befund bei Cookies und Trackern kommen. Im direkten Vergleich der Prüftechniken und -ergebnisse konnte festgestellt werden, dass hier weiterer Anpassungsbedarf besteht.

4. Im Juli 2024 lud der HmbBfDI Vertreter:innen der IT-forensischen Abteilungen des Landeskriminalamts und des Zollfahndungsamts Hamburgs zu einem Austauschtreffen ein. Auch hier waren technische Prüf- und Datensicherungsverfahren und der Austausch von Informationen zu verfügbaren Softwarewerkzeugen das zentrale Thema. Alle Beteiligten bewerteten dieses Treffen als eine große Bereicherung für ihre tägliche Arbeit.

Die Zusammenarbeit des HmbBfDI mit anderen Aufsichtsbehörden und Institutionen ist ein entscheidender Faktor, um den stets wachsenden Anforderungen an technische Prüfungen im Bereich von Apps und des Web gerecht zu werden. Die gemeinsame, thematisch intensive Auseinandersetzung hilft dem HmbBfDI dabei, die Datenschutzanforderungen in Webanwendungen und Smartphone-Applikationen effektiv und mit der für Verwaltungsverfahren erforderlichen Qualität zu überprüfen.

16. Verfahrensabschluss Bundeskartellamt gegen Meta

Der Abschluss des Verfahrens des Bundeskartellamts gegen Meta blickt auf eine lange, gelungene Zusammenarbeit zwischen zwei sektoralen Aufsichtsbehörden zurück, deren Aufgaben enge Bezüge aufweisen. Der HmbBfDI hatte gemeinsam mit dem BfDI das Bundeskartellamtsverfahren jahrelang unterstützend und aus Datenschutzsicht beratend begleitet.

Während das Datenschutzrecht den Schutz der persönlichen Daten der Betroffenen im Fokus hat, schützt das Kartellrecht den Wettbewerb und die Marktintegrität. So ist es auch nicht verwunderlich, dass das Recht auf informationelle Selbstbestimmung in der Vergangenheit eher wenige Überschneidungspunkte mit der Marktregulierung bot. Das änderte sich jedoch mit dem rasanten Aufstieg der Online-Plattformen, deren Marktmacht sich vor allem aus der Menge der gesammelten, in der Regel personenbezogenen Daten und ihrer Verknüpfung speist.

Im Februar 2019 hatte das Bundeskartellamt Meta (vormals Facebook) in seinem Beschluss B6-22-16 untersagt, personenbezogene Daten der Nutzenden ohne Einwilligung aus verschiedenen Quellen zusammenzuführen. Ohne eine entsprechende datenschutzrechtliche Einwilligung sah das Bundeskartellamt einen Missbrauch der Marktmacht durch Meta, der die Annahme eines Monopolisierungsprozesses nahelegte. Gegen den Beschluss hatte Meta Beschwerde eingelegt. Nach einer jahrelangen gerichtlichen Auseinandersetzung und der Bestätigung des Bundeskartellamtes in Grundsatzfragen durch den Bundesgerichtshof (2020) sowie den Europäischen Gerichtshof (2023, C-252/21) haben sich Meta und das Bundeskartellamt auf konkrete Maßnahmen zur Umsetzung der Entscheidung geeinigt, die dann zur Rücknahme der Beschwerde durch Meta und damit zum Ende des Verfahrens führten.

Aufgrund seiner innerdeutschen Zuständigkeit für Facebook nach § 19 Abs. 2 Bundesdatenschutzgesetz begleitete der HmbBfDI diesen Prozess seit seiner Eröffnung 2016, auch wenn die europäische Federführung seit der Geltung der DSGVO ab Mai 2018 bei der irischen Aufsichtsbehörde liegt. Die Regelung des § 50 f des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) ermöglicht unabhängig von der jeweils gewählten Verfahrensart einen Informationsaustausch u.a. zwischen dem Bundeskartellamt und den deutschen Datenschutzaufsichtsbehörden. Diese Regelung schließt den Austausch und die Verwertung von personenbezogenen Daten sowie Betriebs- und Geschäftsgeheimnissen mit ein, soweit dies zur Erfüllung der jeweiligen Aufgaben erforderlich ist. Hiervon wurde in dem genannten Verfahren intensiv Gebrauch gemacht und dadurch erreicht, dass die datenschutzrechtlichen Wertungen durch die jeweilige sektorale Aufsicht nicht auseinanderfielen.

Der EuGH führte in seiner Entscheidung C-252/21 aus, dass Datenschutzaufsichts- und Kartellbehörden an den Grundsatz der loyalen Zusammenarbeit gebunden sind, der sich unter anderem aus Art. 4 Abs. 3 EUV herleitet. Dadurch soll sichergestellt werden, dass keine voneinander abweichenden Auslegungen der DSGVO durch die unterschiedlichen sektoralen Behörden erfolgen. Die nationalen Wettbewerbsbehörden sind nach dem Urteil des EuGH verpflichtet, loyal mit den betreffenden nationalen Aufsichtsbehörden beziehungsweise der federführenden Aufsichtsbehörde zusammenzuarbeiten und sich mit diesen abzustimmen. Dazu haben sie zunächst zu prüfen, ob es bereits einschlägige Entscheidungen durch die zuständige nationale Aufsichtsbehörde oder die federführende Aufsichtsbehörde oder auch durch den Gerichtshof gibt.

Eine zusätzliche Komplexität bildete die Herausforderung, die aktuellen Entwicklungen auf europäischer Ebene sowie die Aufsichtspraxis anderer europäischer Aufsichtsbehörden und Gremien wie dem EDSA in Einklang zu bringen. Denn während des Verfahrens des BKartA hatte auch der EDSA verbindliche Beschlüsse nach Art. 65 DSGVO betreffend Meta erlassen, insbesondere die Beschlüsse

2/2022 und 3/2022, welche eine vertragliche Rechtsgrundlage oder auch berechtigte Interessen für personalisierte Werbung ausschlossen.

Der Grundsatz der loyalen Zusammenarbeit wird künftig eine zentrale Rolle bei der Umsetzung der neuen Regulierungen des Digitale-Dienste-Pakets der EU spielen, so auch beim Gesetz über digitale Märkte (Digital Markets Act, kurz DMA). Das Bundeskartellamt und der HmbBfDI sind jeweils als Vertreter ihrer Gremien gem. Art. 40 DMA in der Hochrangigen Gruppe (High Level Group DMA) aktiv, in der unter anderem auch die Ausgestaltung der Zusammenarbeit zwischen den sektoralen Aufsichtsbehörden diskutiert wird.

KI UND DATENSCHUTZ IV.

KI UND DATENSCHUTZ

1. KI und Datenschutz – Chancen, Herausforderungen und neue Perspektiven

Das Jahr 2024 kann zweifellos als ein weiteres „KI-Jahr" bezeichnet werden, geprägt von rasanten Entwicklungen und einer wachsenden Vielfalt an Einsatzmöglichkeiten von Künstlicher Intelligenz (KI). Mehr denn je rückte KI in den Fokus öffentlicher und politischer Debatten, und auch der HmbBfDI war in diesem Jahr mit einer nie dagewesenen Fülle an KI-bezogenen Themen und Fragestellungen konfrontiert.

Erstmals widmet sich deshalb ein eigenes Kapitel des Tätigkeitsberichts dem Thema „KI und Datenschutz". Die Beiträge in diesem Kapitel geben Einblick in einige der wichtigen Verfahren, in denen sich der HmbBfDI intensiv mit dem Einsatz Künstlicher Intelligenz auseinandergesetzt hat.

Hervorzuheben ist aber zunächst das Diskussionspapier „Large Language Models und personenbezogene Daten" des HmbBfDI, das eine weltweit geführte Debatte in Fachkreisen auslöste und damit sein Ziel – eine fundierte und offene Auseinandersetzung mit den technologischen Gegebenheiten der großen KI-Modelle und deren juristischen Implikationen – schnell erreichte.

Ebenfalls im Berichtsjahr veröffentlichte der HmbBfDI das Positionspapier „Recruiting und Bewerbermanagement", welches die Auswirkungen von KI auf Bewerbungsverfahren beleuchtete.

Von besonderer Bedeutung sind die zahlreichen KI-Projekte im öffentlichen Bereich. So wie Hamburg generell bei der Digitalisierung des öffentlichen Sektors im bundesweiten Vergleich eine Führungsrolle einnimmt, so ist auch die Entwicklung von KI-Systemen und deren konkreter Einsatz weit fortgeschritten. Die frühzeitige und intensive Einbindung des HmbBfDI ist hier sehr zu begrüßen und auch bundesweit vorbildlich. Dies trug nicht nur zu einer deutlich verbes-

serten Rechtslage für das Training und den Einsatz von KI-Modellen bei, sondern – bei noch zu klärenden Divergenzen – auch zu grundrechtsschonenden Anwendungsmodalitäten.

Die folgenden Beiträge zeigen insofern auf, wie der HmbBfDI dazu beiträgt, KI-Entwicklungen mit den Grundrechten in Einklang zu bringen und damit eine datenschutzkonforme digitale Zukunft zu gestalten.

2. Diskussionspapier LLMs und personenbezogene Daten

Am 15.07.2024 veröffentlichte der HmbBfDI das Diskussionspapier „LLMs und personenbezogene Daten". Die darin vertretene These, Large Language Models (LLMs) enthielten keine personenbezogenen Daten, stieß eine wichtige Debatte an. Diese erreichte mit einer Stellungnahme des Europäischen Datenschutzausschusses (EDSA) vom 17.12.2024 einen vorläufigen Abschluss.

Die mittlerweile als „Hamburger Thesen" bekannten Annahmen lauten:

1. Die bloße Speicherung eines LLMs stellt keine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar. Denn in LLMs werden keine personenbezogenen Daten gespeichert. Soweit in einem LLM-gestützten KI-System personenbezogene Daten verarbeitet werden, müssen die Verarbeitungsvorgänge den Anforderungen der DSGVO entsprechen. Dies gilt insbesondere für den Output eines solchen KI-Systems.
2. Mangels Speicherung personenbezogener Daten im LLM können die Betroffenenrechte der DSGVO nicht das Modell selbst zum Gegenstand haben. Ansprüche auf Auskunft, Löschung oder Berichtigung können sich jedoch zumindest auf Input und Output eines KI-Systems beziehen.
3. Das Training von LLMs mit personenbezogenen Daten muss

datenschutzkonform erfolgen. Dabei sind auch die Betroffenenrechte zu beachten. Ein ggf. datenschutzwidriges Training wirkt sich aber nicht auf die Rechtmäßigkeit des Einsatzes eines solchen Modells in einem KI-System aus.

Zum Verständnis der Thesen muss zwischen KI-Systemen und den darin eingebundenen LLMs unterschieden werden. Diese Differenzierung ist entscheidend, um die rechtlichen Anforderungen an verschiedene Bestandteile eines KI-Systems präzise bewerten zu können.

Ein KI-System (z. B. „Frag die DSK" oder „ChatGPT") setzt sich aus verschiedenen Elementen zusammen, von denen das LLM lediglich eine Komponente darstellt. Weitere Bestandteile eines solchen Systems sind etwa die Benutzeroberfläche, Ein- und Ausgangsfilter sowie potenziell Prozesse zur Datenanreicherung, wie etwa durch Datenbankabfragen, Internetsuchen oder Retrieval Augmented Generation (RAG).

Vor dem ersten Training eines LLMs ist es „neutral" und enthält keinerlei Informationen. Während des Trainingsprozesses werden Trainingstexte, häufig solche aus dem frei verfügbaren Internet, in numerische Tokens umgewandelt. Das Modell lernt durch das Training, die Beziehungen zwischen diesen Tokens zu erfassen und die Wahrscheinlichkeiten für bestimmte Sequenzen einzuschätzen. Diese Verknüpfungen, sogenannte Embeddings, bilden die Grundlage für die Fähigkeit des LLMs, zusammenhängende und sinnvolle Texte zu generieren.

Es ist wichtig zu verstehen, dass nicht die Trainingstexte als solche im LLM „gespeichert" werden, sondern nur die beim Training extrahierten allgemeinen Muster und Zusammenhänge innerhalb der Trainingsdaten. Die Ausgaben eines LLMs stellen daher keine Wiedergabe gespeicherter Daten dar. Im Gegensatz zu personenbezogenen Kennungen, wie sie der EuGH etwa bei IP-Adressen anerkennt, dienen die gespeicherten Tokens und Embeddings nicht der gezielten Identifikation einzelner Personen. Es fehlt insoweit an einem von der Rechtsprechung geforderten „Identifier".

Obgleich eine Extraktion von Fragmenten der Trainingsdaten in Einzelfällen nachgewiesen wurde, führe auch dies nicht dazu, dass das Modell selbst personenbezogene Daten speichert. Denn nach der Rechtsprechung des EuGH können Daten nur dann als personenbezogen eingestuft werden, wenn die Identifizierung mit Mitteln des Verantwortlichen oder Dritter keinem gesetzlichen Verbot unterliegt bzw. nicht bloß mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften möglich ist. Dies ist bei LLMs derzeit aber der Fall.

Das Diskussionspapier stieß sowohl in Fachkreisen als auch in der breiteren Öffentlichkeit auf weltweite Resonanz. Neben wissenschaftlichen Zeitschriften berichteten auch Tagesmedien über die kontrovers diskutierten „Hamburger Thesen". Im Rahmen eines von der irischen Datenschutzaufsichtsbehörde angestoßenen Verfahrens gemäß Art. 64 Abs. 2 DSGVO nahm die Debatte zuletzt weiter Fahrt auf. Der EDSA musste bis zum 23.12.2024 darüber befinden, ob KI-Modelle – mithin der Oberbegriff von LLMs – personenbezogene Daten enthalten können. Am 17.12.2024 veröffentlichte er fristgerecht seine Stellungnahme, welche im Abschnitt IV 3 besprochen wird.

3. Stellungnahme des EDSA zur KI-bezogenen Verarbeitung personenbezogener Daten

Ende 2024 hat der Europäische Datenschutzausschuss (EDSA) eine Stellungnahme zur Verarbeitung personenbezogener Daten bei KI-Modellen und -Systemen verfasst. Damit liegt eine erste europäische Positionierung zur Künstlichen Intelligenz vor.

Eine europäische Datenschutzbehörde kann den EDSA gemäß Art. 64 Abs. 2 DSGVO jederzeit um eine Stellungnahme ersuchen in Bezug auf eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat. Von dieser Möglichkeit hat die irische Aufsichtsbehörde IDPC Gebrauch gemacht und hat

dem Ausschuss eine Reihe von Fragen vorgelegt, die von zentraler Bedeutung für Modelle und Anwendungen der Künstlichen Intelligenz sind. Die Stellungnahme dazu wurde vom EDSA am 17.12.2024 beschlossen (https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf). Vorausgegangen waren viele Abstimmungsrunden in verschiedenen Arbeitsgremien des EDSA. Deren deutsche Vertreter wurden von mehreren deutschen Aufsichtsbehörden, darunter auch dem HmbBfDI intensiv unterstützt.

Ohne konkret Gegenstand der Befassung durch den EDSA zu sein, bildeten Planungen von Anbietern großer sozialer Netzwerke, nutzergenerierte Inhalte zum KI-Training zu verwenden (siehe Kapitel IV 10) den Hintergrund des Verfahrens nach Art. 64 DSGVO. Im Einzelnen umfassten die Fragen der IDPC folgende Aspekte:

- Fallen KI-Modelle, die mit personenbezogenen Daten trainiert wurden, selbst unter die DSGVO?
- Unter welchen Umständen können das Training und die Nutzung von KI-Modellen unter Verwendung personenbezogener Daten auf ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO) gestützt werden?
- Wie wirken sich datenschutzrechtliche Mängel bei der Erstellung eines KI-Modells auf die Zulässigkeit seiner späteren Nutzung aus?

Vor dem Hintergrund der komplexen Materie, die durch die Fragen angesprochen wird, ist es nicht verwunderlich, dass die Stellungnahme einen nennenswerten Umfang hat. Ein Stakeholder-Event mit Unternehmen und Verbänden war Teil des Prozesses und konnte im Ergebnis zu zusätzlichen Aspekten beitragen. Gleichwohl, und auch das ist wenig überraschend, bleiben in der Breite und Tiefe des Verhältnisses der DSGVO zu dem sehr dynamischen Feld der Künstlichen Intelligenz weiterhin viele Fragen offen.

Aus den Antworten in der Stellungnahme lässt sich folgendes Bild zusammenfassen:

1.) Ob ein KI-Modell anonym oder personenbezogen ist und damit die DSGVO zur Anwendung kommt, ist in jedem Einzelfall zu bewerten. Der EDSA verweist auf bestimmte Konstellationen, bei denen stets ein Personenbezug vorliegt. Dies sind solche KI-Modelle, die Eigenschaften einzelner Personen erlernen, etwa deren Stimme oder Gewohnheiten. Dort wo Daten mehrerer oder wie bei LLM unüberschaubar vieler Individuen in ein Modell einfließen, hebt der EDSA auf die Risiken ab, Informationen über Betroffene aus dem Modell extrahieren zu können. Dabei werden die Mittel, die nach vernünftigem Ermessen von dem Verantwortlichen oder einer anderen Person eingesetzt werden, zugrunde gelegt. Von Anonymität ist dann auszugehen, wenn solche Mittel mit lediglich vernachlässigbarer Wahrscheinlichkeit zum Erfolg führen. Dazu stellt der EDSA Prüfkriterien auf, die Design, Auswahl und Aufbereitung von Trainingsdaten, Trainingsmethoden und auch Maßnahmen in Bezug auf die Ausgabe eines KI-Modells betreffen. Um diese anzuwenden, soll auf Analysen und Audits, auf praktische Tests und Angriffsresistenz der Modelle sowie auf die Dokumentation der Modellersteller zurückgegriffen werden. Der EDSA legt damit ein anspruchsvolles und bislang in der Praxis regelhaft nicht erreichtes Prüfniveau für KI-Modelle fest.

2.) Bei der Bewertung des berechtigten Interesses als Rechtsgrundlage beim Training oder der Nutzung von KI-Modellen folgt der EDSA den bekannten Auslegungsprinzipien des Art. 6 Abs. 1 lit f DSGVO (https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf). Dabei kann bereits die Prüfung der Erforderlichkeit zu einem negativen Ergebnis führen, wenn KI-Modelle mit unnötig vielen personenbezogenen Daten trainiert werden und der Verzicht auf Teile der Trainingsdaten zu einem vergleichbaren Ergebnis führt. Dies ist vor dem Hintergrund des „Datenhungers“ von generativen Modellen ein durchaus praxisrelevanter Punkt. Hinsichtlich der Abwägung zwischen den berechtigten Interessen der Verantwortlichen und den Grundrechten und Grundfreiheiten der Betroffenen, die immer Gegenstand der Prüfung der Zulässigkeit des Art. 6 Abs. 1 lit f DSGVO ist, ver-

weist der EDSA auf eine Reihe von zu berücksichtigenden Faktoren. Dazu gehören die Risiken, die durch KI-Systeme für Betroffene ausgehen, die Art und Sensibilität der Daten, die Schutzwürdigkeit der Betroffenen (z.B. ob Kinder betroffen sind), Umfang und Qualität von Schutzmaßnahmen durch den Verantwortlichen und vieles mehr. All diese Faktoren werden in der Praxis des Einzelfalls nur durch ausführliche und gut dokumentierte Interessensabwägungen ausreichend berücksichtigt und in ein nachvollziehbares Verhältnis gesetzt werden können.

3.) Zu den Auswirkungen datenschutzrechtlicher Mängel bei der Modellerstellung auf die Zulässigkeit bei der Modellnutzung (sog. Infektionsthese) gibt der EDSA differenzierte Antworten. Dabei spielen die Szenarien, die in den Ausgangsfragen enthalten sind, ebenso eine Rolle wie die Frage, ob es sich beim Modellersteller und späteren Anwender des Modells um denselben oder einen anderen Verantwortlichen handelt. Für den praxisrelevanten Fall der Übereinstimmung von Ersteller und Anwender eines KI-Modells und zudem bestehender Zweckübereinstimmung in den Phasen des Trainings und der Nutzung gibt der EDSA für die fallweise erforderliche Bewertung grobe Anhaltspunkte. Die abschließende Bewertung bleibt den jeweils zuständigen Aufsichtsbehörden überlassen.

Auch wenn sich der HmbBfDI im Rahmen des deutschen und europäischen Abstimmungsprozesses zu dieser Stellungnahme mit seinen Vorschlägen nicht immer durchsetzen konnte, ist im Ergebnis eine stellenweise hilfreiche, wenn auch aus Sicht sowohl der Aufsichtsbehörden wie der Verantwortlichen durchaus herausfordernde Positionierung entstanden. Die Stellungnahme des EDSA zielt dabei offensichtlich auf spezialisierte KI-Systeme, die mit einem einzigen KI-Modell arbeiten, dessen Entstehung im Training und anschließende Funktion im System weitgehend überprüfbar ist. Für diesen use-case und darüber hinaus für die Konzeption zukünftiger KI-Systeme kann sie eine hilfreiche Richtschnur bieten. Für die Bewertung der gegenwärtigen LLMs und von komplexeren KI-Syste-

men mit mehreren interagierenden Modellen werden teilweise mehr Fragen aufgeworfen als beantwortet. Die Tauglichkeit in der Praxis der Aufsichts- und Beratungstätigkeit des HmbBfDI wird sich erweisen müssen.

4. Verwaltungsdigitalisierungsgesetz – Hamburgs Rechtsgrundlage für KI-Training

Das Hamburgische Recht enthält seit November 2024 eine KI-Klausel. Damit sind der Einsatz und das Training künstlicher Intelligenz durch öffentliche Stellen auf Basis einer gesetzlichen Grundlage geregelt. Der entsprechende Passus des neuen Hamburgischen Verwaltungsdigitalisierungsgesetzes bleibt mit seiner relativ pauschalen Erlaubnis jedoch hinter den Möglichkeiten innovativer und rechtssicherer Gesetzgebung zurück.

Der Einsatz und die Entwicklung von KI mit personenbezogenen Daten erfordern eine tragfähige rechtliche Grundlage. Im nichtöffentlichen Bereich kann hierfür je nach Fallgestaltung die Abwägungsklausel des Art. 6 Abs. 1 lit. f) DSGVO herangezogen werden (EDSA, Opinion 28/2024, Ziff. 3.3). Für nichtöffentliche Verantwortliche ist diese Rechtsgrundlage explizit gesperrt. Sie benötigen daher eine andere rechtliche Basis, die ggf. auch durch die mitgliedstaatlichen Gesetzgeber geschaffen werden kann. Ein Rückgriff auf die allgemeine datenschutzrechtliche Generalklausel der Verwaltung in § 4 HmbDSG ist dabei problematisch. Die sehr begriffsoffene Klausel erlaubt ihrem Wortlaut nach alle Datenverarbeitungen, die zur Aufgabenerfüllung der jeweiligen Behörde erforderlich sind. Sie kann jedoch nur für vergleichsweise wenig eingriffsintensive Verarbeitungsvorgänge genutzt werden. Nach der datenschutzrechtlichen Wesentlichkeitslehre ist anerkannt, dass einschneidendere bzw. risikoreichere Verarbeitungen nur auf Basis einer bereichsspezifischen Rechtsgrundlage zulässig sind. Diese hat den genauen Kontext zu beschreiben und einzugrenzen sowie

auf das Einsatzszenario bezogene konkrete Garantien für die Rechte der Betroffenen vorzusehen.

Vor diesem Hintergrund ist es lobenswert, dass der Hamburgische Gesetzgeber eine Rechtsgrundlage für die Entwicklung und den Einsatz von KI-Systemen geschaffen hat. Hamburg nimmt damit eine legislative Vorreiterrolle an, während zahlreiche andere Bundesländer ihre KI-Projekte relativ unsicher auf die dort geltende datenschutzrechtliche Generalklausel stützen müssen. § 13 des Hamburgischen Digitalisierungsgesetzes vom 19.11.2024 (HmbVwDiG) gestattet in Abs. 1 den Einsatz von Systemen Künstlicher Intelligenz zur Wahrnehmung öffentlich-rechtlicher Verwaltungstätigkeit. Abs. 2 regelt das Training von KI-Systemen durch öffentliche Stellen. Abs. 3 ermöglicht die zweckändernde Verwendung von Daten für das Training, die ursprünglich zu einem anderen Zweck erhoben wurden. Der Absatz greift damit die formalen Anforderungen des Art. 6 Abs. 3 lit. b) DSGVO auf. Abs. 4 enthält eine Verordnungsermächtigung, um die Regelungen des § 13 HmbVwDiG zu konkretisieren.

Während der Umstand, dass Hamburg eine solche KI-Klausel geschaffen hat, sehr erfreulich ist, bleibt die konkrete Ausführung hinter dem wünschenswerten und gebotenen Regelungsgehalt zurück. So werden für den Einsatz von KI-Systemen in Abs. 1 keine inhaltlichen Schranken festgelegt, die über eine Zweckbestimmung zur Wahrnehmung der öffentlich-rechtlichen Verwaltungstätigkeit und einen Verweis auf die nicht näher benannten „maßgeblichen Rechtsvorschriften“ hinausgehen. Damit erlaubt der Gesetzgeber die Verwendung von KI-Systemen pauschal, ohne deren Grenzen abzustecken. Gebotene technische bzw. organisatorische Schutzmaßnahmen beschränken sich im Gesetzestext auf ein spezifisches Dokumentationserfordernis. Die Anforderungen an das Training von KI-Systemen sind ein wenig differenzierter, bleiben aber gleichwohl relativ pauschal. Abs. 2 sieht dafür einen Dreischritt vor, nachdem die Verwendung anonymisierter Daten vorzuziehen ist. Kann der Zweck des Trainings mit anonymisierten Daten nicht erreicht werden oder wäre der Anonymisierungsaufwand „nur mit unverhältnismä-

ßigem Aufwand möglich“, sind pseudonyme Daten für das Training zu verwenden. Kann der Zweck des Trainings mit pseudonymisierten Daten ebenfalls nicht erreicht werden oder wird der Pseudonymisierungsaufwand als unverhältnismäßig eingestuft, erlaubt Abs. 2 schließlich die Verwendung personenbezogener Klardaten für das Training, ohne eine weitere Einschränkung vorzunehmen.

Der HmbBfDI wurde frühzeitig und umfassend in die Erstellung des § 13 HmbVwDiG einbezogen. Neben den beiden förmlichen Drucksachenabstimmungen fand ein vorheriger informeller Austausch statt. Infolge dieses Dialogs wurden in den zuvor noch pauschaleren Entwurf einige Differenzierungen aufgenommen. Zudem sind infolge der Konsultation des HmbBfDI unklare Begriffe in der Gesetzesbegründung erläutert worden. Dies betrifft u.a. die Anforderungen an eine Anonymisierung, den Begriff des unverhältnismäßigen Aufwands und an den Umstand, dass der Trainingszweck nicht erreicht werden kann. Hier wäre eine Begriffsbestimmung im Gesetzestext vorzugswürdig gewesen.

Besonders fällt auf, dass die Vorschrift keine Angaben dazu macht, welche Kategorien von Daten zu welchen konkreten Zwecken und mit welchen Anforderungen für das KI-Training verwendet werden dürfen. Dies steht im Spannungsverhältnis zu Art. 6 Abs. 3 DSGVO. Die unionsrechtliche Vorgabe macht deutlich, dass eine Abwägungsentscheidung zu treffen ist und nur eine Norm als Rechtsgrundlage i. S. d. Art. 6 Abs. 1 lit. e) DSGVO dienen kann, die „in einem angemessenen Verhältnis“ zu dem verfolgten Zweck steht. Diese gesetzgeberische Abwägungsentscheidung kann dem Text des § 13 HmbVwDiG nicht entnommen werden. Auch fehlt es an der gebotenen Festlegung technisch-organisatorischer Maßnahmen, die den Schutz betroffener Personen garantieren würden. Eine Rechtsgrundlage, die KI-Nutzung und -Training ermöglicht, müsste erkennen lassen, dass sie den Vorgaben des Art. 6 Abs. 1 lit. e) i.V.m. Abs. 3 DSGVO genügt. Dafür sind konkretere Vorgaben zu machen, unter welchen Voraussetzungen und flankiert durch welche Schutzmaßnahmen und Garantien für die Betroffenen die Verwendung personenbezogener

Daten für das KI-Training zulässig ist. Bei der Ausgestaltung dieser Vorgaben hat der Gesetzgeber einen weiten Spielraum. Er hat in der Summe einen Zustand vorzugeben, der ein angemessenes Verhältnis zwischen dem verfolgten Zweck und den Rechten der Betroffenen herstellt. Der HmbBfDI hatte im Rahmen des Gesetzgebungsverfahren zahlreiche Vorschläge unterbreitet, die z.B. eine Eingrenzung der Verarbeitungszwecke, eine Festlegung der Speicherfristen, eine Etablierung von Garantien gegen unrechtmäßigen Zugang und unrechtmäßige Übermittlung, umfassende Dokumentationen, Transparenz gegenüber Betroffenen und den Umgang mit geltend gemachten Betroffenenrechten beinhalten.

Die relativ pauschale Erlaubnisnorm des § 13 HmbVwDiG wird sich nun bei der Umsetzung zahlreicher Pilotprojekte in der Stadt Hamburg beweisen müssen. Dabei ist trotz der nur marginalen Andeutung im Normtext auf ein angemessenes Schutzniveau der betroffenen Personen zu achten. Über den Verweis in Abs. 1 auf den KI-Einsatz „unter Beachtung der maßgeblichen Rechtsvorschriften“ sind die Anforderungen des Datenschutzrechts vollumfänglich einzubeziehen. Der HmbBfDI wird die Senatsbehörden bei der Gestaltung datenschutzkonformer KI-Systeme auf dieser Basis unterstützen.

5. Zuständigkeit aus der KI-Verordnung

Die KI-Verordnung (KI-VO) ist im August 2024 in Kraft getreten. Bis Sommer 2025 müssen die umsetzenden Marktüberwachungsbehörden benannt werden. Während der Bund die Bundesnetzagentur als einzige zentrale Stelle favorisiert, sieht die KI-VO für bestimmte Hochrisiko-Sektoren die Datenschutzbehörden vor. Im öffentlichen Sektor liegt eine Zuständigkeit der Länder nahe – der HmbBfDI bereitet sich entsprechend vor und steht für diese neue Aufgabe bereit.

Während der Bund die Bundesnetzagentur als zentrale Digitalagentur ins Spiel bringt, die neben dem Digital Services Act und dem

Data Governance Act dann auch die KI-VO als Marktüberwachungsbehörde umsetzen würde, sprechen viele Aspekte für eine jedenfalls teilweise Zuständigkeit der Länder. Insbesondere die Hochrisikosektoren im öffentlichen Bereich berühren häufig die Eigenstaatlichkeit der Länder, etwa bei Bildung und Polizei, weshalb deren Beteiligung unausweichlich ist. Eine zentrale Rolle bei der Marktüberwachung auf Landesebene werden die Datenschutzaufsichtsbehörden in jedem Fall spielen. Die KI-VO weist ihnen in Art. 74 Abs. 8 KI-VO die Überwachungskompetenz für wesentliche Bereiche des Hochrisiko-Katalogs zu, etwa in den Sektoren Strafverfolgung, Justizverwaltung und Migrationskontrolle sowie bei KI-Systemen mit potenziellem Einfluss auf Wahlen.

Die Mitgliedstaaten haben bis zum 2. August 2025 Zeit, ein entsprechendes Durchführungsgesetz zu erlassen. Dieses muss sicherstellen, dass die Marktüberwachungsbehörden unabhängig sind und mit ausreichenden Mitteln befähigt werden, effektiv zu regulieren. Sowohl die Datenschutzkonferenz als auch der Europäische Datenschutzausschuss haben die Bereitschaft der Datenschutzbehörden bekräftigt, diese zentrale Rolle zu übernehmen. In anderen Mitgliedstaaten wie den Niederlanden und Luxemburg sind die Planungen bereits abgeschlossen – die Datenschutzbehörden werden dort wesentliche Aufgaben der Marktüberwachung wahrnehmen.

Der HmbBfDI entwickelt derzeit die konkreten Umsetzungsschritte, um diese wichtige Zukunftsaufgabe mit der erforderlichen personellen und technischen Ausstattung wahrnehmen zu können.

6. LLMoin – ein KI-Chatbot für die öffentliche Verwaltung

Der im Jahr 2023 auf den Weg gebrachte KI-Textassistent „LLMoin" wurde im Berichtsjahr in Bezug auf die Nutzungsmöglichkeiten erweitert, so dass nun im Rahmen der Ein- und Ausgabe auch personenbezogene Daten verarbeitet werden können. In Bezug auf die Verarbeitung von Daten mit einem normalen Schutzbedarf kann dies unter bestimmten Voraussetzungen datenschutzrechtlich zulässig sein. Bei vielen noch offenen Detailfragen ist insgesamt positiv zu bewerten, dass der Senat den HmbBfDI bei der Implementierung dieses KI-Systems vollumfänglich einbindet.

Bereits im Jahre 2023 wurde der HmbBfDI von der Senatskanzlei der FHH bei der Einführung eines KI-Systems beteiligt, die der Arbeitserleichterung in der öffentlichen Verwaltung dienen sollte. Das KI-System LLMoin wurde den Fachbehörden in der FHH im Jahr 2023 im Rahmen eines Piloten unter der Maßgabe zur Verfügung gestellt, dass weder bei der Ein- noch bei der Ausgabe personenbezogene Daten verarbeitet werden dürfen.

Nach einer Evaluation dieses Piloten wurde der KI-Chatbot im Berichtsjahr in Bezug auf das genutzte Sprachmodell und in Bezug auf den Nutzungsumfang angepasst. Es wird nun auf das Sprachmodell GPT-4o gesetzt, das in der Cloud-Infrastruktur von Microsoft in Europa betrieben wird. Während es bei den Nutzungsszenarien bei den Funktionen „Textzusammenfassung", „Recherche-Assistent", „Textgenerierung" und „offenes Prompting" bleibt, wird erweiternd zukünftig die Verarbeitung von personenbezogenen Daten erlaubt sein. Weiterhin bleibt LLMoin auf den Einsatz von Datenverarbeitung mit „normalen" Schutzbedarf beschränkt, was derzeit durch entsprechende Handlungsanweisungen sichergestellt werden soll.

Dem HmbBfDI wurden zu dem Projekt in seiner jetzt erweiterten Funktion zunächst verschiedene Unterlagen zur Prüfung vorgelegt. Es wurden insbesondere das Löschkonzept, die Beschreibung der Verarbeitungstätigkeit und Datenschutzhinweise vorgelegt. Bei der Bewertung durch den HmbBfDI zeigte sich dann, dass die Schwerpunkte der datenschutzrechtlichen Prüfung bei der Frage der Verantwortlichkeitszuweisung, der Umsetzung von Betroffenenrechten, dem Grundsatz der Datenrichtigkeit auf der Seite der Ausgabe, der Umsetzung von Dokumentationspflichten, den die Datenverarbeitung flankierenden Handlungsweisungen und Schulungen der Nutzer:innen des KI-Systems liegen wird.

Im Verlauf des Beratungsprozesses erfolgten fortlaufend Änderungen und Anpassungen des Projektes, um datenschutzrechtlichen Bedenken abzuhelfen. Die Handlungsanweisungen wurden beispielsweise angepasst und in Bezug auf Verarbeitungsverbote zur Erfüllung der Vorgaben bei normalem Schutzbedarf erweitert und konkretisiert. Es wurde eine Schwellwertanalyse nachgereicht. Verschiedene Punkte bleiben aber zum Ende des Berichtsjahres weiterhin offen. Es wurden seitens der Projektverantwortlichen verschiedene Nachbesserungen zugesagt, wie z.B. einzusetzende Filter zur Berücksichtigung von Betroffenenrechten und – soweit möglich – die Nutzung eines durchdachten Systemprompts zur sicheren Begrenzung des vorgegeben Nutzungsumfangs, die aber zum Berichtsschluss noch nicht umgesetzt waren.

Auch wenn der HmbBfDI die Anstrengungen der Senatskanzlei, das Projekt datenschutzgerecht zu gestalten und Rechte der Betroffenen im Blick zu halten, anerkennt, bedarf es an verschiedenen Stellen noch weiterer Informationen und Erläuterungen, um diese Bewertung auch in ein abschließendes Ergebnis überführen zu können. Aus Sicht des HmbBfDI bedarf es insbesondere der zugesagten Implementierung von Filtern, um Betroffenenrechten nachkommen zu können, sowie der Vorlage des Auftragsverarbeitungsvertrages mit Microsoft.

Es bestehen an verschiedenen Stellen noch unterschiedliche Rechtsansichten, wie etwa bei der Frage der Verantwortlichkeitsaufteilung zwischen Senatskanzlei und Fachbehörden bei der tatsächlichen Nutzung der Anwendung, oder bei der Frage, ob eine Datenschutzfolgeabschätzung zu erstellen ist, was aus Sicht des HmbBfDI geboten ist.

Besonders kritisch ist vor allem die geplante umfangreiche und zentrale Protokollierung der Nutzungsdaten in Logfiles zu bewerten. Die zentrale Erfassung und Verarbeitung dieser Daten durch die Senatskanzlei wären problematisch, da auf diesem Weg die eigentlich gebotene Trennung von Daten nach Mandanten durchbrochen würde. Die Senatskanzlei könnte, trotz aus ihrer Sicht getrennter Verantwortlichkeiten, das Nutzungsverhalten von Mitarbeitenden der Fachbehörden nachvollziehen und auswerten. Der Beratungsstand zum Abschluss des Berichtsjahres lässt den Umfang der Auswertung von Protokolldaten noch nicht in Gänze erkennen. Es bleibt insbesondere offen, ob im Rahmen der Speicherung von Nutzungsdaten in den Logfiles auch Dokumente/Uploads, die Teil des Prompts sind, erfasst werden. Hier fehlen noch aufklärende Angaben der Senatskanzlei.

Insgesamt muss der Beteiligungsprozess nun fortgeführt und zeitnah zu einem Abschluss gebracht werden.

7. Automatisierte Erstellung von Entlassbriefen im Krankenhaus

Das Universitätsklinikum Hamburg-Eppendorf (UKE) hat das KI-Sprachmodell „Argo" zur Unterstützung bei der Erstellung von Entlassbriefen entwickeln lassen. Argo soll die Patientenversorgung verbessern und die Mitarbeitenden im klinischen Alltag entlasten. Dies fordert datenschutzrechtliche Grundsätze im Kontext von KI-Training und Gesundheitsdaten heraus.

Im August 2024 wurde in Hamburger Medien darüber berichtet, dass das Universitätsklinikum Hamburg-Eppendorf (UKE) Arzt-

briefe mithilfe von KI erstellen lässt. Das KI-Sprachmodell „ARGO“ soll die Patientenversorgung verbessern und die Mitarbeitenden im klinischen Alltag entlasten. Veranlasst durch die Berichterstattung hat der HmbBfDI eine Prüfung eingeleitet.

Die Anwendung ARGO Clinical Letters (CL) basiert auf einem Large Language Model (LLM), das mit echten Behandlungsdaten aus der 2009 im UKE eingeführten digitalen Patientenakte trainiert worden ist. Dieses Training hat die gemeinnützige Tochtergesellschaft des UKE „Innovative Digitale Medizin“ (IDM) durchgeführt, deren Gründer ehemalige Ärzte aus dem UKE sind. Mit Hilfe von ARGO CL sollen Arztbriefe – also zum Zeitpunkt der Entlassung aus der Klinik zu erstellende Zusammenfassungen des Krankheitsverlaufs, erhobener Diagnosen, veranlasster Therapien und etwaiger Empfehlungen zu deren Fortführung – quasi per Knopfdruck und somit in einem Bruchteil der bisher dafür benötigten Zeit entworfen werden.

Im Rahmen eines durch die Aufsichtsbehörde initiierten Gesprächstermins wurden erstmalig technische Einzelheiten und daran anknüpfende Fragestellungen besprochen, unter anderem zu den datenschutzrechtlichen Verantwortlichkeiten, zu den Rechtsgrundlagen für das Training von ARGO CL, dem Einsatz im UKE sowie zu Informationspflichten. Im Nachgang zu diesem Termin haben IDM und UKE ihre Datenschutzdokumentation vorgelegt. Dazu hat der HmbBfDI Rückfragen gestellt und auch noch einmal um eine detailliertere Darstellung der Prozesse rund um das Training des LLM gebeten. Diese haben die Verantwortlichen beantwortet bzw. zur Verfügung gestellt.

Vorliegend sind in großem Umfang sensible Behandlungsinformationen für das Training eines KI-Modells genutzt worden, das zwar derzeit nur im UKE eingesetzt wird, perspektivisch aber auch in anderen deutschen Kliniken zum Einsatz kommen soll. Deshalb ist den in diesem Zusammenhang ergriffenen technischen und organisatorischen Maßnahmen, wie vor allem der Pseudonymisierung der Patientendaten vor ihrer Verwendung zu Trainingszwecken, eine be-

sondere Bedeutung beizumessen und einer genaueren Betrachtung zu unterziehen. Zu prüfen ist zudem, ob das trainierte Modell sodann nur noch anonymisierte Daten verarbeitet.

Hinzu kommt, dass die Anwendbarkeit bestehender Rechtsgrundlagen für eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO zum Training einer KI-Anwendung voraussetzt, dass damit wissenschaftliche Forschung betrieben wird. Hier kommt insbesondere § 12 des Hamburgischen Krankenhausgesetzes in Betracht. Diese Zielrichtung entspricht dem Leitbild der IDM, die Wissenschaft und Forschung im Bereich der digitalen Medizin fördern soll, was es aber anhand von entsprechender Dokumentation noch weiter zu belegen gilt. Nicht zuletzt die Frage der Transparenz und der Information der Betroffenen, deren Daten zum Training genutzt wurden, gilt es zu bewerten.

Insgesamt ist dies ein hochinteressantes und praxisrelevantes KI-System, das datenschutzrechtliche Herausforderungen mit sich bringt, die aber nicht unlösbar erscheinen. Der HmbBfDI wird in 2025 das System nach Abschluss der Prüfung bewerten können.

8. Erkennung Ertrinkender im Schwimmbad

Im Bereich der Schwimmaufsicht werden KI-Systeme unterstützend eingesetzt, die mit Überwasserkameras Bewegungsmuster erkennen, die zu einem Ertrinkungsunfall führen können. Der HmbBfDI begleitet beratend den Einsatz solcher Erkennungssysteme, die in Hamburg bei der Beaufsichtigung des Badebetriebs erstmalig im Testbetrieb genutzt werden.

Viele Schwimmbäder müssen ihre Öffnungszeiten ändern, später öffnen oder früher schließen. Einige bleiben sogar ganz geschlossen, weil es an ausgebildetem Personal fehlt, das Unfälle im Wasser erkennen und verhindern kann. Gleichzeitig nimmt die Zahl der Kinder, die schwimmen können, stetig ab. In dieser Situation stellt sich

die Frage, ob Künstliche Intelligenz in dieser Situation als wertvoller Helfer eingesetzt werden kann.

Im Bille-Bad im Südosten Hamburgs wird seit November 2024 das KI-basierte Überwachungssystem Lynxight getestet. Über zwei Schwimmbecken sind mehrere Kameras installiert, die frühzeitig Gefahren erkennen und zur Verhinderung schwerer Badeunfälle beitragen sollen. Wenn das System Notfallsituationen erkennt, wie etwa schwimmende Personen, die unterzugehen drohen, sendet es eine Alarmmeldung an die Smartwatch der Badeaufsicht. So kann diese rechtzeitig eingreifen. Die Idee ist nicht neu. Kameragestützte Systeme zur Erkennung von Ertrinkenden in Schwimmbädern existieren bereits seit zwei Jahrzehnten. Diese Systeme können regungslose Körper identifizieren – sei es schwebend im Wasser oder am Beckenboden liegend. Nach einer bestimmten Erkennungszeit lösen sie einen Alarm aus, der das fachkundige Schwimmbadpersonal benachrichtigt. Es handelt sich hierbei um reaktive Systeme, die Ertrinkungsunfälle detektieren, nachdem sie bereits eingetreten sind.

Neuere KI-basierte Erkennungssysteme versprechen Fortschritte in der Prävention von Ertrinkungsunfällen. Diese innovativen Systeme konzentrieren sich auf die frühzeitige Erkennung von Gefahrensituationen, indem sie das Verhalten der schwimmenden Personen an der Wasseroberfläche analysieren. Dazu müssen eine Vielzahl unterschiedlicher menschlicher Verhaltensweisen, Reaktionen und Bewegungsmuster im Wasser erfasst und ausgewertet werden. Dies geschieht mit Hilfe modernster Technologie. Maschinelles Lernen spielt dabei eine Schlüsselrolle.

Der Schwimmbadbetreiber bat den HmbBfDI um beratende Unterstützung. Der Einsatz von Künstlicher Intelligenz zur Unterstützung der Badeaufsicht, der bereits vor drei Jahren in Erwägung gezogen wurde, rückte aufgrund mehrerer Badeunfälle in diesem Jahr, von denen einer sogar tödlich endete, erneut in den Fokus. KI soll dabei helfen, Gefahrensituationen frühzeitig zu erkennen und präventiv darauf zu reagieren. Das schnelle Erkennen eines Notfalls ist von

höchster Bedeutung, da gerettete Personen durch den bis zur Rettung eingetretenen Sauerstoffmangel Hirnschädigungen mit möglichen dauerhaften Behinderungen erleiden können. Mit Hilfe von Kameras können selbst große und unübersichtliche Bereiche im Schwimmbad effektiv überwacht werden.

Der Datenschutz spielt bei der Einführung von KI-Systemen in Schwimmbädern eine zentrale Rolle. Bei der Inbetriebnahme des Lynxight-Systems im Bille-Bad wurden daher folgende Maßnahmen ergriffen:

- Die Kalibrierung erfolgte ohne Anwesenheit von Badegästen.
- Die Speicherung von Videosequenzen erfolgt lokal ohne Nutzung einer Cloud-Lösung.
- Randbereiche des Beckens sind verpixelt und werden nicht überwacht, um das Aufsichtspersonal außerhalb des Beckens nicht zu erfassen.
- Die Alarmierung auf der Smartwatch der Schwimmaufsicht zeigt einen stilisierten Beckenumriss mit einem roten Punkt, der die ungefähre Position eines in Not geratenen Badegasts anzeigt.

Besondere Aufmerksamkeit gilt dem Schutz der Vertraulichkeit.

In enger Zusammenarbeit werden noch offene Fragen im Rahmen einer fortlaufenden Beratung geklärt.

9. Intelligente Videoüberwachung Hansaplatz – Training mit Echtdaten

Die Polizei Hamburg plant, eine Anlage am Hansaplatz zur intelligenten Videoüberwachung mit Echtdaten von Hamburger Bürger:innen zu trainieren. Dieses Vorhaben zeigt den zunehmenden Einsatz intelligenter Systeme im Sicherheitsbereich und verdeutlicht, wie notwendig die nun erfolgte Reaktion des Gesetzgebers auf diesen fortschreitenden Wandel auch für den konkreten Einzelfall ist.

Seit 2019 überwacht die Polizei Hamburg den Hansaplatz und angrenzende Straßen im Stadtteil St. Georg zu bestimmten Zeiten mittels Videoüberwachung. Diese gefahrenabwehrrechtliche Maßnahme war bereits Gegenstand einer umfangreichen Prüfung des HmbBfDI (vgl. 29. Tätigkeitsbericht Datenschutz 2020, Kapitel III 2).

Im Jahr 2023 wurde die Anlage technisch aufgerüstet und das KI-System „IVBeo“ im Rahmen eines dreimonatigen Pilotversuchs getestet. Von Juli bis Oktober 2023 analysierte das KI-System die Videodaten von vier Kameras, um auffällige Bewegungsmuster wie Schläge, Tritte oder Stürze zu erkennen. Bei entsprechender Detektion zeigte das System das Live-Bild ohne weitere Markierungen auf einem separaten Monitor an und informierte die Polizeibeamt:innen vor den Bildschirmen durch ein Signal. Die Entscheidung über weitere polizeiliche Maßnahmen blieb den Beamt:innen vorbehalten. „IVBeo“ basiert auf einem KI-Modell, welches mit Videomaterial aus Mannheim trainiert wurde. Ein weiteres KI-Training im Hamburger Pilotversuch mit Hamburger Daten fand nicht statt. Der HmbBfDI begleitete diesen Pilotversuchs und hatte zunächst keine datenschutzrechtlichen Bedenken (vgl. 32. Tätigkeitsbericht Datenschutz 2023, Kapitel III 1).

Die Polizei Hamburg stellte im Rahmen der Projektevaluation fest, dass zahlreiche Detektionen des Systems nicht nachvollziehbar wa-

ren, da die Beamt:innen keine Gefahrensituation erkennen konnten. Vor diesem Hintergrund plant die Polizei Hamburg, „IVBeo“ an die spezifischen Bedingungen des Hansaplatzes anzupassen, indem das KI-Modell mit Hamburger Videodaten nachtrainiert wird (sog. Finetuning). Hierfür sollen dem Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung Hamburger Videodaten für Trainingszwecke zur Verfügung gestellt werden.

Diese geplante Weiterentwicklung der intelligenten Beobachtung erscheint zwar praktisch sinnvoll, wirft jedoch datenschutzrechtliche Fragen auf. Die Verwendung von Echtdaten u.a. unbeteiligter Passanten und Anwohner:innen auf einem öffentlich zugänglichen Platz für das Training erscheint zwar verfassungsrechtlich nicht von vorneherein unmöglich. Wenn – wie im vorliegenden Fall – aber eine Entwicklung des Systems mithilfe von personenbezogenen Daten durchgeführt werden soll, stellt dies eine datenschutzrechtlich relevante Verarbeitung dar, die einer Rechtsgrundlage bedarf.

Bislang verfügte das PolDVG nicht über eine Rechtsgrundlage für das beabsichtigte KI-Training. Die bisher bestehenden Rechtsgrundlagen für die Polizei dienten überwiegend alleine dem Zweck der Gefahrenabwehr. Die von der Polizei zunächst herangezogenen Normen enthielten zudem weder spezifische Garantien für die Betroffenen, noch berücksichtigten sie die besonderen Risiken, die mit dem Training von KI-Modellen einhergehen. Insbesondere kam die von der Polizei erwogene Vorschrift des § 37 Abs. 1 Satz 1 PolDVG, welche die Fort- und Ausbildung von Polizeibeamt:innen betrifft, nicht als Rechtsgrundlage für das Training einer KI in Betracht, da der Gesetzgeber – unstreitig – bei Schaffung der Norm im Jahr 1990 weder diese Möglichkeit noch die damit einhergehenden Risiken im Blick haben konnte.

Im Hinblick auf diese konkrete Fragestellung, aber auch bezüglich der zu erwartenden weiteren Digitalisierung des polizeilichen Handelns hat der HmbBfDI im Rahmen der im Berichtszeitraum erfolgten Beteiligung zum Senatsdrucksachenentwurf „Drittes Gesetz

zur Änderung polizeilicher Vorschriften“ unter ausdrücklichem Hinweis auf dieses Projekt dafür plädiert, eine Norm zu schaffen, die neue digitale Technologien und die damit einhergehenden neuen Dimensionen von Eingriffstiefen in den Blick nimmt und gesetzgeberische Leitlinien vorgibt. Durch den am 15.1.2025 angenommenen Änderungsantrag (Bü.-Drs. 22/17442) wird nun das Trainieren und Testen von IT-Systemen erfreulicherweise erstmalig und ausdrücklich in § 37a PolDVG auf ein rechtliches Fundament gestellt (vgl. Kapitel III 1.1).

Eine abschließende Beurteilung der beabsichtigten Verarbeitung von personenbezogenen Daten – Training des zur intelligenten Videoüberwachung eingesetzten KI-Modells mit Echtdaten vom Hansaplatz – durch den HmbBfDI ist gleichwohl bislang noch nicht erfolgt, weil es nicht möglich ist nachzuvollziehen, welche konkrete Verarbeitung von personenbezogenen Daten überhaupt erfolgen soll. Die bisherigen Auskünfte durch die Polizei Hamburg sind zu wenig aussagekräftig, insbesondere fehlt es weiterhin an einer hinreichenden Beschreibung der Verarbeitungstätigkeit.

10. KI bei Meta und X

In 2024 kündigten gleich mehrere Betreiber sozialer Netzwerke an, die konzerneigenen KI-Modelle mit personenbezogenen Daten der Nutzer:innen zu trainieren, so auch Meta und Twitter. Das KI-Training warf dabei zahlreiche rechtliche Fragen nach der DSGVO auf. Nach Beschwerden Betroffener und Intervention der in Europa federführend zuständigen irischen Aufsichtsbehörde IDPC wurden die Vorhaben mit Blick auf Betroffene im Geltungsbereich der DSGVO zunächst verschoben.

Den HmbBfDI erreichten Ende Mai 2024 zahlreiche Anfragen besorgter Bürger:innen. Das Unternehmen Meta Platforms Ireland Limited (Meta), Betreiber von u.a. Facebook und Instagram, hatte auf seinen Plattformen Benachrichtigungen zum geplanten Einsatz

einer „KI bei Meta“ veröffentlicht. Europaweit wurden Millionen von Nutzer:innen über die beabsichtigte Verwendung ihrer personenbezogenen Daten für die Entwicklung und Verbesserung generativer KI-Features informiert. Konkret sollten ab dem 26.06.2024 u.a. auf den Plattformen vorhandene Beiträge, Fotos und Bildunterschriften zum Training von Modellen der künstlichen Intelligenz genutzt werden. Ausgenommen werden sollten lediglich Inhalte aus Privatnachrichten nicht öffentlicher Chats.

Für die Verarbeitung der personenbezogenen Daten zu diesem Zweck berief sich Meta auf die Rechtsgrundlage des berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f) DSGVO, führte hierzu jedoch nur vage aus, dass die genutzten Informationen der Entwicklung und Optimierung von „KI bei Meta“ dienen würden. Zudem räumte Meta auf seinen Plattformen Facebook und Instagram den angemeldeten Nutzer:innen und auch Betroffenen ohne einen eigenen Account die Möglichkeit ein, ihr Widerspruchsrecht gegen das KI-Training auszuüben. Hierfür waren die angemeldeten Nutzer:innen gehalten, ein Formular auszufüllen und dort neben bestimmten Kontaktdaten auch eine Begründung für ihren Widerspruch anzugeben. Für Betroffene ohne eigenen Account, deren personenbezogene Daten auf Drittseiten gespeichert sein könnten, stellte Meta ein separates Widerspruchs-Formular zur Verfügung für den Fall, dass der Konzern diese Daten für KI-Trainingszwecke einkauft.

Ob das berechtigte Interesse in diesen Fallkonstellationen eine taugliche Rechtsgrundlage darstellt, war fraglich. Insbesondere die Interessenabwägung wird bei unspezifischen Zwecken, die alle Arten von KI-Modellen und -Anwendungen umfassen, regelmäßig nicht zugunsten der Verantwortlichen ausfallen können. Grundsätzlich gilt: Stützt ein datenschutzrechtlich Verantwortlicher die Verarbeitung personenbezogener Daten auf die Rechtsgrundlage des berechtigten Interesses, steht den Betroffenen ein gesetzliches Widerspruchsrecht zu, Art. 21 Abs. 1 S. 1 DSGVO. Wird von dem Widerspruchsrecht Gebrauch gemacht und führen die Betroffenen Gründe an, die die berechtigten Interessen des Verantwortlichen überwiegen, ist

der Verantwortliche zu einer Verarbeitung der personenbezogenen Daten nicht mehr befugt.

Um möglichst viele Bürger:innen zu erreichen, veröffentlichte der HmbBfDI auf seiner Homepage einen umfassenden Beitrag zu der Ankündigung Metas. Der HmbBfDI zeigte konkret auf, wie Bürger:innen der Verwendung der eigenen Daten auf den Webseiten Metas widersprechen konnten und informierte über die tatsächlichen und rechtlichen Hintergründe eines KI-Trainings mit personenbezogenen Daten.

Insgesamt warfen Metas Pläne zahlreiche rechtliche Fragen auf, u.a. hinsichtlich der gewählten Rechtsgrundlage, aber auch mit Blick auf die in Art. 5 Abs. 1 und 2 DSGVO niedergelegten Grundsätze zu Transparenz und Zweckbindung, die bei der Verarbeitung personenbezogener Daten zu berücksichtigen sind. Angesichts Millionen Betroffener in allen Mitgliedsstaaten war hier eine europaweit einheitliche Bewertung durch die Datenschutzaufsichtsbehörden dringend geboten, insbesondere unter Beteiligung der in Europa für Meta federführend zuständigen irischen Aufsichtsbehörde (IDPC). Der HmbBfDI, der unter den deutschen Datenschutzaufsichtsbehörden zuständigkeitshalber eine hervorgehobene Stellung einnimmt, koordinierte das Verfahren innerhalb Deutschlands und gab im Namen aller deutschen Datenschutzaufsichtsbehörden an Meta adressierte Stellungnahmen ab.

Die IDPC forderte Meta schließlich auf, den Start der Datenverarbeitung zu verschieben. Dieser Aufforderung kam Meta am 14. Juni 2024 nach und gab auch öffentlich bekannt, die konzerneigenen KI-Modelle bis auf Weiteres nicht mit Inhalten zu trainieren, die europäische Nutzer:innen auf Facebook oder Instagram geteilt haben. Der Konzern kündigte an, die Nutzer:innen zu informieren, bevor Meta mit der Verwendung ihrer Daten zum KI-Training beginnt.

Daneben hatte der HmbBfDI auch auf den Beginn des KI-Trainings bei X reagiert. Twitter International Unlimited Company (TIUC), die

wichtigste irische Tochtergesellschaft der Social-Media-Plattform X, hatte bereits im Mai 2024 mit dem Training des konzerneigenen Large Language Models (LLM) namens Grok AI begonnen. Grok sollte nach Plänen des Konzerns als KI-Suchassistent fungieren, der ausschließlich den Inhabern von X-Premiumkonten zur Verfügung steht. Auch TIUC berief sich bei dieser Datenverarbeitung auf berechtigte Interessen nach Art. 6 Abs. 1 lit. f) DSGVO, ohne jedoch den Nutzer:innen ausreichend Informationen über die genutzten Datenkategorien und eine leicht auffindbare Widerspruchsmöglichkeit nach Art. 21 DSGVO zur Verfügung zu stellen.

Dementsprechend leitete die IDPC Anfang August 2024 vor dem irischen High Court ein Verfahren gegen TIUC ein. Die Klage richtete sich gegen die Verwendung personenbezogener Daten von X-Nutzern zu Trainingszwecken, die der DSGVO unterliegen. Auch dieses Training wurde in der EU bzw. EWR zunächst ausgesetzt.

Da das Verfahren vor dem irischen High Court nur einen konkreten Verarbeitungszeitraum umfasste, blieben noch einige wichtige Punkte ungeklärt. Der HmbBfDI stand seit der Unterrichtung im Juni 2024 im intensiven Austausch mit der federführenden IDPC sowie anderen europäischen Aufsichtsbehörden und richtete unter Einbeziehung anderer deutscher Aufsichtsbehörden einen umfangreichen Fragenkatalog an die IDPC, um ein vollständiges Bild über die Verarbeitung zu KI-Trainingszwecken zu gewinnen.

Beide Kooperationsverfahren mit der IDPC nach Art. 61 DSGVO dauern noch an, nicht zuletzt aufgrund einer zwischenzeitlich beantragten und verabschiedeten Stellungnahme durch den Europäischen Datenschutzausschuss (EDSA), siehe Kapitel IV 3. Die inzwischen vorliegende Stellungnahme des Europäischen Datenschutzausschusses zur KI-bezogenen Verarbeitung personenbezogener Daten dürfte allerdings als eine wichtige Weichenstellung für die abschließende Prüfung der konkreten Modelle durch die IDPC dienen.

11. Frag die DSK – KI-System für die interne Nutzung

Der HmbBfDI entwickelte im Jahr 2024 ein eigenes KI-System, mit welchem die Positionen aus den Veröffentlichungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) per Chat abgerufen werden können. Das KI-System „Frag die DSK" soll die Referent:innen beim HmbBfDI bei der täglichen Arbeit unterstützen.

Ein zentrales Anliegen der DSGVO ist die einheitliche Anwendung des Datenschutzrechts im Europäischen Wirtschaftsraum. In Deutschland ist es die Aufgabe der DSK, durch Orientierungshilfen, Beschlüsse und andere Veröffentlichungen für eine konsistente Rechtsanwendung zu sorgen. Über die Jahre hinweg sind von ihr mehrere Hundert Dokumente veröffentlicht worden, welche die Referent:innen u.a. bei der Bearbeitung von Beschwerden im Blick behalten müssen.

Um diese Aufgabe zu erleichtern, wurde das KI-System „Frag die DSK" entwickelt. Es enthält alle Veröffentlichungen der DSK, aktualisiert diese täglich und macht sie mithilfe eines benutzerfreundlichen Webinterfaces zugänglich. Die Nutzer:innen können abstrakte Datenschutzrechtsfragen in das System eingeben und erhalten präzise Antworten, die die Position der DSK wiedergeben. Das Besondere dabei: Das System erkennt die semantische Bedeutung der Nutzer:innenanfrage, auch wenn nicht das „richtige Schlagwort" verwendet wurde, und identifiziert selbständig inhaltlich relevante Dokumente.

Neben einer ausformulierten Antwort erhalten Nutzer:innen Zitate aus den zur Beantwortung herangezogenen Dokumenten nebst Link zu den jeweiligen Original-PDF-Dateien, welche beim Klicken auf der zitierten Seite geöffnet werden. Dies ermöglicht den Nutzer:innen

die Überprüfung, ob die KI-generierten Antworten inhaltlich richtig sind. Durch die verpflichtende Kontrolle der Ergebnisse kann u.a. ausgeschlossen werden, dass die Nutzung des KI-Systems in den Anwendungsbereich des Art. 22 DSGVO (automatisierte Entscheidungsfindung) fällt.

„Frag die DSK" läuft auf einem Server des HmbBfDI und basiert auf einem sog. Retrieval-Augmented Generation (RAG)-System. Die hierfür erforderlichen KI-Modelle, insbesondere ein kleines Large Language Model (LLM), werden bei einem europäischen Dienstleister betrieben. Die Eingabe und das Abfragen von personenbezogenen Daten sind untersagt. Diese organisatorische Maßnahme wird technisch flankiert durch einen Ausgangsfilter, welcher unzulässige Ausgaben unterdrückt. Die Eingaben und Ausgaben werden nicht gespeichert, was die Risiken einer unbeabsichtigten Datenverarbeitung zusätzlich minimiert.

Mit „Frag die DSK" hat der HmbBfDI nicht nur ein Werkzeug zur Effizienzsteigerung geschaffen, sondern zugleich eigene praktische Erfahrungen gesammelt, welche in der Prüfung von vergleichbaren KI-Fällen fruchtbar gemacht werden können. Da das System modular aufgebaut ist, kann es zudem leicht mit weiteren Datensätzen ergänzt werden, wie etwa den Veröffentlichungen des Europäischen Datenschutzausschusses (EDSA) oder den Tätigkeitsberichten der Datenschutzaufsichtsbehörden.

Insgesamt stellt „Frag die DSK" ein Beispiel dafür dar, wie moderne Technologien verantwortungsvoll eingesetzt werden können, um komplexe Aufgaben im Bereich des Datenschutzes effizienter zu gestalten. Seit November 2024 wird es produktiv beim HmbBfDI eingesetzt.

V. BUSSGELDER ANORDNUNGEN, GERICHTSVERFAHREN

Bussgelder, Anordnungen, Gerichtsverfahren

1. Datenschutzverstoß im Forderungsmanagement: Hohes Bußgeld gegen Hamburger Unternehmen

Im Rahmen einer umfassenden Überprüfung der Forderungsmanagement-Branche hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit einen schwerwiegenden Datenschutzverstoß festgestellt und ein Bußgeld in Höhe von 900.000 Euro gegen einen Dienstleister verhängt.

Der HmbBfDI hat in den vergangenen zwei Jahren systematisch die Forderungsmanagement-Branche in Hamburg untersucht. Im Fokus der Überprüfungen standen marktmächtige Unternehmen, deren Datenverarbeitungspraktiken umfangreich geprüft wurden. Die Prüfungen umfassten unter anderem Verzeichnisse der Verarbeitungstätigkeiten, technische und organisatorische Sicherheitsmaßnahmen sowie die Qualität der Transparenz gegenüber betroffenen Personen. Zusätzlich führte der HmbBfDI Vor-Ort-Kontrollen durch.

Im Rahmen dieser Prüfung deckte der HmbBfDI in einem Unternehmen erhebliche Defizite auf, insbesondere in Bezug auf die Umsetzung der Löschpflichten: Zwischen Dezember 2018 und Dezember 2022 speicherte dieses Hamburger Unternehmen aus der Forderungsmanagement-Branche über 420.000 Datensätze mit personenbezogenen Informationen ohne rechtliche Grundlage. Obwohl die gesetzlichen Löschfristen längst abgelaufen waren, fehlte ein wirksames Löschkonzept, sodass die betroffenen personenbezogenen Daten erst zwischen November und Dezember 2023 gelöscht wurden. Dabei handelte es sich teilweise um Datensätze, deren rechtmäßige Speicherung bereits fünf Jahre zuvor geendet hatte. Diese Praxis verstieß insbesondere gegen Art. 5 Abs. 1 lit. a) sowie Artikel 6 Abs. 1 DSGVO.

Aufgrund der großen Anzahl an Datensätzen sowie der Art der gespeicherten Informationen, die typischerweise Angaben über säumi-

ge Schuldner:innen umfassen und daher als tendenziell besonders sensibel einzustufen sind, war die Einleitung eines Ordnungswidrigkeitenverfahrens angezeigt. Der eingeräumte Verstoß führte zur Verhängung eines Bußgelds in Höhe von 900.000 Euro. Bei der Bemessung der Geldbuße wurde im Besonderen berücksichtigt, dass das Unternehmen den Verstoß eingeräumt und an der Aufklärung des Verstoßes umfangreich mitgewirkt hatte sowie im Hinblick auf die überlangen Speicherungen schnell Abhilfe geschaffen hatte.

In diesem Zusammenhang ist die Notwendigkeit eines klaren und wirksamen Löschkonzepts zu betonen. Löschkonzepte sind ein grundlegender Bestandteil datenschutzkonformer Prozesse. Unternehmen, die diesen Anforderungen nicht nachkommen, handeln nicht nur gesetzeswidrig, sondern riskieren auch künftig hohe Geldbußen.

2. Datenleck beim Cashback

Einkaufen, ein Foto des Kassenbons hochladen und für bestimmte Produkte Geld zurückbekommen: Solche Cashback-Werbeaktionen organisierte eine Hamburger Agentur für ihre Kunden. Leider mit unzureichenden technischen Schutzmaßnahmen für die Daten der Teilnehmenden. Dies sanktionierte der HmbBfDI mit einer Geldbuße.

Zwei Hinweisgeber machten den HmbBfDI im Sommer 2023 darauf aufmerksam, dass sie im Internet auf umfangreiche Teilnehmerdaten aus Werbeaktionen zugreifen konnten. Die Agentur, die diese Aktionen als Auftragsverarbeiterin ihrer Werbekunden umsetzte, hatte ein selbst entwickeltes Online-Tool eingesetzt, mit dem die Teilnehmenden Fotos ihrer Kassenbons einreichen und persönliche Informationen angeben konnten, um eine Rückerstattung zu erhalten oder an Gewinnspielen teilzunehmen. Zu diesen Informationen gehörten je nach Art der Werbeaktion Name, Postanschrift, Geburtsdatum, Bankverbindung, E-Mail-Adresse und Kundennummer. Betroffen waren auch Kampagnen bekannter Markenhersteller.

Die Sicherheitsarchitektur, die dem Tool zugrunde lag, erwies sich dabei als zu schwach. Unbefugte konnten ohne jede Überwindung besonderer technischer Hürden Teilnehmerdaten herunterladen. Es kam erschwerend hinzu, dass einige Datensätze teils Monate nach der Abwicklung einer Werbeaktion nicht gelöscht waren. Zudem wurden 270 Backups eines Servers fortlaufend gespeichert, obwohl ausreichend aktuellere Backups vorhanden waren. Auf diese Weise erhöhte sich die Zahl der Personen, die von dem Datenleck betroffen waren. Der HmbBfDI konnte nachweisen, dass ein Zugriff auf mindestens 56.635 Datensätze zeitweise möglich war.

Der HmbBfDI hat die technisch-organisatorischen Maßnahmen intensiv geprüft. Dabei verhielt sich die betroffene Agentur überwiegend kooperativ und stellte die erforderlichen Informationen zur Verfügung. Sie zeigte sich zudem einsichtig, dass ihr Tool in dieser Form für die Art und den Umfang der angebotenen Werbeaktionen ungeeignet war und kündigte an, es – nachdem die bekanntgewordenen Sicherheitslücken kurzfristig geschlossen worden waren – mit dem Abschluss der letzten noch laufenden Aktion vollständig vom Markt zu nehmen.

Wegen der hohen Zahl betroffener Personen und dem erheblichen Missbrauchspotenzial, das insbesondere für gespeicherte Bankdaten bestand, verhängte der HmbBfDI ein Bußgeld im unteren fünfstelligen Bereich. Sanktioniert wurden damit ein Verstoß gegen Artikel 32 DSGVO sowie mehrere Verstöße gegen Art. 5 Abs. 1 lit. e DSGVO. Die Agentur hat das Bußgeld akzeptiert.

3. Verspätete Beantwortung von Auskunftsersuchen

Bürger:innen haben das Recht, von Unternehmen Auskunft über die Verarbeitung sie betreffender personenbezogener Daten zu erhalten. Wird dieser Anspruch nicht fristgerecht erfüllt, drohen Bußgelder.

Im Berichtszeitraum hat der HmbBfDI ein Bußgeldverfahren gegen ein in Hamburg ansässiges Unternehmen wegen Verstößen gegen Art. 12 DSGVO i.V.m. Art. 15 DSGVO durchgeführt. Der HmbBfDI wurde durch fünf Beschwerden, die den HmbBfDI innerhalb eines halben Jahres erreichten, auf das Unternehmen aufmerksam. Die Beschwerdeführer:innen bemängelten, dass ihnen das Unternehmen jeweils die beantragte Auskunft nach Art. 15 DSGVO nicht erteilt habe.

Das Auskunftsrecht soll natürliche Personen u.a. in die Lage versetzen, die Rechtmäßigkeit einer Datenverarbeitung sowie die Richtigkeit der verarbeiteten Daten zu überprüfen und die Ausübung weiterer Rechte, wie etwa das Recht auf Löschung oder das Widerspruchsrecht, erleichtern. Die Auskunft ist unverzüglich, spätestens aber binnen eines Monats nach Antragseingang zu erteilen. Nur ausnahmsweise darf eine Beantwortung binnen drei Monaten erfolgen. In diesem Fall sind Verantwortliche jedoch verpflichtet, Antragsteller:innen innerhalb eines Monats nach Antragseingang über die Fristverlängerung und die Gründe für die Verzögerung zu informieren.

Dieser Verpflichtung ist das Unternehmen in den fünf vorgeworfenen Fällen sorgfaltspflichtwidrig nicht nachgekommen. Der HmbBfDI hat wegen dieser Verstöße insgesamt eine Geldbuße im niedrigen fünfstelligen Bereich verhängt. Der HmbBfDI verkennt dabei nicht, dass eine fristgerechte Beantwortung von Auskunftsersuchen insbesondere sehr kleine, aber auch – wie in diesem Fall – sehr große Unternehmen, die jährlich mehrere tausend Auskunftsersuchen erhalten, die nicht selten gemeinsam mit anderen (zivilrechtlichen)

Anliegen vorgetragen werden, vor Herausforderungen stellt. Gerade großen Unternehmen, deren Kerngeschäft in der Verarbeitung personenbezogener Daten besteht, ist es aber zuzumuten, zuverlässige organisatorische Maßnahmen einzurichten, um geltend gemachte Betroffenenrechte zu erkennen und fristgerecht zu bearbeiten. Bei der Zumessung der (Einzel-)Bußgelder wurde mildernd berücksichtigt, dass das Unternehmen den Antragstellern die Auskünfte unverzüglich erteilt hat, nachdem die Fristüberschreitungen bei ihm bekannt geworden waren und es zudem erhebliche Anstrengungen unternommen hat, um seinen Prozess zur Erfüllung von Anträgen gemäß den Artikeln 15 bis 22 DSGVO weiter zu verbessern. Ferner hat das Unternehmen umfangreich und konstruktiv mit dem HmbBfDI zusammengearbeitet und die Verstöße eingeräumt sowie sein Bedauern über die Vorfälle glaubhaft zum Ausdruck gebracht. Auch dies hat der HmbBfDI mildernd gewertet.

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

4. Datenverarbeitung in Kindertagesstätten

In Kitas werden zur Kommunikation mit den Eltern vermehrt Apps eingesetzt. Bei der Einführung und dem Betrieb von Kita-Apps müssen datenschutzrechtliche Vorschriften beachtet werden. Unterbleibt dies, drohen empfindliche Bußgelder.

Im Berichtszeitraum hat der HmbBfDI ein Bußgeldverfahren gegen einen Betreiber von Kindertagesstätten durchgeführt. Der Betreiber hatte in seinen Kitas eine App eingeführt, die es Eltern ermöglicht, die Entwicklungsdokumentation des Kindes sowie Vertrags- und Stammdaten in einem bestimmten Umfang einzusehen und zu verwalten. Zudem gibt die App den Eltern die Gelegenheit, den Alltag ihrer Kinder durch eingestellte Bilder und Videos „live“ mitzuverfol-

gen und bestimmte Anliegen wie die An- und Abmeldung des Kindes im Krankheitsfall bequem zu erledigen.

Nach der Einführung der App erhielt der HmbBfDI mehrere Beschwerden von Eltern. Im Rahmen der daraufhin eingeleiteten Prüfung stellte der HmbBfDI diverse Verstöße gegen Vorschriften der DSGVO fest. So hatte das Unternehmen Fotoaufnahmen mindestens eines Kindes ohne Rechtsgrundlage in der App verarbeitet. Die Verarbeitung von Fotos der betreuten Kinder kann nur auf eine Einwilligung der Eltern gemäß Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO gestützt werden, da diese Verarbeitung weder zum Zweck der Vertragserfüllung noch zur Erfüllung obliegender Dokumentationspflichten erforderlich ist. Eine solche Einwilligung hatte die Beschwerdeführerin aber nicht erteilt. Ferner hatte es das Unternehmen unterlassen, geeignete technische und organisatorische Maßnahmen zu treffen, um zu verhindern, dass Eltern nach Beendigung des eigenen Vertragsverhältnisses weiterhin personenbezogene Daten anderer Kinder, hier insbesondere neue Fotos anderer Kinder, in der App einsehen konnten. Zudem hat das Unternehmen es versäumt, Eltern, mit denen bereits vor der Einführung der App ein Vertragsverhältnis bestand, über die Datenverarbeitung in der App gemäß Art. 13 Abs. 1, 2 DSGVO zu informieren. Schließlich hat das Unternehmen auch sorgfaltspflichtwidrig gegen Art. 9 Abs. 1 DSGVO verstoßen, indem es ohne Einwilligung der Eltern im Rahmen einer sogenannten Windeltracker-Funktion Gesundheitsdaten der betreuten Kinder verarbeitete.

Der HmbBfDI hat wegen dieser Verstöße insgesamt eine Geldbuße im hohen fünfstelligen Bereich verhängt. Bei der Zumessung der (Einzel-)Bußgelder wurde mildernd berücksichtigt, dass das Unternehmen nach Bekanntwerden der Verstöße alle notwendigen Maßnahmen nachgeholt hat. Ferner hat das Unternehmen umfangreich mit dem HmbBfDI zusammengearbeitet und die Verstöße eingeräumt. Auch dies hat der HmbBfDI mildernd gewertet.

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

5. Verwarnung im Bezirksamt Wandsbek

Den HmbBfDI erreichte ein Hinweis auf unabgeschlossene Aktenräume im Bezirksamt Wandsbek. Bei einer unangekündigten Vor-Ort-Kontrolle konnte bestätigt werden, dass ein Archivraum zur Aufbewahrung von Fallakten nicht ordnungsgemäß verschlossen war. In den öffentlich zugänglichen Räumlichkeiten des Bezirksamts stellt dies einen untragbaren Sicherheitsmangel dar. Der HmbBfDI hat daher das zuständige Fachamt verwarnt. Die Bezirksamtsleitung hat für Sensibilisierung im Bezirksamt gesorgt, um derartige Vorfälle zukünftig zu vermeiden.

Ausgangspunkt des Verfahrens war der Hinweis einer Bürgerin, die das Bezirksamt Wandsbek besuchte und auf der Suche nach einem als öffentlich besuchbar ausgewiesenen Gemälde auf einen nicht verschlossenen Raum stieß, der Regale mit unzähligen Akten enthielt. Die Hinweisgeberin betrat den Raum nicht und öffnete auch keine der vorhandenen Akten. Dies ist allen Personen, die sich in einer vergleichbaren Position wiederfinden, genauso zu empfehlen. Merken Sie sich die Details, aber lassen Sie sich keinesfalls zu eigenen Ermittlungen hinreißen.

Mit der Meldung an den HmbBfDI wählte die Hinweisgeberin die korrekte Vorgehensweise. Derartige Hinweise auf datenschutzrechtliche Verstöße sind ein wichtiger Baustein bei der Arbeit des HmbBfDI.

Der HmbBfDI entschied sich dazu, die Lage im Bezirksamt vor Ort selbst zu überprüfen, bevor eine Anhörung erfolgen sollte. Mitarbeitende haben daher unangekündigt während der regulären Besuchszeiten eine verdeckte Kontrolle vorgenommen. Dabei wurde ein unverschlossener Raum mit Akten vorgefunden. Eine Stichprobe ergab, dass es sich um aktuell in Bearbeitung befindliche Akten handelte. Erschwerend kam hinzu, dass es sich um Fälle aus dem sozialen Be-

reich handelte mit sensiblen Daten von Bürger:innen. Der HmbBfDI konnte damit selbst bestätigen, dass der gemeldete Vorfall kein Einzelfall gewesen ist. Da ein systematisches Problem in diesem Bereich gar nicht erst entstehen soll, hat der HmbBfDI eine Maßnahme ergriffen.

Der HmbBfDI übt nicht nur die Aufsicht über private Verantwortliche aus, sondern überwacht gem. § 19 Abs. 2 HmbDSG auch öffentliche Stellen, wie bspw. die hamburgischen Bezirksämter. Auch die physische Akte unterfällt dem Datenschutz. Zwar denken die meisten Menschen beim Thema Datenschutz zunächst an die elektronische Verarbeitung personenbezogener Daten. Doch ist in Art. 2 Abs. 1 und Erwägungsgrund 15 der DSGVO klargestellt, dass auch die „manuelle Verarbeitung" personenbezogener Daten unter die DSGVO fällt, wenn diese „in einem Dateisystem [...] gespeichert werden sollen". Da eine elektronische Weiterarbeitung stets erfolgt, ist auch die Aufbewahrung der Aktenbestände nach den Grundsätzen der DSGVO zu gewährleisten. Dem Grundsatz der „Integrität und Vertraulichkeit", Art. 5 Abs. 1 lit. f) DSGVO, folgend bedeutet dies, personenbezogene Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit gewährleistet, einschließlich dem Schutz vor unbefugter Verarbeitung. Übertragen auf den Sachverhalt sind Aktenarchive daher stets verschlossen zu halten, wenn diese nicht überwacht werden können und theoretisch dem Zugriff durch die Öffentlichkeit ausgesetzt sind.

Der HmbBfDI hat nach Anhörung der zuständigen Stelle eine Verwarnung gegenüber dem Fachamt Jugend- und Familienhilfe ausgesprochen. Dieses Fachamt ist formell für den unverschlossen vorgefundenen Raum zuständig. Doch kam es dem HmbBfDI nicht darauf an, ein einzelnes Fachamt besonders herauszuheben. Die Aufgabe der Aktensicherung betrifft alle Bereiche aller Bezirksämter. Das angestoßene Verfahren wurde zum Anlass genommen, allgemein und amtsübergreifend auf die Wichtigkeit der korrekten Aktenverwahrung hinzuweisen.

6. Der Spanner ist kein Künstler: sexualisierte Aufnahmen verletzten die Privatsphäre

Der HmbBfDI hat erneut Ordnungswidrigkeitenverfahren wegen heimlich angefertigter Fotos eingeleitet, die die Privatsphäre verletzen, insbesondere bei minderjährigen und jungen Frauen. Während Kritiker befürchten, dass die Regulierung die sog. Streetphotography beeinträchtigen könnte, sieht der HmbBfDI keine Schwierigkeit, zwischen Straßenfotografie und rechtswidriger „Creeptography" zu unterscheiden.

Auch im zurückliegenden Berichtszeitraum hat der HmbBfDI Ordnungswidrigkeitenverfahren aufgrund der Anfertigung rechtswidriger Lichtbilder geführt und Geldbußen verhängt. Die Fallgruppe beschäftigt den HmbBfDI bereits über mehrere Berichtszeiträume hinweg, ohne dass Besserung in Sicht wäre. Kennzeichnend für diese Fallgruppe sind heimlich angefertigte Schnappschüsse ohne erkennbaren Schöpfungsgehalt, die gleichzeitig einen erheblichen Eingriff in Privat- oder Intimsphäre der Opfer darstellen. Die Opfer sind ausschließlich minderjährige oder junge Frauen.

Für die Anfertigung derartiger Schnappschüsse ist der Anwendungsbereich der DSGVO eröffnet. Die Anfertigung von Bildern fremder Personen in der Öffentlichkeit verlässt den privaten Raum und damit den Schutzbereich, der durch Art. 2 Abs. 2 lit. c) DSGVO („Haushaltsausnahme") eingeräumt wird, da sich letztlich bereits das Objekt der fotographischen Betrachtung schon außerhalb der eingeräumten Privatsphäre befindet und daher nicht durch Anfertigung eines Bildes in diese hineingezogen werden kann. Dies ist auch in der Vergangenheit bereits gerichtlich bestätigt worden (AG Hamburg, Beschl. v. 03.07.2020 – 163 Gs 656/20). Dadurch wäre eine Rechtsgrundlage erforderlich, die nicht ersichtlich ist.

Folgende Fallgestaltungen waren Gegenstand von Ordnungswidrigkeitsverfahren:

- In einem Fall fertigte eine Person auf dem Hamburger Dom, einem überregional bekannten Jahrmarkt, heimlich Schnappschüsse einer Geschädigten mit seinem Mobiltelefon an, wobei der Fokus der Aufnahmen auf ihrem Gesäß lag. Nach mehrfacher Aufforderung durch die Geschädigte und ihre Begleiterinnen, löschte er die Lichtbilder. Bei Eintreffen der herbeigerufenen Polizei gab er nach Aufforderung das zwischenzeitlich in seiner Unterhose versteckte Mobiltelefon heraus.

- In einem anderen Fall zeichnete ein Radfahrer fortlaufend eine Geschädigte auf, die vor ihm mit einem Longboard eine frequentierte Straße entlangfuhr. Auch ihm kam es dabei insbesondere auf eine Dokumentation des Gesäßes der Geschädigten an. Der Aufzeichnungsvorgang wurde von zufällig vorbeifahrenden Polizeibeamt:innen bemerkt. Die Aufzeichnung wurde auf Aufforderung hin gelöscht.

- In einer U-Bahn der Linie U1 fertigte ein Fahrgast Schnappschüsse mit seinem Mobiltelefon von einer 13-jährigen und einer 14-jährigen Jugendlichen an. Auf den Fotos waren Teile der Hüfte, der Gesäßbereiche und die nicht bedeckten Beine der sommerlich bekleideten Geschädigten zu sehen. Aus den Aufnahmen ergab sich, dass es dem Fahrgast hierauf im Besonderen ankam. Die Aufzeichnung wurde von Begleitern der Geschädigten bemerkt. Auf deren Aufforderung hin löschte der Fahrgast die Fotos, aber erst auf Aufforderung herbeigerufener Polizist:innen auch aus dem Papierkorb seines Mobiltelefons.

- Auch ein Fahrgast einer Hamburger Buslinie fertigte Fotos einer jungen Frau an, die ihm gegenübersaß und sommerlich gekleidet war. Ihm kam es dabei auf eine Ablichtung ihres Intimbereichs und ihrer Unterwäsche an, die aufgrund eines leicht verrutschten Jeansrocks sichtbar war. Der Vorgang wurde von Mitarbeiter:innen der Hamburger Hochbahn AG beobachtet. Die herbeigerufene Polizei beschlagnahmte das Mobiltelefon.

Da die Staatsanwaltschaft keinen hinreichenden Tatverdacht im Hinblick auf § 184k StGB (Verletzung des Intimbereichs durch Bildaufnahmen) feststellte, wurde der Vorgang an den HmbBfDI abgegeben und von uns eine Geldbuße festgesetzt. Der Bescheid ist aufgrund eines eingelegten Einspruchs noch nicht rechtskräftig.

- Ein Mann, der der Geschädigten lediglich über Instagram bekannt war, bot ihr seine Wohnung zur Übernachtung an. Entgegen vorheriger Absprachen war der Mann dann doch in seiner Wohnung anwesend, während die spätere Geschädigte die Wohnung für mehrere Tage nutzte. Die Geschädigte machte dabei deutlich, dass kein romantisches Interesse ihrerseits bestand. Bevor die Geschädigte am letzten Tag des Aufenthalts das Badezimmer der Wohnung betrat, versteckte der Gastgeber sein Mobiltelefon dort und startete eine Videoaufnahme, um sie im Badezimmer nackt aufnehmen zu können. Die Geschädigte bemerkte das dilettantisch versteckte Mobiltelefon sowie die laufende Aufzeichnung und brachte den Vorfall zur Anzeige.

- Ein Betreuer einer Kirchengemeinde nahm heimlich Fotos weiblicher Mitglieder der Gemeinde auf und wandelte diese mittels Bildbearbeitung in pornographische Bilder um, indem er Köpfe der Personen in pornographische Aufnahmen eingefügte. Geschädigte waren sowohl volljährige Betreuerinnen als auch betreute Jugendliche.

Soweit der HmbBfDI in der Vergangenheit über derartige Fälle berichtet hatte, stellen Fotografen regelmäßig die Frage, ob durch die Festsetzung derartiger Geldbußen die Kunstform der sog. Streetphotography gefährdet wäre. Dabei handelt es sich um ein Genre der Fotografie, das spontane und ungestellte Szenen des öffentlichen Lebens festhält, meist in urbanen Umgebungen. Diese Kunstgattung konzentriert sich auf Menschen, Situationen und Momente, um den Alltag oder besondere Stimmungen einzufangen und visuelle Geschichten zu erzählen.

So wird etwa vorgebracht, dass z.B. Personen im öffentlichen Raum abgelichtet werden könnten, die im Einzelfall nicht mehr als Beiwerk einzuordnen sind (i.S.d. § 23 Abs.1 Nr. 2 KUG), mit der Folge der Rechtswidrigkeit dieser Aufnahmen. Auch in fachspezifischen Blog-Beiträgen wurde in diesem Zusammenhang bereits das Ende der Streetphotography als Kollateralschaden der Regulierungspraxis des HmbBfDI heraufbeschworen. Die Anwendbarkeit der DSGVO auf die private Personenfotografie sei danach fragwürdig und im Übrigen auch nicht erforderlich, da der Schutz der fotografierten Personen durch andere Rechtsvorschriften (zivil- und strafrechtlich) bereits ausreichend gewährleistet sei, so dass die Anwendung der DSGVO zu übermäßiger Bürokratie und unangemessenen Pflichten führe.

Folgte man dieser Auffassung, entstünden massive Rechtsschutzlücken. § 184k StGB wird streng interpretiert, sodass selbst das Fotografieren von Unterwäsche, die durch einen verrutschten Rock sichtbar wird, nicht unter den Straftatbestand fällt. Betroffene müssten sodann auf den Zivilrechtsweg verwiesen werden. Das ist deswegen besonders problematisch, weil die Opfer oft Minderjährige sind. Auch der Löschungsanspruch gem. Art. 17 DSGVO, der in der Regel instinktiv geltend gemacht wird und effektiv durchgesetzt werden kann, wäre nicht anwendbar.

Aus Sicht des HmbBfDI gibt es zudem keine Schwierigkeiten, heimliche Aufnahmen weiblicher Intimbereiche („Creeptography“) von gewöhnlicher Straßenfotografie zu unterscheiden. Eine klare Abgrenzung ist auch für Fotografen ohne juristische Vorkenntnisse möglich. Die Täter haben in aller Regel ein Unrechtsbewusstsein. Soweit überhaupt Versuche der Rechtfertigung unternommen wurden, waren diese fernliegend. Im Ergebnis sind die Einwände gegen die Regulierungspraxis des HmbBfDI daher nicht überzeugend.

7. Auskunft über Kommunikation auf Datingportalen

Wird von der Betreiberin einer Online-Plattform Auskunft über die auf einem bestimmten Account erfolgte Kommunikation verlangt, kann dieser Auskunftsanspruch auf Art. 15 DSGVO gestützt werden. Dieser Anspruch erstreckt sich auch die Eltern in Bezug auf die Kommunikation minderjähriger Kinder.

Den HmbBfDI erreichte im Dezember 2023 eine Beschwerde zu einem Online-Datingportal, das darauf ausgerichtet ist, Beziehungen zwischen älteren Männern und jüngeren Frauen anzubahnen. Eine Minderjährige hatte sich dort ohne Einverständnis ihrer Eltern einen Account angelegt. Nachdem die Eltern hiervon Kenntnis erlangten, hatten sie das Portal zur Sperrung des Accounts sowie zur Auskunft aufgefordert, wobei das Auskunftsersuchen explizit die auf der Plattform erfolgte Kommunikation ihrer Tochter umfasste. Der Sperrungsaufforderung war das Portal nachgekommen, die Auskunft jedoch war nur unzureichend erteilt worden; insbesondere fehlten die Informationen zum Kommunikationsverlauf. Das Portal berief sich u.a. auf vermeintlich schwerer wiegende Datenschutzinteressen Dritter und stellte dabei offensichtlich auf die Personen ab, mit denen sich die Tochter auf der Plattform ausgetauscht hatte.

Das Portal bzw. die Betreiberin des Portals als Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO war aber verpflichtet, den Eltern eine Auskunft gemäß Art. 15 DSGVO zu erteilen, die sich auf die Kommunikation der Tochter erstreckte: Art. 15 Abs. 1 und Abs. 3 DSGVO beziehen sich auf „personenbezogene Daten“ bzw. „personenbezogene Daten, die verarbeitet werden“. Der Umfang des Auskunftsrechts wird daher in erster Linie durch die Reichweite des Begriffs der personenbezogenen Daten bestimmt, der in Art. 4 Abs. 1 DSGVO definiert wird. Dort bezieht sich die Definition auf „alle Informationen über eine bestimmte oder bestimmbare natürliche Person“. Der Europäi-

sche Datenschutzausschuss (EDSA) führt in den von ihm veröffentlichten „Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht (Version 2.1, angenommen am 28. März 2023)“ aus, dass eine unbegrenzte Vielfalt von Daten unter die Definition fallen könne, und zwar neben grundlegenden personenbezogenen Daten wie Name, Anschrift, Telefonnummer u.a. auch medizinische Befunde, Kaufhistorien, Bonitätsindikatoren und eben Kommunikationsinhalte. Die Vorgaben der Leitlinien sind insofern eindeutig. Als Träger der elterlichen Sorge waren die Beschwerdeführer u.a. gemäß §§ 1626 ff. BGB auch berechtigt, ihre Tochter zu vertreten und im Interesse des Kindeswohls ihr Auskunftsrecht wahrzunehmen.

Vor diesem Hintergrund wies der HmbBfDI gemäß Art. 58 Abs. 2 lit. c) DSGVO die Betreiberin des Datingportals an, den Beschwerdeführenden nach Art. 15 DSGVO die begehrte Auskunft über den Account ihrer Tochter einschließlich der Kommunikationsinhalte zu erteilen. Die Betreiberin des Datingportals erteilte den Beschwerdeführenden sodann ordnungsgemäß Auskunft. In Hinblick auf die Angaben zu den Personen, die in Kontakt mit der Minderjährigen gestanden hatten, war die Auskunft nur insoweit zu erteilen, als dies zum Nachvollziehen der Kommunikation erforderlich war. Dass die Namen der Chatpartner von Seiten der Verantwortlichen unkenntlich gemacht worden waren, wurde daher vom HmbBfDI nicht beanstandet.

Weil die Betreiberin des Datingportals den geltend gemachten Auskunftsanspruch gemäß Art. 15 DSGVO erst nach Aufforderung durch den HmbBfDI vollständig erfüllt hatte, sprach der HmbBfDI eine Verwarnung gemäß Art. 58 Abs. 2 lit. b) DSGVO aus. In Abgrenzung zu sonstigen Abhilfebefugnissen des Art. 58 Abs. 2 DSGVO wie beispielsweise der Verhängung eines Bußgeldes kommt eine Verwarnung regelmäßig bei einfachen Verletzungen der DSGVO in Betracht, die zu keiner erheblichen Gefährdung des Datenschutzgrundrechts geführt haben. Dabei ist zu beachten, dass die Verwarnung nicht nur auf die festgestellten Verstöße reagiert, sondern auch auf die Zukunft gerichtet ist, um dem Verantwortlichen die Möglichkeit zu geben, sein Verhalten zu ändern und künftige Verstöße zu vermeiden.

8. Verwarnung eines Betreuers wg. der Versendung einer nicht Ende-zu-Ende-verschlüsselten E-Mail mit hochsensiblen Informationen zur betreuten Person.

Der Schutz sensibler Daten wie Sozial- und Gesundheitsdaten einer betreuten Person macht bei einem Versand als E-Mail regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine genaue Adressatenprüfung erforderlich. Ein Verstoß im Berichtszeitraum führte zur Verwarnung eines gesetzlichen Betreuers.

Den HmbBfDI erreichte ein Hinweis einer Person, die mitteilte, dass Sie von einem Betreuer eine E-Mail mit diversen sensiblen Unterlagen zu einer betreuten Person erhalten hat. Bei Durchsicht der E-Mail stellte sich heraus, dass der Betreuer mit dieser eine Gesundheitseinrichtung ansprach und dabei diverse Dokumente übermittelte, die sich auf die betreute und nun in der Einrichtung behandelte Person bezogen. Dies umfasste eine Kopie eines vorläufigen Personalausweises, den Betreuerausweis, einen Notfallbericht eines Krankenhauses und einen Feststellungsbescheid zu einem Grad der Behinderung. Dem Notfallbericht war eine Diagnose zu einer schweren psychischen Erkrankung der betreuten Person zu entnehmen. Zudem wurden die schwierige aktuelle Situation und die prägende familiäre Geschichte dargelegt. Der Betreuer führte in der E-Mail zudem selbst aus, dass für die betreute Person Grundsicherung beantragt werden soll. Die hinweisgebende Person hatte die E-Mail fälschlicherweise in Kopie erhalten, da der Betreuer eine Ärztin adressieren wollte, die mit der Angelegenheit befasst war und den gleichen Namen trug wie die tatsächliche Empfängerin. Beim Ausfüllen des entsprechenden Feldes war es wegen einer automatisch vorgeschlagenen E-Mail demnach zu einem Fehler in der Empfängerauswahl gekommen.

Verantwortliche haben gem. Art. 32 DSGVO technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit

zu ergreifen. Dabei sind der Stand der Technik und die Implementierungskosten, aber auch die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung bei den organisatorischen Maßnahmen zu berücksichtigen. Auch sind die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen in die Kalkulation einzubeziehen. Es muss ein dem Risiko angemessenes Schutzniveau gewährleistet werden. Die Geeignetheit der Maßnahmen bezieht sich auf das Ziel der Risikovermeidung. Es ist weithin anerkannt, dass bei der Weiterleitung personenbezogener Daten per E-Mail einzig eine Ende-zu-Ende-Verschlüsselung (Internet-Standards S/MIME und OpenPGP) einen durchgreifenden Schutz der Vertraulichkeit der Inhaltsdaten darstellt.

Der E-Mail-Versand von hochsensiblen Informationen betreuter Personen, die etwa Behandlungsberichte, Ausweisunterlagen und Feststellungsbescheide nach dem Behindertenrecht umfassen, verlangt einen hohen Schutzstandard. Werden solche Daten verarbeitet, ist von einem hohen Risiko für die Rechte und Freiheiten der betroffenen Person auszugehen, denn es sind kaum Daten denkbar, die in ihrer Gesamtheit einen sensibleren Inhalt darstellen. Bereits dem Betreuerausweis lässt sich entnehmen, dass die aufgeführte Person ihre Angelegenheiten ganz oder teilweise rechtlich nicht mehr besorgen kann und daher in ihrer Lebensweise eingeschränkt ist. Werden dann noch Gesundheitsdaten wie Behandlungsberichte hinzugefügt, wird für potenziell zugreifende Personen ein umfassendes Bild der betroffenen Person einsehbar.

Die Schwere des Risikos für die Rechte und Freiheiten der betreuten Person waren daher enorm. Es sind zahlreiche Informationen übermittelt worden, die einem sehr hohen Diskriminierungsrisiko unterliegen. Erschwerend kam hinzu, dass die Informationen einwandfrei einer konkreten Person zugerechnet werden konnten, da sogar ein Ausweisdokument mit Foto übermittelt wurde. Der Betreuer hätte bei der Übermittlung also eine Ende-zu-Ende-Verschlüsselung durchführen müssen, um den hohen Schutzstandard der äußerst sensiblen

personenbezogenen Daten gewährleisten zu können. Als Versender der E-Mail trägt der Betreuer die datenschutzrechtliche Verantwortung für eine sichere technische Gestaltung, so dass auch der Vortrag, dass die empfangende Gesundheitseinrichtung die Daten per E-Mail angefordert und technisch den Empfang Ende-zu-Ende-verschlüsselter E-Mail nicht unterstützt hat, nicht greift. Der Betreuer kann diesen Aspekt lediglich bei der Auswahl der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO berücksichtigen. Umstände dafür, dass die Situation so dringlich war, dass sofort eine Übermittlung sämtlicher Unterlagen in technisch niedrigschwelliger Weise erfolgen musste, um die entscheidenden Informationen an die Gesundheitseinrichtung zu übermitteln, waren nicht ersichtlich gewesen.

Was die Auswahl des falschen Adressaten betraf, hatte der Betreuer angekündigt, vor der Versendung von E-Mails künftig in einem separaten Schritt zu prüfen, ob die richtigen Empfänger ausgewählt wurden. Damit zeigte der Betreuer einerseits, dass er zuvor einen solchen Schritt nicht vorgenommen hatte. Zum anderen handelt es sich dabei um ein Standardvorgehen, das bei dem Versand jeder E-Mail mit personenbezogenen Daten vorzunehmen ist und nicht um eine organisatorische Maßnahme, die für sich genommen das erhebliche Risiko bei der Versendung von Daten der betreuten Person ausgleichen kann. Eine angemessenere Maßnahme wäre in Anbetracht der Umstände etwa die zusätzliche Anwendung des Vieraugenprinzips, bei dem die Prüfung der Empfängeradressen durch – wenn vorhanden – zwei Personen der verantwortlichen Stelle vorgenommen wird, bevor eine Absendung erfolgt. Wenn bei Betreuenden keine zugriffsberechtigten Mitarbeiter:innen vorhanden sind, muss jedenfalls eine gründliche Prüfung der Empfänger durch die betreuende Person erfolgen.

9. Gerichtsverfahren NOYB wegen Pur-Abo-Modellen

Der HmbBfDI wurde von der Organisation NOYB – Europäisches Zentrum für digitale Rechte – vor dem Verwaltungsgericht Hamburg im Zusammenhang mit den Pur-Abo-Modellen Hamburger Medienunternehmen verklagt. NOYB kritisiert dabei u.a. eine vermeintlich unzulässige Rechtsberatung des HmbBfDI im Rahmen des Beschwerdeverfahrens.

Hintergrund waren mehrere Beschwerdeverfahren von NOYB gegen europäische Medienhäuser wegen sogenannter Pur-Abo-Modelle, die 2023 zu einem DSK Beschluss und vor allem zu Verbesserungen in der Ausgestaltung der Modelle führten (siehe dazu Tätigkeitsbericht 2023, Kapitel III 16 und auch ergänzend im vorliegenden Tätigkeitsbericht das Kapitel VI 2 zu „Pay or OK" Modellen großer Plattformen im europäischen Kontext).

In dem Klagverfahren bezweifelt NOYB u.a., dass Aufsichtsbehörden rechtliche Beratungen verantwortlicher Stellen durchführen dürften. Dies ist zum einen generell nicht richtig, da die Beratung sowohl gesetzlich verankert (vgl. § 40 Abs. 6 BDSG; Art. 58 Abs. 3 DSGVO) als auch eine wichtige und von verantwortlichen Stellen nachgefragte Praxis ist.

Zum anderen ging es aber in den konkreten Beschwerdeverfahren nicht um unverbindliche Beratung, sondern vor allem darum, gegenüber den Verantwortlichen auf eine richtige Umsetzung des DSK-Beschlusses bei der Ausgestaltung der Pur-Abo-Modelle hinzuwirken.

In dem Verfahren werden auch weitere förmliche Aspekte des Beschwerdeverfahrens wie bspw. Anhörungserfordernisse zu klären sein, wobei sich hinter den verwaltungsrechtlichen Fragestellungen Unterschiede in der rechtspolitischen und ökonomischen Bewertung der realen Sachlage sowie auch der Rechtsprechung des EuGH ver-

bergen. Im Ergebnis bleibt abzuwarten, wie weitgehend das Verwaltungsgericht in das Themenfeld einsteigt. Der HmbBfDI wird dazu weiter berichten und natürlich weiter die Unternehmen vor Ort beraten.

GRENZÜBERSCHREITENDE THEMEN VI.

GRENZÜBERSCHREITENDE THEMEN

1. Die High Level Group DMA der EU-Kommission und ihre sub-groups

Der Digital Markets Act (DMA) zielt darauf ab, faire Wettbewerbsbedingungen im digitalen Raum zu schaffen und Innovationen zu fördern. Die Mitgliedschaft des HmbBfDI in der High Level Group der EU-Kommission und ihren sub-groups bietet eine wertvolle Gelegenheit, aktiv an der Gestaltung der digitalen Zukunft Europas teilzunehmen.

Das Gesetz über digitale Märkte (DMA) regelt die Wettbewerbsbedingungen, den Verbraucherschutz und nicht zuletzt die Förderung von Innovationen im digitalen Sektor. Der intersektorale Regelungsgehalt des DMA erfordert, dass sich die unterschiedlichen Regulierungsregime und -behörden enger verzahnen. Eine zentrale Rolle nimmt dabei die EU-Kommission ein, die als zuständige Stelle die sogenannten Torwächter nach DMA benennt, überwacht und – wenn nötig – sanktioniert.

Art. 40 DMA sieht die Einrichtung der sogenannten „Hochrangigen Gruppe“ (High Level Group DMA, kurz HLG) vor. Diese hat die EU-Kommission im März 2023 einberufen, um die Rahmenbedingungen für den digitalen Markt in Europa zu verbessern und den Austausch zwischen den europäischen Gremien und Netzwerken für eine kohärente und komplementäre Umsetzung des DMA sowie anderer relevanter sektoraler Vorschriften zu gewährleisten. Die eingesetzte HLG setzt sich aus 30 Vertretern zusammen, die vom Gremium der europäischen Regulierungsbehörden für elektronische Kommunikation (GEREK), dem Europäischen Datenschutzbeauftragten (EDSB) und dem Europäischen Datenschutzausschuss (EDSA), dem Europäischen Wettbewerbsnetz (ECN), dem Netz für die Zusammenarbeit im Verbraucherschutz (CPC-Netz) und der Europäischen Regulierungsgruppe der Regulierungsbehörden für audiovisuelle Medien (ERGA) benannt wurden.

Als Vertreter des EDSA ist der HmbBfDI gleich auf mehreren Ebenen der HLG aktiv. Als Mitglied der HLG sowie ihrer Untergruppen berät er in seiner Vertretungsfunktion für den EDSA die EU-Kommission bei der Umsetzung des DMA. Die Untergruppen der HLG bilden spezifische Arbeitsgruppen, die sich mit einzelnen Aspekten der Umsetzung und Überwachung des DMA befassen, so z.B. mit den Betroffenenrechten nach Art. 5 und 6 DMA („Digital Markets Act Data related Obligations Sub-Group") oder auch mit Blick auf Vorschriften betreffend die künstliche Intelligenz („Artificial Intelligence Sub-Group"). In beiden Untergruppen ist der HmbBfDI für die EU-Kommission beratend tätig. Eine weitere Untergruppe der HLG ist die "Article 7 Digital Markets Act Sub-Group", die sich vor allem mit technischen Aspekten der Interoperabilität beschäftigt und von anderen europäischen Datenschutzbehörden vertretend für den EDSA begleitet wird.

Die ersten Erfahrungen in der sektoralen Zusammenarbeit konnten im Rahmen des Verfahrens des Bundeskartellamts (BKartA) bezüglich Meta (Az. B6-22-16) gesammelt werden. Die HmbBfDI hat dieses Verfahren seit seiner Eröffnung im Jahr 2016 als nationale Datenschutzaufsichtsbehörde beratend begleitet. Das Verfahren hatte Auswirkungen auf mehrere Aufsichtssektoren. Auf Antrag des HmbBfDI, gemeinsam mit zwei weiteren europäischen Datenschutzbehörden, hatte der EDSA in seiner Stellungnahme 08/2024 die Frage der „Wirksamkeit von Einwilligungen im Kontext von „Consent or Pay"-Modellen großer Online-Plattformen" behandelt. Dabei wurde die relevante Rechtsprechung des EuGH (Az. C-252/21) zum Verfahren des Bundeskartellamts aus datenschutzrechtlicher Perspektive aufgegriffen, wobei auch bestimmte Aspekte des DMA berücksichtigt wurden. Im Juli 2024 stellte die EU-Kommission vorläufig fest, dass Meta mit seinem Bezahlmodell aufgrund mangelnder Einwilligungsmöglichkeiten gegen Art. 5 Abs. 2 DMA verstößt. Das inzwischen abgeschlossene Verfahren des BKartA hat nicht nur eine Vielzahl von datenschutzrechtlichen Fragen aufgeworfen, sondern ist auch ein gelungenes Beispiel dafür, wie die vom EuGH in C-252/21 geforderte „loyale Zusammenarbeit" in der sektoralen Aufsicht ge-

staltet werden kann, um eine kohärente Anwendung verschiedener sektoraler Vorschriften sicherzustellen.

Zudem ist der HmbBfDI in der „Artificial Intelligence Sub-Group to the High-Level Group for the Digital Markets Act" aktiv. Im Rahmen dieser Untergruppe verfolgt die HLG die Entwicklungen in diesem innovativen, aber auch kritischen Bereich und untersucht die Wechselwirkungen zwischen dem DMA und anderen Regulierungsinstrumenten. Zugleich soll auch in dieser Untergruppe der Austausch von Erfahrungen mit der Rechtsdurchsetzung und von Fachwissen im Bereich der Regulierung fortgesetzt werden, die nach DMA in Bezug auf KI relevant sein können. Eine weitere Aufgabe der Untergruppe ist es, Methoden zu entwickeln, um eine wirksame Zusammenarbeit zu gewährleisten, die zu einem kohärenten Regulierungsansatz im Rahmen des DMA und anderer Rechtsinstrumente führt. Im Zuge des ersten konstituierenden Treffens dieser Untergruppe im Oktober 2024 präsentierten die nach DMA benannten Torwächter ihre KI-Strategien. Zudem stellte sich das AI Office der EU-Kommission vor, das anlässlich des Inkrafttretens des AI Acts einberufen wurde. Auch hier sind die sektorale Zusammenarbeit und ein enger Austausch entscheidend für eine kohärente und erfolgreiche Aufsichtspraxis in verschiedenen Bereichen.

Die Teilnahme an der HLG zum DMA sowie ihren Untergruppen ist insgesamt eine bedeutende Chance, die Verzahnung der Regelungen des EU Digitalen Dienste Pakets besser zu verstehen und die digitale Landschaft Europas aktiv mitzugestalten.

2. Stellungnahme des EDSA zu „Consent or Pay“

Die Entscheidung des EuGH im Fall Bundeskartellamt sowie die Einführung eines „Consent or pay“ Modells durch Meta erforderten eine Klärung der Wirksamkeit von Einwilligungen für Abo-Modelle von großen Plattformen. Gemeinsam mit Kolleg:innen aus Norwegen und den Niederlanden hat der HmbBfDI den Europäischen Datenschutzausschuss um eine Stellungnahme zur Gültigkeit der Einwilligung zur Verarbeitung personenbezogener Daten für verhaltensbezogene Werbung im Rahmen von solchen digitalen Abo-Modellen ersucht.

„Consent or Pay“ ist ein Geschäftsmodell, bei dem Unternehmen den Nutzern die Wahl bieten, entweder kostenlos auf Online-Dienste zuzugreifen, sofern sie in die Nutzung ihrer persönlichen Daten für personalisierte Werbung einwilligen, oder eine Gebühr zu zahlen, wenn sie diese Zustimmung verweigern. Im deutschsprachigen Raum hat sich dafür der Begriff des Pur-Abo-Modells etabliert

Im März 2023 hat die Datenschutzkonferenz (DSK) einen Beschluss gefasst, der die Zulässigkeit von Pur-Abo-Modellen unter bestimmten Bedingungen feststellt. Dazu gehört, dass die kostenpflichtige, einwilligungsfreie Leistung eine im Wesentlichen gleichwertige Alternative zur kostenlosen, einwilligungsbedürftigen Leistung darstellen muss und der Preis marktüblich ist. Zudem muss eine wirksame Einwilligung den Anforderungen der DSGVO entsprechen, insbesondere den in Artikel 4 Nr. 11 und Artikel 7 genannten Voraussetzungen.

Im Juli 2023 eröffnete der Europäische Gerichtshof (EuGH) im Rahmen eines Vorlageverfahrens grundsätzlich die Möglichkeit, dass auch große Anbieter von Social-Media-Diensten ein Abo-Modell als Alternative zur Einwilligung für die Verarbeitung personenbezogener Daten zum Zweck der personalisierten Werbung in Betracht ziehen können, wenn der Preis angemessen ist. Der EuGH erläuterte jedoch nicht im Detail, unter welchen Bedingungen dies rechtmäßig wäre.

Auch auf der Grundlage dieses Urteils und vor dem Hintergrund eines Verfahrens der Kommission im Zusammenhang mit dem DMA führte Meta ein Bezahlmodell mit Abofunktion ein.

Nach Einführung durch Meta bei seinen sozialen Netzwerken Facebook und Instagram hat der HmbBfDI gemeinsam mit Kolleg:innen aus Norwegen und den Niederlanden den Europäischen Datenschutzausschuss (EDSA) um eine Stellungnahme ersucht. Ziel war es, Anbietern auf dem europäischen Markt mehr Orientierung zu geben, gemeinsame Standards unter den Aufsichtsbehörden zu etablieren und relevante Fragen der Nutzenden zu klären.

Im April 2024 nahm der EDSA umfassend Stellung, wobei er ausschließlich auf Dienste großer Online-Plattformen (large online platforms) abhob. Die wichtigsten Punkte aus der Stellungnahme des EDSA sind:

- „Consent or Pay"-Modelle genügten bei den betrachteten Plattformen bzw. Diensten im Allgemeinen nicht den Anforderungen an eine wirksame Zustimmung nach der DSGVO.
- Denn eine Zustimmung könne nicht als freiwillig angesehen werden, wenn Nutzer:innen Nachteile erleiden, weil sie entweder keine Zustimmung erteilen oder diese widerrufen. Nachteile können aus Sicht des EDSA auch entstehen, wenn Nutzer:innen von wichtigen Online-Diensten ausgeschlossen werden, weil sie sich entscheiden, weder zu zahlen noch ihre Zustimmung zur Datenverarbeitung zu geben, ohne dass ihnen eine äquivalente Alternative angeboten wird.
- In Anlehnung an den Digital Markets Act empfiehlt der EDSA, dass Anbieter von großen Online-Plattformen eine dritte, zahlungsfreie Variante (sog. dritte Option) entwickeln, die es Nutzern ermöglicht, ohne Einwilligung in die Verarbeitung personenbezogener Daten für verhaltensbasierte Werbung den Dienst weiterhin zu nutzen.

Der EDSA legte zudem einige Voraussetzungen fest, um sicherzustellen, dass eine zahlungspflichtige Alternative tatsächlich äquivalent zur einwilligungsbasierten ist. Hierzu zählt der Verzicht auf solche Verarbeitungsoperationen, die für die Bereitstellung des Dienstes nicht erforderlich sind und normalerweise auf Zustimmung basieren.

Bezogen auf das konkrete Bezahlmodell von Meta stellte die EU-Kommission im Juli 2024 vorläufig fest, dass Meta wegen unzureichender Einwilligungsmöglichkeiten gegen Art. 5 Abs. 2 DMA, der auf die Anforderungen der DSGVO verweist, verstößt. Eine endgültige Feststellung durch die EU-Kommission wird bis März 2025 erwartet, die auch eine mittlerweile von Meta eingeführte dritte Option bewerten wird.

Insgesamt ist festzuhalten, dass das EDSA-Papier sich argumentativ auf die großen, gatekeeper-artigen internationalen Plattformen bezieht. Eine Übertragung dieses Ansatzes auf kleinere nationale oder regionale Angebote erscheint wenig sinnvoll, da hier Ausweichmöglichkeiten bestehen. Der o.g. DSK-Beschluss bleibt daher von der EDSA-Entscheidung unberührt.

Ergänzend zu der Stellungnahme des EDSA sind nun Leitlinien in Vorbereitung, die das Thema „Consent or Pay“ für alle Anbieter aufbereiten sollen. Diese Leitlinien werden im Laufe des Jahres 2025 erwartet.

3. Registerinformationen im Internet

Wer eine Vertretungsfunktion in einer Handelsgesellschaft ausübt und seinen Namen in eine Internetsuchmaschine eingibt, erhält häufig Suchergebnisse, die den Bezug zu dem Unternehmen anzeigen. Die Veröffentlichung von personenbezogenen Handelsregisterdaten aus mehreren Mitgliedstaaten im Internet durch ein Unternehmen aus Hamburg hat im Berichtszeitraum zum Austausch des HmbBfDI mit anderen europäischen Aufsichtsbehörden geführt. Wenn Daten von Bürger:innen aus anderen Mitgliedstaaten durch in Hamburg ansässige Unternehmen verarbeitet werden, hat der HmbBfDI die dortigen Aufsichtsbehörden in seinen Entscheidungsprozess einzubeziehen.

Handelsregisterinformationen stellen hochwertige Datensätze dar: Informationen, die mit wichtigen Vorteilen für Wirtschaft und Gesellschaft verbunden sind. Die PSI und Open Data Richtlinie (EU) 2019/1024 sieht vor, dass staatliche Stellen deren digitale Weiterverwendung erleichtern, um Unternehmen bei der Entwicklung neuer Dienstleistungen und Produkte zu unterstützen. Der HmbBfDI hat zu kontrollieren, ob die kommerzielle Weiterverwendung von im Handelsregister enthaltenen personenbezogenen Daten mit datenschutzrechtlichen Anforderungen in Einklang steht.

Eine Vielzahl der Mitgliedstaaten hat die PSI und Open Data Richtlinie bereits umgesetzt. Nationale Register bieten häufig z.B. eine Anwendungsprogrammierschnittstelle (API) für die Übertragung der Registerdaten an die weiterverarbeitenden Unternehmen an. Die durch eine Weiterverarbeitung ermöglichte erhöhte Transparenz steht dabei häufig in Kontrast zu früheren datenschutzrechtlichen Vorgaben der Registergesetzgeber, eine Indexierung durch Suchmaschinen und eine Personensuche in den Registern zu vermeiden.

Das in Hamburg ansässige Unternehmen veröffentlicht Registerdaten z.B. aus Handels- und Vereinsregistern auch mit Personenbezug auf seinen Internetseiten und erstellt Übersichten zu personellen Verflechtungen. Diese werden von Suchmaschinen wie Google indexiert, so dass die Informationen bei namensbezogener Suchmaschinenrecherche angezeigt werden. Dies stellt einen intensiveren Grundrechtseingriff dar als bei der bloßen Abrufbarkeit der Daten bei einer Suche nach einer Firma im Handelsregister und der Anzeige von Personennamen lediglich in den dort nur einzeln abrufbaren Dokumenten.

Die Aufsichtsbehörden anderer Mitgliedstaaten (Spanien, Frankreich) haben sich vor diesem Hintergrund im Berichtszeitraum im Rahmen informeller Konsultationen (Art. 61 Abs. 1 DSGVO) gegenüber dem HmbBfDI in Einzelfällen kritisch zu dessen Beurteilung geäußert, dass die Veröffentlichung von personenbezogenen Registerdaten auf den Internetseiten des Unternehmens aus Hamburg zulässig sei. Dienste wie der des in Hamburg ansässigen Unternehmens sind in vielen anderen Mitgliedstaaten nicht bekannt. Gleichwohl haben Behörden anderer Mitgliedstaaten gegen die bisherigen Entscheidungsentwürfe des HmbBfDI in Fällen mit Auslandsbezug noch in keinem Fall Einspruch (Art. 60 Abs. 4 DSGVO) eingelegt.

Dies dürfte auch an den von dem Unternehmen eingerichteten und im Berichtszeitraum in Abstimmung mit dem HmbBfDI erweiterten Beschränkungen bei der Veröffentlichung personenbezogener Registerdaten liegen. Letztere gehen unter anderem auf die im Jahr 2024 zu Registerdaten ergangenen höchstrichterlichen Entscheidungen zurück.

Der BGH (II ZB 7/23) hat 2024 als Begründung für die Zulässigkeit einer zeitlich unbegrenzten Abrufbarkeit von personenbezogenen Daten eines früheren GmbH-Geschäftsführers im Online-Handelsregister darauf abgestellt, dass eine gezielte Personensuche dort nicht möglich ist. Mit Bezug auf das Online-Vereinsregister hat der BGH dagegen geurteilt, dass nach Ablauf von 20 Jahren seit dem

Ausscheiden einer Person aus dem Vereinsvorstand deren personenbezogene Daten online nur für Personen offengelegt werden dürfen, die zuvor ein berechtigtes Interesse an dem Abruf dargelegt haben (II ZB 10/23).

Die zeitlich unbeschränkte Veröffentlichung aller Personendaten aus den Registern auf suchmaschinenindexierten Internetseiten hält der HmbBfDI datenschutzrechtlich nicht für zulässig. Das seiner Aufsicht unterliegende Unternehmen veröffentlicht auch nicht sämtliche personenbezogenen Registerdaten zeitlich unbeschränkt. Vielmehr werden nur Angaben zu Vertretungspersonen abgebildet (nicht etwa auch Angaben zu Gesellschaftern oder wirtschaftlichen Eigentümern). Kleinunternehmen wie in Deutschland e.K., GbR und OHG werden ohne Angabe der konkreten Adresse angezeigt. Denn diese ist häufig auch die private Wohnadresse einer Vertretungsperson.

Zudem hat das Unternehmen Sperrfristen eingerichtet bzw. verkürzt: Nach Ausscheiden der gesetzlichen Vertretungsperson aus dem Unternehmen werden die Daten nicht zeitlich unbegrenzt angezeigt, sondern nach Ablauf von zehn, bei kleinen Unternehmen nach Ablauf von fünf Jahren gesperrt. Nach zehn Jahren werden auch die personenbezogenen Daten von Vereinsvorständen in den Übersichten zum Vereinsregister nicht mehr angezeigt. Auf diese Weise wird nach Auffassung des HmbBfDI ein angemessener Ausgleich zwischen dem öffentlichen Informationsinteresse und den Grundrechten der betroffenen Personen geschaffen.

Auch sind weitergehende Löschpflichten im Einzelfall denkbar. Hierzu hat der EuGH (C-200/23) 2024 entschieden, dass ein Löschungsanspruch nach Art. 17 DSGVO besteht mit Bezug auf personenbezogene Angaben in zum Handelsregister eingereichten und im Internet veröffentlichten Dokumenten, die nicht der Veröffentlichungspflicht unterliegen (wie etwa Unterschriften in Dokumenten, Ausweisnummern o.ä.). Dementsprechend wäre es wünschenswert, wenn für das deutsche Online-Handelsregister die Möglichkeit genutzt werden könnte, Dokumente auszutauschen, die Angaben enthalten, die über

die Pflichtangaben hinausgehen. Das frühere Dokument sollte aus datenschutzrechtlicher Sicht dann jedenfalls in der Online-Veröffentlichung nicht mehr abrufbar gemacht werden und damit auch nicht durch Dritte weiterverwendet werden können.

Der HmbBfDI begrüßt die Bereitschaft des seiner Aufsicht unterliegenden Unternehmens, aktuelle Entwicklungen in der Rechtsprechung zu berücksichtigen und die zeitnahe Vornahme von Anpassungen bei Umfang und Dauer der Veröffentlichung personenbezogener Daten. Hierdurch werden die Grundrechte von Unternehmens- und Vereinsvertretern (z.B. Geschäftsführern und Vorstandspersonen) stärker geschützt. Dazu, ob andere europäische Aufsichtsbehörden weitergehende Beschränkungen für geboten halten, steht der HmbBfDI mit diesen in engem Austausch.

4. Ermessen der Datenschutzbehörden – Vorgaben des EuGH

Der Europäische Gerichtshof hat Grundsätze für die Arbeitsweise der Datenschutzbehörden aufgestellt. In einem wegweisenden Urteil hat er konkretisiert, nach welchen Kriterien sie zu entscheiden haben, ob sie förmliche Maßnahmen wie Anordnungen, Geldbußen und Verwarnungen ergreifen. Es ermutigt datenverarbeitende Stellen zur lösungsorientierten Zusammenarbeit mit der Aufsicht.

In der Entscheidung C-768/21 vom 25.9.2024 hat sich der Europäische Gerichtshof (EuGH) mit einem Fall im Bankensektor befasst. Eine Sparkassenmitarbeiterin hatte darin mehrfach unberechtigt auf Kontodaten eines konkreten Kunden zugegriffen. Ihr Arbeitgeber reagierte darauf mit Disziplinarmaßnahmen. Zudem ließ er sich schriftlich versichern, dass die abgerufenen Daten weder kopiert noch weitergeleitet worden waren und dies auch in Zukunft nicht passieren werde. Die anschließend durch den Betroffenen eingeschaltete hessische Datenschutzbehörde trat in einen Dialog mit

der Sparkasse ein. Darin einigten sich beide Seiten auf verschiedene zukunftsgerichtete Maßnahmen wie z.B. die ausgeweitete Speicherung der Zugriffsprotokollierung. Der EuGH bestätigte schlussendlich, dass es richtig war, dass in dem Fall kein förmlicher Bescheid erlassen wurde, sondern der Beschwerdefall mit der Einigung auf technische Verbesserungen abgeschlossen wurde.

In seiner Entscheidung stellt der Gerichtshof ein Regel-Ausnahme-Verhältnis für die Behandlung von Datenschutzbeschwerden auf. Zunächst wiederholt er seinen im Vorjahr bereits betonten Grundsatz (Urt. v. 7.12.2023 – E-26/22 u. C-64/22), dass eine Datenschutzbehörde festgestellte Verstöße in der Regel mit einer Abhilfemaßnahme aus Art. 58 Abs. 2 DSGVO zu beantworten hat. Neu ist im aktuellen Urteil die Auseinandersetzung mit den Konstellationen, in denen von diesem Grundsatz abgewichen werden kann. Der EuGH betont, dass „ausnahmsweise" eine förmliche Maßnahme entbehrlich ist, wenn z.B. die Verletzung nicht dauerhaft besteht und die verantwortliche Stelle proaktiv Gegenmaßnahmen ergriffen hat, um den aktuellen Verstoß abzustellen bzw. eine Wiederholung zu vermeiden. Die Aufzählung der Kriterien ist nicht abschließend formuliert, sodass auch in anderen, vergleichbaren Konstellationen von förmlichen Maßnahmen abgesehen werden kann. Es ist den Aussagen des EuGH zufolge stets die Verhältnismäßigkeit im Einzelfall zu prüfen, wofür die oben genannten Kriterien eine Richtschnur bilden.

Die Ausführungen im Urteil zeigen, dass es dem EuGH im Kern darauf ankommt, dass Verstöße abgestellt werden und sich in Zukunft nicht wiederholen. Diese Zielrichtung hat das Vorgehen der Aufsichtsbehörden zu lenken. Wie es konkret erreicht wird, ob durch förmlichen Verwaltungsakt oder auf anderem Wege, ist nachrangig. Die Beurteilung, wann dieser Weg im konkreten Fall zielführend ist, bleibt im gerichtlich überprüfbaren Ermessen der Aufsichtsbehörden.

Die Linie des EuGH bestätigt die langjährige Praxis des HmbBfDI. Beschwerdefälle, in denen er einen Datenschutzverstoß ermittelt,

wurden bereits in der Vergangenheit regelhaft mit einer Maßnahme nach Art. 58 DSGVO beendet, indem mindestens ein Gebührenbescheid erlassen wird. Art. 58 Abs. 6 Satz 1 DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, den Maßnahmenkatalog des Abs. 2 durch zusätzliche Befugnisse zu ergänzen. Der Hamburgische Gesetzgeber hat davon Gebrauch gemacht mittels § 25 HmbDSG in Verbindung mit der Gebührenordnung für die datenschutzrechtliche Kontrolle im nichtöffentlichen Bereich (Datenschutzgebührenordnung – DSGebO). Danach hat die Verantwortliche Stelle den Verwaltungsaufwand des HmbBfDI zu ersetzen, wenn die Untersuchung einen Mangel aufgezeigt hat. Die Gebühr beträgt ab dem Jahr 2025 mindestens 232 Euro und erreicht nicht selten einen deutlich vierstelligen Bereich. Nur in seltenen Fällen einer groben Unbilligkeit wird trotz des Verstoßes von einer Verwaltungsgebühr abgesehen. Da der die Summe festsetzende Verwaltungsakt an das Bestehen eines datenschutzrechtlichen Mangels geknüpft ist, handelt es sich um eine mitgliedstaatlich vorgesehene Abhilfemaßnahme im Sinne des Art. 58 Abs. 2, Abs. 6 DSGVO.

Darüber hinaus wird auch die Praxis des HmbBfDI bei der Entscheidung über Warnungen, Verwarnungen, Anordnungen und Geldbußen vom EuGH bestätigt. Hier besteht das generelle Vorgehen der Behörde darin, einen Fall in der Regel nicht zu schließen, bevor nicht der datenschutzrechtliche Mangel beseitigt wurde bzw. die Position der beschwerdeführenden Person verbessert wurde. Das Anliegen der Menschen, die sich an den HmbBfDI gewandt haben, steht im Mittelpunkt seines Handelns. Es geht darum, Einzelpersonen wirksam zu helfen, die in ihren Rechten verletzt sind. Die Referent:innen entscheiden dabei jeweils anhand der Umstände des Einzelfalls, auf welchem Weg dieses Ziel effektiv erreicht werden kann. Die formlose Kontaktaufnahme mit der Aufforderung zur Stellungnahme und ggf. Beseitigung des Verstoßes ist dabei schon aus Verhältnismäßigkeitsgründen zumeist der erste Schritt. Ein Großteil der Beschwerdefälle, in denen tatsächlich ein Verstoß vorliegt, kann bereits durch diesen Dialog zu einem positiven Ausgang geführt werden.

Die Entscheidung des EuGH kann als Einladung an datenverarbeitende Stellen zum konstruktiven Dialog mit der Aufsicht verstanden werden. Auch diesen ist zu raten, das Anliegen der beschwerdeführenden Personen als Leitbild ihrer Datenschutzcompliance zu sehen. Im Einklang mit dem Urteil berücksichtigt der HmbBfDI bei einer Kontrolle proaktiv ergriffene Maßnahmen zur Schadensminderung positiv. In komplexeren Fällen steht auch der lösungsorientierte Austausch zwischen datenverarbeitender Stelle und dem HmbBfDI mit der EuGH-Entscheidung im Einklang. Es ist nicht nur oftmals sinnvoll und zielführend, wenn die Aufsichtsbehörde auf den Verantwortlichen zugeht und ihm erklärt, wie er seine Verarbeitungen in Einklang mit der DSGVO bringen kann. Auch die gemeinsame Entwicklung von Lösungsansätzen kann in anspruchsvollen Konstellationen mit neuartigen Technologien eine gewinnbringende Herangehensweise sein. Entscheidend ist, dass die Datenschutzbehörde damit eine Beendigung des Verstoßes erreicht.

Von gewichtiger Bedeutung für das Ermessen des HmbBfDI in Beschwerdefällen ist damit auch das Nachtatverhalten. Verfahren können in der Regel schnell beendet werden, wenn die kontrollierten Stellen dem HmbBfDI proaktiv Maßnahmen anbieten, mit denen den beschwerdeführenden Personen tatsächlich geholfen wird und sich die Situation der Betroffenen auch für die Zukunft verbessert. Vor und während des Verfahrens ist es empfehlenswert, konkrete Handlungen zu ergreifen. Die aktive Mitwirkung kann sich nach den Maßstäben des EuGH dann besonders auszahlen. Dies bedeutet jedoch nicht, dass Unternehmen erst nach Aufforderung durch die Aufsichtsbehörde aktiv werden müssten. Das Urteil ist kein Freifahrtschein, rechtswidrige Zustände solange aufrecht zu halten, bis der HmbBfDI sie bemerkt und erst dann kooperativ abzustellen. Der EuGH hat im konkreten Vorlagefall besonders hoch gewichtet, dass die Sparkasse bereits im Vorfeld zur Behördenkontrolle Maßnahmen ergriffen hatte. Nach den Vorgaben des Gerichtshofs wird der HmbBfDI stets anhand der Umstände des Einzelfalls entscheiden, ob von einer Sanktion abgesehen werden kann.

5. Der Data Act – Herausforderung für Unternehmen, neue Aufgabe für die Datenschutzaufsicht

Der europäische Data Act verpflichtet Unternehmen ab September 2025, bestimmte Daten mit Antragstellern zu teilen. Im Fokus stehen zwar nichtpersonenbezogene Daten aus vernetzten Geräten und Maschinen. Teilweise sind jedoch auch personenbezogene Daten mit umfasst. In diesem Fall beaufsichtigen die Datenschutzbehörden die Durchsetzung des Data Act.

Der Data Act ist ein wesentlicher Baustein der europäischen Datenstrategie. Sein Ziel ist die bessere Nutzbarmachung von Daten, die bislang exklusiv in einzelnen Unternehmen vor allem des Industriebereichs vorgehalten werden. Der Austausch und die Nutzung von Unternehmensdaten soll die Wertschöpfung in der europäischen Wirtschaft verbessern und Synergieeffekte bilden. Zugleich sollen die Nutzenden von einem Mehr an Transparenz und Datenzugang profitieren. Nutzer:innen können sowohl Verbraucher als auch Unternehmen sein. Diejenigen, die vernetzte Geräte und Produkte verwenden, sollen darüber entscheiden können, wer von den dabei erzeugten Daten profitiert. Der Data Act soll sie in die Lage versetzen, diese Daten selbst auszuwerten oder auch an Dritte weiterzugeben. Die Rechtspflichten zielen vor allem auf Hersteller und Dateninhaber vernetzter Geräte ab. Dazu können zum einen Maschinen in der Industrie oder Fahrzeuge im Fuhrpark oder Privatbestand zählen. Zum anderen sind auch internetfähige Haushaltsgeräte wie Fernseher, Kühlschränke oder Blutdruckmessgeräte umfasst.

Ab dem 12. September 2025 ist die europäische Verordnung unmittelbar anwendbar und u.a. durch Hamburger Unternehmen umzusetzen. Zunächst haben diese sich einen Überblick zu verschaffen über die in ihrem Bereich erzeugten Daten. Eine gute Datenschutzorganisation kann dafür ein sinnvoller Startpunkt sein, jedoch ist sie nur der Anfang. Die Bestandsaufnahme anlässlich des Data Act muss auf

nichtpersonenbezogene Daten ausgeweitet werden. Um den künftigen Datenzugang zu ermöglichen, sind gegebenenfalls auch die Produkte und IT-Prozesse umzugestalten. Eine besondere, praxisrelevante Rechtspflicht betrifft das sogenannte Cloud-Switching. Anbieter von Onlinespeicherplatz haben Vorkehrungen für einen unkomplizierten Wechsel hin zu anderen Dienstleistern zu treffen.

Die Aufsichtszuständigkeit für die Umsetzung des Data Act ist zweigeteilt. Hinsichtlich der Pflichten in Bezug auf nichtpersonenbezogene Daten wird die Aufgabe einer durch Bundesgesetz zu bestimmenden Behörde zufallen. Diese in der Praxis wichtigste Zuständigkeit wird voraussichtlich der Bundesnetzagentur zugewiesen. Die Auswahl erscheint wahrscheinlich, weil der Entwurf des Umsetzungsgesetzes zum Data Governance Act, eines Parallelrechtsakts zum Data Act, die Bundesnetzagentur als Aufsichtsstelle vorsieht. Einen Teilbereich der Aufsicht werden jedoch die Datenschutzbehörden zu übernehmen haben. Art. 37 Abs. 3 bestimmt sie als zuständig für die Überwachung der Anwendung des Data Act in Bezug auf den Schutz personenbezogener Daten. Anders als z.B. in der KI-Verordnung handelt es sich dabei um eine unmittelbar wirkende Zuständigkeitsbestimmung durch das Europarecht, die keiner mitgliedstaatlichen Umsetzung bedarf. Die Datenschutzbehörden werden mit Geltungsbeginn des Data Act automatisch aufgrund unionsrechtlicher Zuweisung zuständig. Die Details des Zusammenwirkens wird ggf. das noch zu erlassende Umsetzungsgesetz regeln.

Einige Vorschriften des Data Act enthalten ausdrücklich nur Pflichten bezüglich nichtpersonenbezogener Daten. Für die Einhaltung dieser Normen wird der HmbBfDI nicht zuständig sein. Eine Vielzahl der Vorschriften betrifft jedoch beide Arten von Daten – solche mit Personenbezug und solche ohne. Hier wird bei der Aufsichtszuständigkeit danach zu differenzieren sein, ob im konkreten Fall personenbezogene Daten betroffen sind oder nicht. Eine enge Abstimmung zwischen den Datenschutzbehörden und der Aufsichtsbehörde nach dem Data Act gerade in Zweifelsfällen ist daher unausweichlich.

Sowohl für die Aufsicht als auch für die datenverarbeitenden Stellen stellt sich anlässlich des Geltungsbeginns des Data Act verschärft die Frage, wann Daten personenbezogen sind. Bislang waren alle Beteiligten gut beraten, in unklaren Konstellationen sowie bei gemischten Datensätzen von einem Personenbezug auszugehen und die Regelungen der DSGVO anzuwenden. Künftig ist ein genauerer Blick notwendig. Es gilt, Daten trennscharf danach abzugrenzen, ob sie personenbezogen und damit schützenswert sind oder ob sie keinen Personenbezug haben und damit potenziell auf Antrag mit Dritten zu teilen sind. Die nach wie vor herausfordernde Abgrenzung ist ein Kernthema der Datenschutzbehörden für das Jahr 2025, insbesondere sind Festlegungen durch die Anonymisierungsleitlinien des Europäischen Datenschutzausschusses zu erwarten.

Neben inhaltlichen Fragestellungen bereitet sich der HmbBfDI organisatorisch auf die neue gesetzliche Aufgabe vor. So wird er, sofern das deutsche Umsetzungsgesetz nichts Abweichendes regelt, z.B. Beschwerden nach dem Data Act entgegen zu nehmen haben und Befugnisse nach dem Rechtsakt ausüben können. Darüber hinaus wird im Jahr 2025 die Sensibilisierung der Öffentlichkeit sowie der Hamburger Wirtschaft im Mittelpunkt stehen. Infolge der vorgezogenen Neuwahl zum Deutschen Bundestag ist es fraglich, ob im September 2025 eine Aufsichtsbehörde für die Umsetzung in Bezug auf nichtpersonenbezogene Daten pünktlich gesetzlich benannt und arbeitsfähig eingerichtet sein wird. Jedenfalls in der für die Vorbereitung entscheidenden Phase im ersten Halbjahr 2025 werden die Datenschutzbehörden voraussichtlich die einzigen Stellen sein, für die eine künftige Aufsichtszuständigkeit unionsrechtlich vorgegeben ist. Damit kommt ihnen eine besondere Verantwortung bei der öffentlichen Aufklärung über die künftigen Rechte und Pflichten zu.

BERATUNGEN ÖFFENTLICHER STELLEN VII.

BERATUNGEN ÖFFENTLICHER STELLEN

1. Microsoft 365 in der Hamburger Verwaltung

Der Senat plant die flächendeckende Einführung von Microsoft 365 auf der Mehrzahl der Dienstrechner in den Behörden. Vor dem Hintergrund der aus Sicht der Datenschutzaufsichtsbehörden bisher geringen Transparenz über die Datenflüsse zwischen Microsoft und den das Produkt einsetzenden Stellen, ist dies herausfordernd. Der HmbBfDI ist daher aktiv an den Verhandlungen zwischen der Stadt und Microsoft beteiligt, um eine tragfähige Lösung zu erreichen.

Der HmbBfDI und die Datenschutzbehörden in der DSK beschäftigen sich mit der Frage der Nutzbarkeit von Microsoft 365 in der öffentlichen Verwaltung zumindest seit dem Jahr 2022 sehr intensiv. Eine eigens in der DSK gegründete AG „Microsoft Onlinedienste“ bewertete den Auftragsverarbeitungsvertrag, den Microsoft mit seinen Auftraggebern im Stil von allgemeinen Vertragsbedingungen vorformulierten Data Protection Addendum (DPA) schließt. Allein die daraus ersichtliche Rollenverteilung bei der Festlegung des Inhalts des Auftragsverarbeitungsvertrages ließ erahnen, dass die DSK vor dem Hintergrund des Regelungsinhalts des Art. 28 DSGVO zu einer kritischen Beurteilung kommen würde. Die Ergebnisse schlugen sich dann in den Beschlüssen der DSK im November 2022 nieder (nachzulesen unter https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf).

Gleichwohl verfolgten viele öffentliche Träger und Stellen das Vorhaben, Microsoft 365 zur Nutzung in der Verwaltung einzuführen. Auch in Hamburg hielt die Senatskanzlei an der Einführung von Microsoft 365 fest und beteiligte den HmbBfDI an diesem Projekt. Es folgte dazu ein intensiver Austausch, von dem bereits im Tätigkeitsbericht für das Jahr 2023 berichtet wurde. Es galt vor dem Hintergrund der DSK-Beschlüsse aus 2022, einen Weg für die Fortführung des Beratungsprozesses zu finden.

Der HmbBfDI ist zu diesem Zweck beratend in die Verhandlungen zwischen dem Senat und Microsoft eingebunden. Alleine im Jahr 2024 fanden acht trilaterale Workshops statt, in denen vertragliche Anpassungen vereinbart, technische Fragestellungen erläutert und individuelle Anpassungsmöglichkeiten diskutiert wurden. An den halbtägigen Treffen hat der HmbBfDI seine Expertise mit jeweils drei Leitungspersonen eingebracht. Die Workshopreihe wird im Jahr 2025 fortgesetzt.

In der datenschutzrechtlichen Bewertung von Microsoft 365 spielen grundsätzlich verschiedene Themenkomplexe eine Rolle. Eine besondere Schwierigkeit in der Bewertung spielt der Umstand, dass es sich bei Microsoft 365 nicht um ein homogenes Produkt handelt, sondern um eine Sammlung von verschiedenen Anwendungen, wie Teams, SharePoint, Office-Produkte usw., die wiederum über verschiedene „Hilfsdienste", wie die sogenannten verbundenen Erfahrungen, verbunden sein können bzw. ergänzt werden. Dieses System aus verschiedenen Anwendungen und Diensten löst komplexe Datenströme aus, die zum einen in tatsächlicher Hinsicht nur schwer nachvollziehbar sind, zum anderen sich nicht ohne weiteres in einem allgemeingültig formulierten Auftragsverarbeitungsvertrag abbilden lassen, ohne die Rollenverteilung aus Art. 28 DSGVO umzudrehen.

Aus dieser ersten Analyse ergeben sich folgende datenschutzrechtliche Themenfelder, die der HmbBfDI im Beratungsprozess zum Teil bereits erfolgreich bearbeiten konnte. Zunächst muss der Inhalt des DPA als Auftragsverarbeitungsvertrag an die Vorgaben aus Art. 28 DSGVO angepasst werden. Diese Anpassungen sind zumindest in Teilen in Bezug auf die tatsächliche Umsetzungsmöglichkeit zu prüfen, intransparente Datenflüsse sind aufzuklären, die einzelnen Produkte müssen in Bezug auf die Erforderlichkeit ihres Einsatzes genau geprüft und daraus resultierende Risiken ausreichend dokumentiert werden, lesende/sichtbarmachende Zugriffe auf Inhaltsdaten durch Microsoft sind auszuschließen und die allgemein möglichen Risiken müssen durch das Ausschöpfen aller für die verantwortliche Stelle verfügbaren Konfigurationsmöglichkeiten abgefedert werden.

Folglich war Gegenstand des Beratungsprozesses zunächst der Inhalt des DPA. Einige Aufsichtsbehörden hatten sich zu einer Zusammenarbeit in der DSK zusammengefunden und einen Weg gefunden, mit welchen Änderungen im DPA den Beschlüssen der DSK aus November 2022 abgeholfen werden könnte. Der Landesbeauftragte für den Datenschutz Niedersachsen veröffentlichte dazu eine Handlungsanweisung, die öffentlichen Stellen eine Art Verhandlungleitfaden für eine Nachverhandlung des DPA mit Microsoft an die Hand gab (vgl. https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/einsatz-von-microsoft-365-praxis-tipps-fur-vertrage-mit-microsoft-225722.html).

Der HmbBfDI teilte diesen Beratungsansatz und nahm die niedersächsische Handreichung als Grundlage, um die Senatskanzlei der FHH in einem Verhandlungsprozess zu begleiten und zu unterstützen. In diesem, noch nicht gänzlich abgeschlossenen Verhandlungsprozess, konnten verschiedene Erfolge erzielt und mit Microsoft eine Zusatzvereinbarung entworfen werden, die einige der aus den DSK-Beschlüssen hervorgehende Kritikpunkte ausräumen konnte. Insbesondere eine der im Vordergrund der Kritik stehenden Fragen, ob und in welchem Umfang Microsoft aus dem Auftragsverarbeitungsvertrag erlangte Daten für eigene Zwecke verarbeiten darf, konnte weitgehend ausgeräumt werden. Mit der entworfenen Zusatzvereinbarung konnte erreicht werden, dass zum einen die eigenen Zwecke Microsofts konkretisiert und eingegrenzt werden und zum anderen für die verbleibenden Zwecke nur nicht personenbezogene oder nicht personenbeziehbare Daten verarbeitet werden dürfen. Zudem erhält die Zusatzvereinbarung eine klarstellende Klausel, die die Verwendung von Inhaltsdaten für das Training von KI-Foundation-Modellen ausschließt. Zum Ende des Berichtszeitraums liegt die das DPA abändernde Zusatzvereinbarung bislang im Entwurf vor. Es zeichnet sich aber ab, dass die wesentlichen Punkte, insbesondere die vorstehend genannten Ergänzungen, von allen Parteien geteilt werden.

Aus Sicht des HmbBfDI gehört zu einem Beratungsprozess aber auch die sich an die Nachverhandlung anschließende Frage, ob sich

die Ergänzungen und Änderungen auch tatsächlich umsetzen lassen. Bei der Frage der Verarbeitung von Auftragsdaten zu eigenen Zwecken Microsofts wird diese Frage besonders relevant. Eine Verarbeitung von Daten zu eigenen Zwecken, die ausschließlich anonyme Daten umfasst, muss für Microsoft auch tatsächlich technisch möglich sein. Es muss ausgeschlossen sein, dass z.B. mittels sogenannter Lookup Tables eine Rückführbarkeit auf einzelne, natürliche Personen, die aus der Datenhaltung bei Microsoft resultiert, besteht und für diese zu einem Risiko führt. Zu dieser offenen Frage hat Microsoft im Beratungsverlauf eine Übersicht über die verschiedenen Datenauswertungsverfahren (Reports) gegeben und zugesagt, die bei der Verarbeitung von Daten zu eigenen Zwecken auftretenden Datenströme in Form von verschiedenen tatsächlich auftretenden Praxisfällen und Beispielen zu erläutern. Eine vom HmbBfDI geforderte Übersicht an Beispielen im Sinne einer repräsentativen Stichprobe, die einen praxistauglichen Überblick über die auftretenden Datenflüsse gibt, steht zum Ende des Berichtszeitraums offen. Hier wird sich zeigen, ob Microsoft in diesem Sinne eine tatsächliche Transparenz herstellen können wird.

Bei dem lesenden bzw. sichtbarmachenden Zugriff auf Inhaltsdaten des Auftraggebers stellt Microsoft hingegen deutlich klar, dass dieser nicht ohne ausdrückliche Weisung des Auftraggebers vorgenommen wird. In der Praxis soll dieser Fall nur bei Supportanfragen eine Rolle spielen. Um die verantwortliche Stelle zusätzlich in Bezug auf den Ausschluss eines entsprechenden Zugriffs durch Microsoft abzusichern, stellt Microsoft die sog. Customer Lockbox zur Verfügung. Diese Möglichkeit wird die FHH entgegen des Rats des HmbBfDI voraussichtlich nicht in Betracht ziehen, weil Supportfragen ausschließlich über Dataport als IT-Dienstleister der FHH abgewickelt werden sollen. Es bleibt abzuwarten, wie im weiteren Beteiligungsprozess eine Festschreibung des Supports in dieser Form rechtsverbindlich erfolgen können wird.

Noch offen ist, ob im Beratungsprozess eine Übersicht hinsichtlich der Erforderlichkeit aller für die Nutzung in Betracht gezogenen An-

wendungen aus dem Microsoft 365 Produktpaket erreicht werden kann. Entsprechende Zweifel bestehen insbesondere derzeit bezüglich der angedachten Nutzung von Viva Engage, eine Art internes Soziales Netzwerk. Zwar kann dies für den fachlichen Austausch der Mitarbeiter:innen in der FHH und die Identifizierung mit dem Arbeitgeber durchaus förderlich sein, führt aber zu einer im Vergleich zu den sonstigen Microsoft 365 Produkten beispiellosen Sammlung von Inhaltsdaten zu Beschäftigten der FHH, die zudem die Grenze zwischen rein dienstlichen und privaten Informationen verschwimmen lassen kann. Es bedarf daher differenzierter Erforderlichkeitsbetrachtungen und Risikobewertungen. Gerade die zuletzt genannten, eigens auf Viva Engage bezogenen Risikobetrachtungen, d.h. Schwellwertanalyse und ggf. Datenschutzfolgeabschätzung, blieb die Senatskanzlei aus für den HmbBfDI nicht nachvollziehbaren Gründen bislang schuldig, eine Nachreichung ist aber angekündigt. Im Ergebnis bleiben diese zwar abzuwarten, eine datenschutzrechtliche Bewertung der Nutzung von Viva Engage ist aus Sicht des HmbBfDI aber unabhängig von den sonstigen Diensten aus der 365 Familie vorzunehmen und ggf. von einer finalen Bewertung des Gesamtprojektes auszuklammern.

Im Ergebnis befindet sich der Beratungsprozess auf einem guten Weg und lebt von der aktiven Beteiligung der Senatskanzlei und der Kooperation von Microsoft. In Bezug auf den Auftragsverarbeitungsvertrag konnte mit der Zusatzvereinbarung zum DPA ein gutes Ergebnis in Hinblick auf die Wahrung der Rechte und Freiheiten von Betroffenen erzielt werden, wobei der konkrete Abschluss der Zusatzvereinbarung abzuwarten bleibt. Der Beratungsprozess im Übrigen wird fortgesetzt werden und hoffentlich zeitnah in eine finale Phase überführt werden können.

Bei allen vorstehenden Ausführungen ist zu bedenken, dass sich das derzeitige Projekt ausschließlich auf die Nutzung von Microsoft 365 für die Verarbeitung von Daten mit normalen Schutzbedarfsanforderungen bezieht. Die Nutzung für die Verarbeitung von Daten mit hoher Schutzbedarfsanforderung muss Gegenstand eines eigenständi-

gen Beratungsprozesses werden, der den Fokus auf die genannten Fragstellungen intensivieren und das Projekt vor neue Herausforderungen stellen wird.

2. Löschen im Aktenführungssystem Eldorado

Der HmbBfDI berät die Senatskanzlei der FHH bei der Implementierung einer Löschfunktion im Aktenführungssystem Eldorado, um die Voraussetzungen für die Umsetzung von Betroffenenrechten zu schaffen – was aus Datenschutzsicht selbstverständlich scheint, aber auch zu Konflikten mit Archivierungsinteressen führen kann, die zu lösen sind.

Die Frage des Löschens von Aktenbestandteilen und Dokumenten, die personenbezogene Daten enthalten, begegnet ganz verschiedenen rechtlichen Gesichtspunkten. Zunächst kann das entsprechende Löschen der Verwirklichung des Rechts auf informationelle Selbstbestimmung im Sinne von Art. 17 DSGVO dienen. Zudem berührt das Löschen personenbezogener Daten, was in der Konsequenz die Herausnahme von Dokumenten aus einer Akte bedeuten kann, Grundsätze wie den der ordnungsgemäßen Aktenführung. Ergänzt wird dieses Spannungsfeld durch die Berücksichtigung öffentlich-rechtlicher Archivzwecke, die beispielsweise in Art. 17 Abs. 3 lit. d DSGVO privilegiert werden und ggf. einer Löschung entgegenstehen könnten.

In der FHH wird zentral durch die Senatskanzlei unter anderem ein IT-Fachverfahren mit dem Namen Eldorado zur Führung von Akten zur Verfügung gestellt, das bislang keine reine Löschfunktion aufweist. Die Schaffung einer entsprechenden Funktion ist Gegenstand eines Beratungsprozesses, in dem sich der HmbBfDI mit der Senatskanzlei und dem Hamburgischen Staatsarchiv zu einem Dialog zusammengefunden hat. Im Kern steht die Frage im Raum, ob die Anbietungspflicht gemäß § 3 Hamburgisches Archivgesetz

(HmbArchG) durch die Schaffung einer Löschfunktion unterlaufen wird und damit berechtigte öffentlich-rechtliche Archivierungszwecke verhindert werden können.

Im Ergebnis sind sich alle Beteiligten einig, dass eine Löschfunktion vor dem Hintergrund der Regelung in Art. 17 DSGVO grundsätzlich gegeben sein muss, Aktenführungsgrundsätze und berechtigte Archivierungsinteressen aber durch klare Vorgaben an die Vornahme einer Löschung und ihrer organisatorischen Ausgestattung Berücksichtigung finden müssen. Die archivrechtliche Vorschrift in § 3 Abs. 2 Satz 2 HmbArchG berücksichtigt dabei bereits datenschutzrechtliche Gesichtspunkte, was eine Bildung von Fallgruppen, bei denen eine Löschung zu erfolgen hat, nahelegt. Technisch-organisatorische Maßnahmen, wie ein Vier-Augen-Prinzip bei der tatsächlichen Löschung bzw. Herausnahme von entsprechenden Dokumenten aus einer Akte sollen darüber hinaus berechtigte Archivierungsinteressen schützen. Diese Vorgaben gilt es nun in konkrete Handlungsanweisungen umzusetzen, damit die Anwender:innen in den Fachbehörden bei der Umsetzung von Löschansprüchen in jeder Hinsicht rechtssicher handeln können. Der Beratungsprozess war im Berichtsjahr nicht abzuschließen, befindet sich aber auf einen guten Weg.

3. Beteiligung an der neuen Authentisierungsrichtlinie RAuPE

Die bisherige Passwortrichtlinie wurde durch die Richtlinie zur Authentisierung von Personen und technischen Entitäten (RAuPE) ersetzt. Diese sieht neben der Absicherung von IT-Systemen mittels Benutzerkonto und Passwort bei entsprechendem Schutzbedarf nun auch den Einsatz von weiteren Faktoren vor.

Bereits im Jahr 2023 hat das Amt ITD der Senatskanzlei Hamburg die bisherige Passwortrichtlinie der FHH überarbeitet. Der HmbBfDI nahm die Möglichkeit wahr, sich neben weiteren Behörden der FHH in die Abstimmung einzelner Punkte einzubringen.

Seit dem 1. Mai 2024 ist die neue Richtline unter dem Namen „Richtlinie zur Authentisierung von Personen und technischen Entitäten (RAuPE)“ nach erfolgter Behördenanhörung über die IT-Beauftragten in Kraft und bringt die technischen Vorgaben der Authentisierung für Verfahren näher an den Stand der Technik. Die Überarbeitung orientiert sich an den Anforderungen des Identitätsmanagements nach IT-Grundschutz des BSI.

In der neuen Richtlinie werden die Anforderungen an Passwörter erhöht und der Einsatz von weiteren Faktoren für den Identitätsnachweis an IT-Systemen ermöglicht und geregelt. Zu den Faktoren zählen software- und hardwarebasierte Token und Biometrie. Für IT-Systeme mit hohem oder sehr hohem Schutzbedarf wird die Verwendung eines weiteren Faktors hier dringend empfohlen. Die Verantwortung und die Entscheidung über den Einsatz verbleiben jedoch in der Regel bei den fachlich Verantwortlichen.

Der HmbBfDI begrüßt die Überarbeitung der Richtlinie, da nun bereits bestehende und zukünftige IT-Systeme und damit verbundene Verfahren besser ihren Anforderungen und Schutzbedarfen entsprechend abgesichert werden können. In diesem Zusammenhang hob der HmbBfDI die Notwendigkeit der Überprüfung der Identität einer Person bei der Erstellung eines Nutzerkontos hervor.

Seit 2024 baut der IT-Dienstleister der öffentlichen Verwaltung der Stadt Hamburg ein zentrales System für die Verwendung von mehreren Authentisierungsfaktoren auf. Im Jahr 2025 soll das stadtweite Ausrollen der Unterstützung dieser Faktoren in einzelnen Verfahren beginnen. Bei einzelnen Verfahren mit erhöhtem Schutzbedarf wird die Verwendung eines zweiten Faktors anschließend verpflichtend sein.

4. E-Akte Soziales

Seit Ende 2023 ist der HmbBfDI in das Projekt E-Akte Soziales eingebunden, mit dem die Stadt Hamburg eine Schnittstelle zwischen unterschiedlichen Anwendungen aufbauen möchte, um eine digitale Akte für den Sozialbereich zu schaffen.

Ziel des Projektes ist es, einen einheitlichen Aktenplan für den Bereich Soziales zu schaffen, die in den Sozialämtern (Fachämter für Grundsicherung und Soziales) eingehenden Unterlagen frühzeitig zu digitalisieren und diese damit digital nutzbar zu machen. Hierfür wird auf den Scanprozess des Projektes elektronische Posteingangsbearbeitung (ePob) zurückgegriffen. Bei der Nutzung von ePob für die Verarbeitung von Sozialdaten ist jedoch zu berücksichtigen, dass die örtlichen Gegebenheiten beim Scanprozess anzupassen sind. So sieht die Geschäftsordnung der Bezirksämter in Ziffer 4. vor, dass Posteingänge der Sozialämter nicht von einer zentralen fachamtsübergreifenden Poststelle geöffnet werden sollen. Die Eingänge sind verschlossen an die zuständige Geschäftsstelle weiterzuleiten. Im Rahmen der Nutzung von ePob ist dieser sich selbst auferlegten Regelung, die eine Wahrung besonderer Vertraulichkeit darstellt, hinreichend Rechnung zu tragen. Bei einem zentralisierten Postbearbeitungsverfahren sind daher weitere Maßnahmen zu treffen, um eine Verarbeitung außerhalb der zuständigen Geschäftsstelle datenschutzkonform zu gestalten. Dabei gilt es insbesondere für eine strikte Trennung von Eingangspost aus anderen Fachbehörden zu sorgen und den Zugriff im Rahmen des Scanvorgangs und seinen vor- und nachgelagerten Bearbeitungsschritten auf einen klar eingegrenzten, klein gehaltenen und ausgewählten Kreis an Mitarbeitenden zu beschränken.

Um eine Speicherung der Unterlagen und einen Zugriff auf diese durch die zuständige Fachkraft zu ermöglichen, wird von dem ausführenden Projekt zwischen den Anwendungen ELDORADO und

OPEN/PROSOZ eine Schnittstelle geschaffen. Dies führt zu weiteren datenschutzrechtlichen Problemen, da die etablierten Anwendungen in ihrer ursprünglichen Nutzung eine Verarbeitung von Sozialdaten, also Daten mit hohem Schutzbedarf, nicht vorgesehen haben. Hinsichtlich der Anwendung ELDORADO, die als Speicherort der Metadaten genutzt wird und somit als elektronische Akte gilt, bestehen Unsicherheiten. Denn die Anwendung sieht eine Löschung oder Schwärzung von Dokumenten derzeit nicht vor. Selbstverständlich muss aber eine Anwendung, die sensible Daten verarbeitet, auch in der Lage sein, diese zu löschen. Der Sozialdatenschutz, der im Falle der Verarbeitung durch die Fachämter zum Tragen kommt, sieht zudem eine strenge Trennung der verarbeiteten Daten, auch innerhalb einer Behörde, vor. Nur die konkret betraute Fachkraft sowie zwangsläufig mitverantwortliche Leitungs- und Unterstützungsstellen sollen Zugriff auf die konkrete Akte haben. Insofern müssen Zugriffsrechte auch innerhalb einer Organisationseinheit richtig eingestellt werden. Der HmbBfDI setzt sich im Rahmen der Projektbeteiligung für eine Beachtung der datenschutzrechtlichen Belange in diesem Sinne ein und befindet sich weiter im Austausch mit der Projektleitung, die sich derzeit um eine Umsetzung der datenschutzrechtlichen Anforderungen bemüht.

5. Anforderungen an Benennungen von behördlichen Datenschutzbeauftragten

Der HmbBfDI hebt die Wichtigkeit einer gesetzeskonformen Benennung von Datenschutzbeauftragten hervor. Die Vorabprüfung der Unabhängigkeit dieser Personengruppe durch die öffentlich verantwortlichen Stellen stellt einen wichtigen Baustein der DSGVO zur Sicherung des Datenschutzes dar.

Die Benennung und Stellung von Datenschutzbeauftragten ist eine wesentliche Grundlage für einen zielführenden Schutz personenbezogener Daten im Sinne der DSGVO. Art. 37 DSGVO und Art. 38

DSGVO regeln die Voraussetzungen für eine ordnungsgemäße Aufgabenerfüllung. Die dort verankerten Maßstäbe sind stets kritisch und aktuell daraufhin zu überprüfen, wie sie in der Verwaltungspraxis umgesetzt werden.

Bei dieser Aufgabe begleitete der HmbBfDI beratend die gesamte Verwaltung, auch im Berichtsjahr 2024. Verantwortliche Stellen in Hamburg verfügen bereits über Hilfestellungen bezüglich ihrer Pflichten, die bei der Benennung von Datenschutzbeauftragten zu beachten sind. Informationen zur Benennungspflicht finden sich auf der von dem HmbBfDI zur Verfügung gestellten Homepage unter dem Link: https://datenschutz-hamburg.de/service-information/dsb-an-/abmelden sowie im Kurzpapier der DSK zur Benennung von Datenschutzbeauftragten (vgl. Kurzpapier Nr. 12 Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern).

Der HmbBfDI hält es in Ergänzung dazu insbesondere für erforderlich, auf Art. 38 Abs. 6 DSGVO hinzuweisen. Dieser Vorschrift kommt eine wichtige Bedeutung zu. Der Verantwortliche darf einem/r Datenschutzbeauftragten grundsätzlich andere Aufgaben zusätzlich übertragen, dabei muss er/sie jedoch sicherstellen, dass diese weiteren Tätigkeiten nicht zu Interessenkonflikten führen, die vorliegen, wenn parallel Leitungspositionen im Management oder im Personalbereich eingenommen werden bzw. die Aufgabenfelder eine Steuerung von Zwecken und Mitteln der Datenverarbeitung erfordern. Die Benennungsvoraussetzung als echte Organisationspflicht dient der Sicherstellung, dass der/die Datenschutzbeauftragte bei der Prüfung datenschutzrechtlicher Sachverhalte unabhängig ist. Diese Bedingungen sind nicht erfüllt, soweit Interessenkonflikte derart zu erwarten sind, dass der/die Datenschutzbeauftragte/r beispielsweise Aufgaben überprüfen muss, die er/sie selbst in anderer Funktion ausgeübt hat. Das Fehlen ausreichender personeller Kapazitäten darf nicht dazu führen, dass es in der Person der/des Datenschutzbeauftragten zu der oben beschriebenen Doppelrolle als Leitungsverantwortliche/r und Datenschutzbeauftrage/r kommt und damit ein unzulässiger Zustand hergestellt wird. Der Position

der/des Datenschutzbeauftragen sind gerade vor dem Hintergrund einem mit der Digitalisierung der öffentlichen Verwaltung verbundenen „Mehr“ an Datenverarbeitung und komplexer werdenden Verarbeitungsvorgängen ausreichende Ressourcen zur Aufgabenerfüllung einzuräumen. Knappen personellen Ressourcen im öffentlichen Bereich wird daher auch durch die Regelung in Art. 37 Abs. 3 DSGVO Rechnung getragen, so dass die beschriebene Vermischung von fachrechtlichen und datenschutzrechtlichen Aufgaben durchaus vermieden werden kann.

6. Sichere Kommunikation beim ASD

Die Einführung einer Ende-zu-Ende-Verschlüsselung zwischen dem Allgemeinen Sozialen Dienst (ASD) und den Jugendhilfeträgern erfolgt zunächst nicht. Stattdessen wird eine Lösung in Form eines E-Mail-Gateways in Aussicht gestellt. Der HmbBfDI hat in diesem Zusammenhang darauf hingewiesen, dass es sich bei einer solchen technischen Gestaltung nur um eine Zwischenlösung handeln kann und das Erfordernis einer Ende-zu-Ende-Verschlüsselung weiterhin besteht.

In der Vergangenheit ist der HmbBfDI bereits mit der E-Mail-Kommunikation mit externen Stellen durch den ASD befasst gewesen (vgl. 32. TB Datenschutz 2023, Kapitel II 3). Es war eine nicht ausreichende Verschlüsselung in der Kommunikation bei sensiblen personenbezogenen Sozialdaten festgestellt worden. Der HmbBfDI ist nun erneut gebeten worden, zum Erfordernis einer Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung) für den Anwendungsfall des ASD Stellung zu nehmen. Vor dem Hintergrund einer neuen Lösungsoption, der Verwendung eines sogenannten „Zentralen Mailgateway“ (ZGW), hat der HmbBfDI die zuständigen öffentlichen Stellen beraten.

Der HmbBfDI vertritt weiterhin die Ansicht, dass die Umstände der Datenverarbeitung beim ASD einen hohen Schutzstandard für die

digitalen Kommunikationswege verlangen. Dies liegt an den konkret verarbeiteten Sozialdaten, die durch ein besonderes Vertrauensverhältnis geprägt sind, unter diversen Aspekten einer Geheimhaltungspflicht unterliegen und – allein durch die Art der Daten – ein hohes Risiko für die Rechte und Freiheiten der Betroffenen darstellen. Aus den dem HmbBfDI vorliegenden Informationen geht hervor, dass das ZGW mit der Funktion „Domänenzertifikat" keine Ende-zu- Ende-Verschlüsselung im engeren Sinne bietet. Domänenzertifikate stellen eine proprietäre Abweichung zur Standard-S/MIME-Nutzung dar, wodurch ein X.509-Zertifikat durch ZGWs auf beiden Seiten der Kommunikation auf mehrere E-Mail-Identitäten abgebildet wird. Sowohl die Ver- als auch Entschlüsselung findet auf den ZGWs und nicht im E-Mail-Client des Endnutzenden statt. Der avisierte Kommunikationsweg beim ZGW nutzt mit S/MIME zwar eine Technologie, die E2E-Verschlüsselung gewährleisten kann, setzt die tatsächlichen Endpunkte der S/MIME-Verschlüsselung mit den ZGWs aber so, dass kein E2E-Schutz besteht. Das gilt sowohl für die Vertraulichkeit als auch für die Authentizität und Integrität der E-Mails. Aufgrund der Domänenzertifikate hat der Empfänger weder eine kryptographische Garantie über die Authentizität des tatsächlichen, individuellen Absenders, noch über die E2E-Integrität der Inhalte. In diesem Sinne steht die Nutzung von Domänenzertifikaten im Gegensatz zu der individualisierten Adressierung bei E2E-Verschlüsselung, wie sie die Orientierungshilfe der DSK („Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" vom 27.05.2021) als Maßnahme nennt. Weiter ist die Vertraulichkeit nicht E2E gewahrt, da durch die zentrale Ver- und Entschlüsselung Inhalte unverschlüsselt in Postfächern vorliegen. Die Schutzwirkung des ZGW mit Domänenverschlüsselung geht daher nicht wesentlich über eine qualifizierte Transportverschlüsselung hinaus, da Vertraulichkeit, Authentizität und Integrität nicht im E2E-Verhältnis zwischen den individuellen Kommunikationspartnern erreicht wird. Vielmehr beschränkt sich die Wirkung auf die Kommunikation zwischen den ZGWs, was analog ist zur Schutzwirkung einer qualifizierten Transportverschlüsselung zwischen den Mailservern von Sender und Empfänger. Der HmbBfDI sieht den ZGW daher nur als Zwischenlösung an, hat sich aber nicht grundsätzlich gegen eine sol-

che Zwischenlösung ausgesprochen. Mittelfristig ist der Aufbau von Lösungen für E2E-verschlüsselter Kommunikation im Sinne einer Basisinfrastruktur eine Aufgabe für die öffentliche Verwaltung als Ganzes. Diesbezüglich unterstützt der HmbBfDI auch Bestrebungen zur Schaffung FHH-weiter Lösungen.

7. Datenschutz im Parlamentarischen Untersuchungsausschuss

Im Zwischenbericht des Cum-Ex-Untersuchungsausschusses der Bürgerschaft wurden zahlreichen Zeug:innen namentlich erwähnt. Eine dagegen gerichtete Beschwerde einer Zeugin hat Fragen zur Datenschutzaufsicht im parlamentarischen Bereich aufgeworfen. Der konkrete Fall wurde in Kooperation zwischen dem Datenschutzgremium der Bürgerschaft und dem HmbBfDI gelöst.

Das Datenschutzrecht der DSGVO gilt auch für den parlamentarischen Bereich. Diese in der Vergangenheit umstrittene Fragestellung hat der Europäische Gerichtshof mit seiner Entscheidung vom 16.1.2024 (Rs. C-33/22, Rn. 40) klar bejaht. Gegenstand des Urteils war die Namensnennung von Zeugen in veröffentlichten Ausschussdokumenten des österreichischen Parlaments. Die in der Alpenrepublik bislang geltende Rechtslage, die das Parlament aus der Aufsichtszuständigkeit der dortigen Datenschutzbehörde ausgeklammert hatte, erklärte der Europäische Gerichtshof für unionsrechtswidrig.

Das Urteil hatte direkte Auswirkungen auf ein Beschwerdeverfahren in Hamburg. Eine Zeugin, die zuvor im Untersuchungsausschuss „Cum-Ex-Steuergeldaffäre“ ausgesagt hatte, wandte sich an den HmbBfDI. Sie bat um Überprüfung, ob die Nennung ihres Vor- und Nachnamens im Zwischenbericht des Untersuchungsausschusses mit der DSGVO vereinbar gewesen war. Für ein Tätigwerden des HmbBfDI bestand jedoch das Hindernis, dass nach § 19 Abs. 3 HmbDSG der parlamentarische Bereich der Bürgerschaft aus-

drücklich aus seiner Aufsichtszuständigkeit ausgenommen ist. Er beaufsichtigt das Parlament gemäß der Vorschrift nur, soweit es in Verwaltungsangelegenheiten tätig wird. Die inhaltliche Arbeit des Untersuchungsausschusses sowie die Anfertigung und Veröffentlichung von Dokumentationen und Berichten daraus ist jedoch eine parlamentarische Tätigkeit.

Um aufsichtsfreie Räume zu vermeiden, hat die Hamburgische Bürgerschaft ein eigenes Datenschutzgremium eingerichtet. Dieses besteht aus jeweils einer bzw. einem Abgeordneten pro Fraktion. Seine Einrichtung, Aufgaben und Befugnisse ergeben sich aus der Datenschutzordnung, die sich die Bürgerschaft gegeben hat. Die Datenschutzordnung enthält auch materiellrechtliche Datenschutzregeln. Eine Bezugnahme auf die DSGVO findet sich in der Datenschutzordnung nicht, weil der Gesetzgeber offenkundig davon ausgegangen war, dass die DSGVO nicht für parlamentarische Aufgaben einschlägig ist. Statt eines Verweises auf die Befugnisse aus Art. 58 DSGVO stattet die Datenschutzordnung das Datenschutzgremium der Bürgerschaft mit eigenen Befugnissen aus, die jedoch weniger weit reichen als die nach der DSGVO.

Bislang konnte es für den HmbBfDI dahinstehen, ob Art und Befugnisse des Datenschutzgremiums den Anforderungen der DSGVO an eine unabhängige Datenschutzbehörde entsprechen. Der eindeutige gesetzliche Ausschluss des parlamentarischen Bereichs aus der Zuständigkeit des HmbBfDI galt aus seiner Sicht unbeschadet von der Frage, ob eine europarechtskonforme Aufsichtsstelle diese Lücke füllt. Die aktuelle Entscheidung des Europäischen Gerichtshofs schafft neue Komplexität. In der österreichischen Rechtslage bestand ebenfalls ein expliziter Ausschluss der Zuständigkeit der Datenschutzbehörde. Der Gerichtshof hat diesen Ausschluss jedoch für unanwendbar erklärt mit der Folge, dass die einzige Datenschutzbehörde Österreichs nun auch das Parlament vollständig datenschutzrechtlich beaufsichtigt. Die Lage ist nur begrenzt auf Hamburg zu übertragen, denn in Hamburg gibt es anders als seinerzeit in Österreich ein parlamentsinternes Aufsichtsgremium.

Der HmbBfDI und das Datenschutzgremium der Bürgerschaft haben sich entschieden, die nicht eindeutige rechtliche Situation im Einzelfall durch Kooperation zu lösen. Dieser Weg diente der angemessenen Behandlung des Anliegens der Beschwerdeführerin. Ihr ging es um eine Beurteilung in der Sache, sodass eine langfristige Erörterung von Zuständigkeitsfragen nicht hilfreich gewesen wäre. Der HmbBfDI hat deshalb nach Zustimmung der Beschwerdeführerin die Beschwerde an das Datenschutzgremium der Bürgerschaft weitergeleitet. Das Gremium hat sich aus diesem Anlass sodann erstmals in der Legislativperiode konstituiert. Bei der inhaltlichen Beurteilung des Beschwerdefalls hat es den HmbBfDI zu seiner Sitzung eingeladen. Dort hat sich der HmbBfDI für die Belange der Beschwerdeführerin eingesetzt. Das Vorgehen geschah im Einklang mit § 14 Abs. 7 der Datenschutzordnung, wonach das Datenschutzgremium den bzw. die HmbBfDI um Beratung ersuchen kann.

8. Onlineübertragung und Aufzeichnung von Lehrveranstaltungen der Universität

Die Universität Hamburg (UHH) hat den HmbBfDI für eine Gesetzinitiative zur Änderung des Hamburgischen Hochschulgesetzes (HmbHSG) hinzugezogen, um insbesondere datenschutzrechtliche Anforderungen an eine Rechtsgrundlage für die Onlineübertragung und Aufzeichnung von Lehrveranstaltungen der Universität abzustimmen.

Die Corona Pandemie war ein entscheidender Impulsgeber für die Digitalisierung ganz verschiedener Bereiche, wovon auch im besonderen Maße der Hochschulbetrieb betroffen war. Die Notwendigkeit, Lehrveranstaltungen in digitaler Form abzuhalten, erkannte der Gesetzgeber, auch wenn zum damaligen Zeitpunkt das Abhalten von Lehrveranstaltungen in digitaler Form noch eindeutig als Ausnahmefall identifiziert wurde. Aus dieser Ausgangssituation entstand die jetzt in § 111 HmbHSG enthaltene Regelung, die für die Übertragung von digitalen Lehrveranstaltungen und deren Aufzeichnung

verschiedene Einschränkungen enthält, die aus rein datenschutzrechtlicher Sicht zu begrüßen waren.

Aus dem pandemiebedingten Impuls für die Digitalisierung des Lehralltags ergaben sich ganz wesentliche Folgen für den regulären Lehrbetrieb. Digitale Formate wurden als gute Ergänzung des Hochschulbetriebs wahrgenommen und sollten auch weiterhin genutzt und weiterentwickelt werden, um neue Formen des Lehrens und Lernens zu ermöglichen. Dementsprechend beschäftigte sich die UHH mit einer Reform der hochschulrechtlichen Regelungen.

Die Vorschläge der UHH insbesondere zur Anpassung des § 111 HmbHSG orientieren sich an den praktischen Bedarfen der Universität. Dabei erkennt die UHH Reformbedarf der hochschulrechtlichen Änderungen, denn das HmbHSG unterstreiche in seinem Begründungsteil zwar die „erhebliche praktische Bedeutung digitaler Lehr-, Lern- und Prüfungsformate für den modernen Hochschulbetrieb" und erkenne an, dass digitale Formate ein „wichtiger Baustein zu einer qualitativ hochwertigen und zeitgemäßen Lehre" seien, die konkrete gesetzliche Regelung würde diesem Anspruch jedoch nicht gerecht. Insbesondere das Einwilligungserfordernis für Wortbeiträge gemäß § 111 Abs. 2 HmbHSG und das strikte Verbot der bildlichen Aufzeichnung der Teilnehmenden stellten keinen Fortschritt, sondern einen Rückschritt in der Digitalisierung der Lehre dar. Die Bild- und Tonaufnahme von Teilnehmenden durch die Hochschule sei nicht nur als Veranstaltungsaufzeichnung, sondern auch in anderen Situationen aus didaktischen Gründen unverzichtbar. Darüber hinaus werde derzeit die Eigenveröffentlichung der Lehrenden zu stark eingeschränkt. Damit die Lehrenden die ihrerseits veranlassten und nur sie betreffenden Aufzeichnungen über den Kreis der Lehrveranstaltung hinaus weiterverwenden können, wurden entsprechende Änderungen des HmbHSG vorgeschlagen.

Der Vorschlag der UHH sieht auch die Streichung des Begriffs der „Online Lehre" vor. Die bisherige Intention des Gesetzgebers wurde aber bislang so verstanden, dass in Bezug auf die Aufzeichnungs-

befugnis hinsichtlich Lehrveranstaltungen bewusst zwischen Präsenzbetrieb und Fernlehre unterschieden werden und ein Regel-/Ausnahmeverhältnis geschaffen werden sollte. Die Streichung dieses Begriffs würde diese Wirkungsrichtung durchbrechen und unter datenminimierenden Gesichtspunkten auch als datenschutzrechtlich problematisch einzuordnen sein, insbesondere wenn im Folgenden eine sehr weit gefasste Aufzeichnungsbefugnis geschaffen werden soll.

Den Kern des Vorschlags der Universität stellte aber die angestrebte Änderung in § 111 Abs. 2 Satz 2-3 HmbHSG dar. In erster Linie soll das Anknüpfen an eine Einwilligung der Betroffenen aufgelöst werden. An der jetzt in § 111 HmbHSG formulierten Einwilligungslösung lässt sich tatsächlich auch aus datenschutzrechtlicher Hinsicht Kritik formulieren, denn es scheint fraglich, ob eine tatsächliche Freiwilligkeit gegeben sein kann. Die bislang restriktiv formulierten Voraussetzungen für die Aufzeichnung der Teilnehmenden an Lehrveranstaltungen sollen zudem durch eine sehr weit gefasste, regelbeispielartige Ergänzung aufgehoben werden. Die dafür aufgeführten Fallgruppen sind bisher so allgemein gehalten, dass sich aus Sicht des HmbBfDI keine wesentliche Einschränkung der Aufzeichnungsbefugnis mehr finden würde. Die Begründung für die ausbleibende Differenzierung von Fallgruppen ist zwar unter praktischen Gesichtspunkten verständlich, aber unter Verhältnismäßigkeitsgesichtspunkten nicht tragbar, zumindest konträr zu den bisherigen Auffassungen des HmbBfDI.

Die Möglichkeit, Lehrveranstaltungen aufzuzeichnen, wurde von Seiten des HmbBfDI bislang kritisch begleitet. Gerade kleinere Lehrveranstaltungen bieten aufgrund des kleinen Kreises an Teilnehmenden oftmals eine Art intimen Rahmen, der Einfluss auf die Sensibilität der Wortbeiträge und Schutzbedürftigkeit der Teilnehmenden haben kann. Auch könnte aufgrund des Inhalts von Wortbeiträgen der Anwendungsbereich von Art. 9 DSGVO betroffen sein, gerade bei politischen oder weltanschaulichen Wortäußerungen, die aufgrund der bildlichen Abbildung eine eindeutige Personenbeziehung auf-

weisen können. Vor diesem Hintergrund hatte der HmbBfDI bislang angeregt, in der Norm für die Aufzeichnungsbefugnis nach Art und Format der Lehrveranstaltungen zu differenzieren. Der Gesetzgeber hatte die jetzige Vorschrift in § 111 Abs. 1 HmbHSG auch vor dem Hintergrund dieser Bedenken, und unter Berücksichtigung eigener Verhältnismäßigkeitsabwägungen geschaffen.

Die Beteilung des HmbBfDI in dieser Angelegenheit ist noch nicht abgeschlossen. Die bisherigen Gespräche mit den Vertreter:innen der UHH verlaufen sehr kooperativ. Die UHH erkennt an, dass die Modernisierung in der Lehre nicht zu unzumutbaren Einschränkungen der Studierenden in ihrem Recht auf informationelle Selbstbestimmung führen darf. Insoweit ist es auch im Interesse der UHH, eine DSGVO-konforme Digitalisierung der Lehre dauerhaft zu etablieren, die zugleich die Lehre zukunftsfähig ausgestaltet.

9. Kostenloses HVV-Ticket für alle Schüler:innen

Seit Beginn des Schuljahres 2024/2025 erhalten Schüler:innen, die in Hamburg wohnen ein kostenloses Deutschlandticket. Die damit zwangsläufig verbundene Berechtigungsprüfung warf verschiedene datenschutzrechtliche Fragen auf, die aber aus Sicht des HmbBfDI auch vor dem Hintergrund der verfolgten Ziele, nämlich eine erhebliche finanzielle Entlastung für Familien zu erreichen und durch die stärkere Nutzung öffentlicher Verkehrsmittel einen Beitrag für den Klimaschutz zu leisten, gut gelöst werden konnten.

Der Berechtigtenkreis umfasst alle in Hamburg wohnhaften Schüler:innen bis zur Vollendung des 15. Lebensjahres sowie Schüler:innen nach Vollendung des 15. Lebensjahres an öffentlichen oder privaten allgemeinbildenden Schulen, berufsbildenden Schulen und Einrichtungen des zweiten Bildungsweges; mithin insgesamt circa 210.000 Schüler:innen.

Vor Einführung dieses kostenlosen Deutschlandtickets wurde auch der HmbBfDI konsultiert und um eine rechtliche Einschätzung der vom hvv entwickelten Konzepte gebeten.

Eingangs wurde seitens des hvv – unabhängig vom Alter der Schüler:innen – ein vollständig digitaler Bestellprozess angestrebt. Zunächst war hier beabsichtigt, mithilfe einer validen Datenbasis und eindeutiger Schülerkennung digital und in Echtzeit eine Berechtigungsprüfung zwischen dem System der Behörde für Schule und Berufsbildung (BSB) und dem des hvv durchzuführen. Zum Zweck dieser Berechtigungsprüfung wurde unter anderem in Betracht gezogen, dem hvv Zugriff auf bereits bestehende Datenquellen (z.B. DIVIS, Melderegister, Zentrales Schülerregister [ZSR]) zu ermöglichen.

Eine digitale Echtzeit-Berechtigungsprüfung für Personen an öffentlichen Schulen durch direkten Abgleich mit einer der oben genannten Datenquelle mag zwar der Vereinfachung dienen, ist aber aus Sicht des HmbBfDi mit wesentlich größeren Risiken für die Betroffenen verbunden. Ein solcher Abgleich setzt voraus, dass der Datenbestand über das Internet bspw. für das hvv Kundenportal zugänglich ist – damit aber auch durch Dritte angreifbar.

Insbesondere das Zentrale Schülerregister enthält sensible personenbezogene Daten besonders zu schützender Personen, nämlich von Kindern. Dieses Register beinhaltet auch Anschriften, für welche eine melderechtliche Auskunftssperre besteht. Der HmbBfDI ist daher der Auffassung, dass dieser Datenbestand nicht für Abfragen oder Zugriffe durch den hvv zum Zwecke der Berechtigungsprüfung freigeschaltet werden sollte. Derartige Daten fordern einen sensiblen Umgang.

Das nun gewählte Antragsverfahren stieß beim HmbBfDI auf keine Bedenken: Bei Schüler:innen im Alter von 6 bis inklusive 15 Jahren wird eine Berechtigung lediglich anhand des Geburtsdatums geprüft, welches während der Bestellung erfasst wird. Da die als Ticketmedium verwendete Chipkarte postalisch zugesendet wird, kann

auf diesem Wege auch sichergestellt werden, dass es sich hierbei um Schüler:innen mit Wohnort Hamburg handelt. Ein Abgleich dieser Daten mit anderen Datenbeständen ist daher nicht erforderlich.

Die Gruppe der Schüler:innen, welche nicht vollumfänglich von der Schulpflicht erfasst sind, mithin Schüler:innen ab 16 Jahren, müssen im Rahmen der Berechtigungsprüfung während des Bestellprozesses einen entsprechenden Nachweis vorlegen. Diesen Berechtigungsnachweis erhalten die Schüler:innen im Sekretariat ihrer jeweiligen Schule. Dieser Nachweis wird während des Bestellprozesses mit eingereicht. Durch die frühe Einbindung des HmbBfDI konnte eine angemessene Balance zwischen datenschutzrechtlichen Anforderungen und praktischen Erwägungen gefunden werden, um die Rechte und Freiheiten der betroffenen Personengruppe zu verwirklichen.

10. Automatisierte Verkehrsmengenerfassung – aVME 3.0

Seit etwa fünf Jahren begleitet der HmbBfDI bereits das Projekt „Automatisierte Verkehrsmengenerfassung – aVME", das die Auslastung der Straßen Hamburgs durch den Verkehr misst und damit eine Tatsachengrundlage für Maßnahmen der Verkehrsplanung und -steuerung schafft. Aus Anlass eines Vergabeverfahrens, in dessen Rahmen insbesondere neue Erfassungsgeräte erprobt und ausgewählt werden sollten, haben auch im Berichtszeitraum intensive Beratungsgespräche mit den zuständigen Stellen, vor allem mit der Behörde für Verkehr und Mobilitätswende und dem Landesbetrieb Straßen, Brücken und Gewässer stattgefunden.

Zum Zwecke der automatisierten Verkehrsmengenerfassung kommen in Hamburg seit dem Jahr 2020 an 420 Straßenkreuzungen und 90 weiteren Orten Wärmebildkameras zum Einsatz. Diese fertigen Infrarotaufnahmen, die die Wärmestrahlung von Verkehrsobjekten abbilden und diese so ihrer Art nach – als Pkw, Lkw oder Zweirad – erkennbar machen. Nach automatisierter Zählung und Klassifizie-

rung der Fahrzeuge, die in Echtzeit durch eine Bildanalysesoftware erfolgt, werden die Aufnahmen gelöscht. Die Analyseergebnisse werden auf der Urban Data Plattform Hamburg bereitgestellt.

Der HmbBfDI hat das Projekt bereits 2019 aus datenschutzrechtlicher Perspektive beleuchtet und die technische Ausgestaltung im Ergebnis als datensparsam und daher unbedenklich eingestuft (vgl. zu den Einzelheiten den 28. Tätigkeitsbericht des HmbBfDI aus dem Jahr 2019, Kapitel V 2.2). Zu der im Jahre 2021 beabsichtigten Projekterweiterung, die u.a. eine Reisezeitermittlung ermöglichen sollte, äußerte sich der HmbBfDI hingegen kritisch (vgl. hierzu den 30. Tätigkeitsbericht des HmbBfDI aus dem Jahr 2021, Kapitel 6.6.5). Der Ansatz wurde durch die zuständigen Stellen nicht weiterverfolgt.

Im Jahr 2023 ging das Projekt unter der Bezeichnung „aVME 3.0“ in seine dritte Phase über. Die Projektverantwortlichen eröffneten ein Vergabeverfahren mit dem Ziel, neue Geräte zur automatisierten Verkehrsmengenerfassung auszuwählen, die zunächst an 50 Verkehrsknotenpunkten eingesetzt werden sollten. Der HmbBfDI nahm 2024 eine datenschutzrechtliche Bewertung der Bietersysteme vor und beriet die zuständigen Stellen insbesondere zur Frage des Personenbezugs.

Im Hinblick auf videogestützte Erfassungssysteme regte der HmbBfDI an, einen Personenbezug der Verkehrsaufnahmen mittels einer geeigneten Systemkonfiguration und flankierender technisch-organisatorischer Maßnahmen auszuschließen. So kann der Personenbezug von Verkehrsaufnahmen etwa dann entfallen, wenn diese in einer möglichst niedrigen Auflösung und in Schwarz-Weiß gefertigt und/oder insgesamt verpixelt werden, so dass die Verkehrsteilnehmenden ihrer Kategorie nach, also bspw. als Radfahrende, für das Kamerasystem erkennbar bleiben, aber nicht aufgrund äußerer Merkmale identifiziert werden können. Auch in Ansehung der bisherigen Lösung, wonach die Aufnahmen automatisiert in Echtzeit ausgewertet werden und unmittelbar im Anschluss verfallen, empfahl der HmbBfDI, das Bildmaterial auch weiterhin umge-

hend zu löschen sowie technisch-organisatorische Maßnahmen zur Absicherung der gewählten Konfiguration zu treffen.

Ob es zu einem Austausch der Datenerfassungsgeräte an ausgewählten Verkehrsknotenpunkten im Rahmen des Projekts „aVME 3.0“ kommen wird, ist derzeit offen. Bis dahin wird die Verkehrsmengenerfassung in Hamburg weiterhin mithilfe der datensparsamen Wärmebildkamerasysteme vorgenommen.

VIII. ÖFFENTLICHKEITSARBEIT UND MEDIENBILDUNG

ÖFFENTLICHKEITSARBEIT UND MEDIENBILDUNG

1. Pressearbeit

Im Jahr 2024 haben Presseanfragen im Zusammenhang mit dem Schutz personenbezogener Daten bei Anwendung von künstlicher Intelligenz stark zugenommen. 22 Prozent aller Anfragen hatten einen KI-Bezug. Mehr als 16 Prozent der Anfragen bezogen sich auf das geplante KI-Training des Meta-Konzerns mit Nutzerdaten. Insgesamt 32 Prozent der Presseanfragen des Berichtsjahres 2024 bezogen sich auf die Internet-Konzerne Meta/Facebook (25 Prozent) und Google (7 Prozent). Rund um Datenschutzverstöße und Data Breaches im medizinischen Sektor, bei Telemedizinanbietern, Arztpraxen und Krankenhäusern, wurden 15 Prozent aller Anfragen gestellt.

Den HmbBfDI erreichten zahlreiche Presseanfragen zu dem für den 26. Juli 2024 bei Meta geplanten Start des KI-Trainings mit Nutzerdaten. Der Konzern hatte einige Wochen vor dem geplanten Trainingsbeginn seine User:innen informiert, dass, sofern sie der Verarbeitung nicht aktiv widersprächen, Nutzerdaten wie etwa persönliche Posts, private Bilder oder Daten aus dem Online-Tracking, die Meta seit 2007 gesammelt hatte, zum Training eines nicht näher definierten KI-Modells verwendet werden würden. Meta berief sich dabei auf ein berechtigtes Interesse gemäß der DSGVO. Als zuständige Datenschutzbehörde für Meta in Deutschland arbeitete der HmbBfDI auf europäischer Ebene aktiv mit den anderen Datenschutzbehörden zusammen, um den Start des Trainings zu verhindern. Dies gelang auch – Meta gab am 14. Juli 2024 bekannt, den Trainingsstart bis auf weiteres zu verschieben. So ist bis Redaktionsschluss innerhalb der EU kein neuer Starttermin für ein Training mit Nutzerdaten durch den Meta-Konzern anberaumt.

Auch das Pay-or-Consent-Modell von Meta, das im November 2023 in der Europäischen Union eingeführt wurde, war im Jahr 2024 immer wieder Gegenstand von Presseanfragen. Vor dem Hintergrund der Einführung des Digital Markets Act (DMA) war dem Konzern

per Beschluss des EDSA vom 27. Oktober 2023 untersagt worden, als Betreiber der Dienste Facebook und Instagram personalisierte Werbung ohne Vorliegen einer entsprechenden Einwilligung auszuspielen. Das daraufhin kurzfristig eingeführte Bezahlmodell stellt die Nutzer:innen vor die Wahl, der Nutzung ihrer personenbezogenen Daten für personalisierte Werbung entweder zuzustimmen oder eine monatliche Gebühr für eine werbefreie Version der Plattformen zu bezahlen. Das Bezahlmodell erntete jedoch einige Kritik. So gab die EU-Kommission 1. Juli 2024 in einer vorläufigen Feststellung bekannt, dass das Pay-or-Consent-Modell von Meta gegen den DMA verstößt, weil es keine gleichwertige, weniger personalisierte Alternative anbietet und das Recht der Nutzer:innen auf freie Einwilligung zur Datenzusammenführung einschränkt. Aus Sicht des EDSA fehlt für eine „echte oder freie Wahl" eine „gleichwertige Alternative, für die keine Gebühr zu entrichten ist, wie etwa die kostenlose Alternative ohne verhaltensbezogene Werbung". Auch hier kam der HmbBfDI seinen Informationspflichten durch die Wahrnehmung diverser Interviews und Presseanfragen nach.

Des Weiteren gab es im Gesundheitswesen zu verschiedenen Verstößen ein verstärktes Presseinteresse: Im Fall des Telemedizinanbieters Dr. Ansay erreichten den HmbBfDI einige Presseanfragen, als im Mai ein schwerwiegendes Datenleck auf der Plattform entdeckt wurde. Über die Suchmaschinen DuckDuckGo und Bing waren zahlreiche Rezepte mit hochsensiblen personenbezogenen Daten öffentlich auffindbar. Ein weiterer Fall betraf den Diebstahl von zwei Servern mit Patientendaten aus den Räumen einer Hamburger Arztpraxis. Auf den Datenträgern der Server waren 100.000 Sätze von Patientendaten hinterlegt. Die Fälle zeigen, dass die Öffentlichkeit im Gesundheitssektor, mit den dort häufig gegebenen hochsensiblen Daten, Datenschutzverstöße besonders interessiert verfolgt.

Die Beispiele zeigen, dass insbesondere überregionale Themen die Pressearbeit bestimmen. 78 Prozent der Anfragen stammen von überregionalen deutschen Medien, wie die nachstehende Tabelle zeigt. Anfragen regional hamburgisch-norddeutscher Medien sind

im Vergleich zum Jahr 2023 von 29 auf 17 Prozent gesunken, ebenso wie die Anfragen von ausländischen Medien von 9 auf 5 Prozent.

Presseanfragen	2022	2023	2024
Regionale Medien	26 %	29 %	17 %
Überregionale Medien	53 %	62 %	78 %
Ausländische Medien	21 %	9 %	5 %

Tabelle1: Presseanfragen beim HmbBfDI 2022, 2023 und 2024

Im Berichtszeitraum 2024 hat der HmbBfDI insgesamt 17 Pressemitteilungen und Website-Informationen veröffentlicht. Zudem haben der HmbBfDI selbst sowie zahlreiche Mitarbeiter:innen der Behörde diverse Vorträge und Präsentationen zu verschiedenen Themen des Datenschutzes gehalten und sich an öffentlichen Gesprächsrunden und Podiumsdiskussionen beteiligt. Auch die Teilnahme an Podcasts ist ein fester Bestandteil der Pressearbeit geworden. Durch den häufig weiter gesteckten Zeitrahmen dieses Formats ist es oft möglich, einen tieferen Einblick in das jeweilige Themengebiet zu geben.

Weiterhin machen die „klassischen" Themen im Datenschutz einen Großteil der presserelevanten Inhalte aus. Jedoch zeichnet sich in Hinblick auf die Automatisierung vieler Arbeitsprozesse durch künstliche Intelligenz ab, dass Fragen nach personenbezogenen Daten im Training und der Anwendung von KI-Modellen in der Presse- und Medienlandschaft immer wichtiger werden. Mit diesem Innovationsschub müssen die Datenschutzbehörden schritthalten, indem sie weitreichend und allgemeinverständlich darüber informieren. In diesem Zusammenhang gewinnen die Kommunikationsmaßnahmen des HmbBfDI weiter an Reichweite und Relevanz, und der HmbBfDI nimmt weiterhin eine strategisch wichtige Rolle in der deutschlandweiten Datenschutz-Kommunikation ein.

2. Öffentlichkeitsarbeit

Die im Oktober 2023 erfolgreich gelaunchte neue Website des HmbBfDI wurde weiter verfeinert. Der Tätigkeitsbericht 2023 konnte erstmals nicht nur in Form eines PDFs digital veröffentlicht werden, sondern auch als HTML-Seite auf der Website, die es ermöglicht, einzelne Kapitel anzuwählen, zu verlinken und auch die Auffindbarkeit von Themen in Suchmaschinen zu steigern.

Ein Schwerpunkt der Öffentlichkeitsarbeit lag in der vertiefenden Aufklärung der Hamburger Bevölkerung über ihre Datenschutzrechte. Ein Faltblatt mit den grundlegenden Informationen über das Recht auf Datenschutz und die zugehörigen Beschwerdemöglichkeiten wurde entwickelt. Dabei stand auch eine neue, ansprechende Bildsprache mit grafischen Illustrationen im Fokus. Der Flyer wurde in einer Auflage von 20.000 Stück produziert und an über 20 Filialen des Hamburg Service, die Hamburger Bücherhallen und die Landeszentrale für politische Bildung Hamburg verteilt. Im Zuge dessen wurde auch ein neues Verteilernetzwerk für die HmbBfDI-Printerzeugnisse mit Kontakten etabliert, das auch für die Distribution künftiger Druckerzeugnisse zur Verfügung steht.

Ein weiteres umfassendes Projekt war die Erstellung einer Handreichung in Kooperation mit der Sozialbehörde. Darin wurden Leitplanken für eine Nutzung von Messenger-Diensten in der Kinder- und Jugendhilfe etabliert. Es konnte eine übersichtliche Checkliste im neuen grafischen Design des HmbBfDI entwickelt werden, die nicht nur staatlichen, sondern auch privaten Trägern der Kinder- und Jugendhilfe in gedruckter und digitaler Form zugänglich gemacht wurde. Zusätzlich wurde der Flyer bei einer digitalen Informationsveranstaltung vorgestellt und die Inhalte bei einer Rückfragerunde vertieft (siehe hierzu Kapitel III 6)

Seit Oktober 2024 besteht die Möglichkeit, in der Stabsstelle Presse- und Öffentlichkeitsarbeit des HmbBfDI ein Freiwilliges Soziales Jahr in Politik und Demokratie zu absolvieren. Seit Herbst unterstützt die erste FSJ-lerin die Stabsstelle sowohl in der Pressearbeit als auch im Bereich der Medienbildung und -kompetenzförderung, insbesondere im laufenden EU-geförderten Projekt #DigitaleVorbilder.

3. Medienbildung

Das EU-Projekt #DigitaleVorbilder hat in zwei Jahren Laufzeit viele Familien mit wertvollen und hilfreichen Tipps versorgt und sie dabei unterstützt, ihre Kinder sicher im Netz zu begleiten. Die Veranstaltungen und entstandenen Bildungsmaterialien stoßen auf große Resonanz bei Familien und Interessierten. Das zeigt, wie wichtig leicht zugängliche, zielgruppenspezifische Formate für die Vermittlung komplexer Themen wie Datenschutz und Medienkompetenz sind.

Im Vorjahr wurde das EU-Projekt **#DigitaleVorbilder – Familien gehen online** ins Leben gerufen. Im zweiten Projektjahr 2024 führte der HmbBfDI zusammen mit der Datenschutzaufsichtsbehörde von Mecklenburg-Vorpommern und dem Medienpartner TIDE verschiedene Veranstaltungsformate durch und entwickelte Bildungsprodukte, die von der Zielgruppe sehr gut angenommen wurden. Im Fokus stand dabei immer der Wunsch, Familien für die digitale Lebenswelt ihrer Kinder und für neue technologische Entwicklung zu begeistern sowie ihnen Hilfestellungen zum Schutz ihrer Privatsphäre aufzuzeigen und sie zu ermutigen, das eigene Mediennutzungsverhalten zu hinterfragen. Das Projekt #DigitaleVorbilder hat sein Hauptziel, das Thema Datenschutz für Familien erlebbar und verständlich zu machen, erreicht. Die zentralen Aktivitäten umfassten Webinare, Medienaktionstage, Elterncafés und Fachtagungen, die durch interaktive Formate und praxisnahe Inhalte positiv zur Medienkompetenzbildung der Teilnehmenden beigetragen haben.

Eltern und Interessierte waren 2024 zu insgesamt zehn Webinaren eingeladen, in denen sie von Fachexpert:innen Informationen zu Themen wie „Kinderbilder im Netz“, „sichere Nutzung von KI“ oder „Rechte & Pflichten im Netz“ erhielten. Im professionell eingerichteten Tonstudio von TIDE gaben Expert:innen den Zuhörenden wertvolle Tipps für den sicheren digitalen Familienalltag an die Hand. Pro Webinar nahmen zwischen 40 und 300 Menschen teil. Alle Webinare wurden durch TIDE aufgezeichnet und durch eine Illustratorin mithilfe sogenannter Graphic Recordings auf ansprechende und verständliche Weise festgehalten. Sie umfassen die Kerninhalte und zentralen Botschaften und können helfen, sich die wesentlichen Aspekte schnell ins Gedächtnis zu rufen.

Das Projektteam besuchte im zweiten Projektjahr insgesamt acht Elterncafés im primären Lebensumfeld von sozioökonomisch benachteiligten Eltern in Hamburg und Mecklenburg-Vorpommern. Diese informellen Treffen waren barrierefrei und niedrigschwellig, sodass Eltern ohne Anmeldeverfahren an der Veranstaltung teilnehmen konnten. Einige Eltern verfügten bereits über Basiswissen, währenddessen andere sich bisher wenig mit datenschutzspezifischen Themen auseinandergesetzt haben.

In Hamburg und Schwerin fanden Anfang Juli jeweils ein Fachtag für pädagogische Fachkräfte statt. Die Teilnehmenden erhielten dort tiefgehende Einblicke in medienpädagogische Themen mit dem Fokus auf die Zusammenarbeit von Schule, (sozial-)pädagogischen Einrichtungen und Familien. Neben Vorträgen wurden Workshops zu datenschutzrelevanten Themen angeboten. Im Familienzentrum Schorsch in Hamburg gab es im Anschluss an den Fachtag eine Podiumsdiskussion mit Vertreter:innen vom HmbBfDI und aus den Bereichen Politik, Wissenschaft und Pädagogik zum Thema „Medienerziehung und Datenschutz“.

Die Website www.digitale-vorbilder.eu weist eine große Fülle an Bildungsmaterialien auf. Alle Videos, mehrsprachigen Kurzclips, Podcasts, Graphic Recordings, Infokarten und die Broschüre sind dort

zur Nachnutzung vorhanden und können auch runtergeladen werden. Über den Medienpartner TIDE sind die Videos, Podcasts und Kurzclips zusätzlich auf YouTube verfügbar. Viele Produkte wurden in verschiedene Sprachen übersetzt, damit möglichst viele Menschen mit den Inhalten erreicht werden können. Außerdem besteht die Möglichkeit, sich auf YouTube Untertitel in noch mehr Sprachen anzeigen zu lassen.

Die umfangreiche Broschüre „Orientierungshilfe Datenschutz: Ein Familien-Guide für den digitalen Dschungel" stößt auf eine sehr hohe Resonanz. Die 80-seitige Broschüre bildet das Herzstück des Projekts, fasst zentrale Themen des Projekts kompakt zusammen und bietet praktische Anleitungen und Hinweise, die direkt im Alltag angewendet werden können. Neben Tipps, was Eltern im Notfall tun können und an wen sie sich neben den Datenschutzaufsichtsbehörden noch wenden können, bietet die Broschüre auch präventive Tipps, um zu verhindern, dass Datenschutzverletzungen überhaupt auftreten. Durch die Mehrsprachigkeit (Englisch, Französisch und Spanisch) erreicht die Broschüre ein breites Publikum.

Mithilfe des Projekts wird der HmbBfDI in vielen lokalen Netzwerken der Medienbildung, bei Bildungsträgern und darüber hinaus verstärkt als kompetenter Partner wahrgenommen, wenn es um die Aufklärung und Bildungsarbeit im Bereich Medienerziehung und Datenschutzbewusstsein geht. Das führt zu vielen Anfragen von Vereinen, Institutionen und auch Privatpersonen, die Expertenwissen benötigen oder aber ihre Datenschutzrechte wahrnehmen wollen. Anfragen für Workshops und Vorträge nehmen daher stetig zu. Teilnehmende gaben häufig das Feedback, nach Besuch der Angebote komplexe Themen mit Datenschutzbezug verständlicher und in der Praxis einfacher umsetzen zu können.

Der HmbBfDI hat sich im Herbst 2024 wiederum erfolgreich um die EU-Fördergelder für ein Folgeprojekt zu #DigitaleVorbilder beworben. Durch die Erfahrungen im ersten Projekt hat sich herausgestellt, dass insbesondere pädagogische Fachkräfte in ihrem be-

ruflichen Alltag viele datenschutzrechtliche Fragen haben. Deshalb richtet sich das Folgeprojekt an Menschen, die im Bereich Pädagogik arbeiten. Es geht also im Jahr 2025 weiter mit Angeboten wie Workshops, Fachtagen und Bildungslunches zu datenschutzrelevanten Themen.

INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT IX.

INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT

1. Statistische Informationen (Zahlen und Fakten)

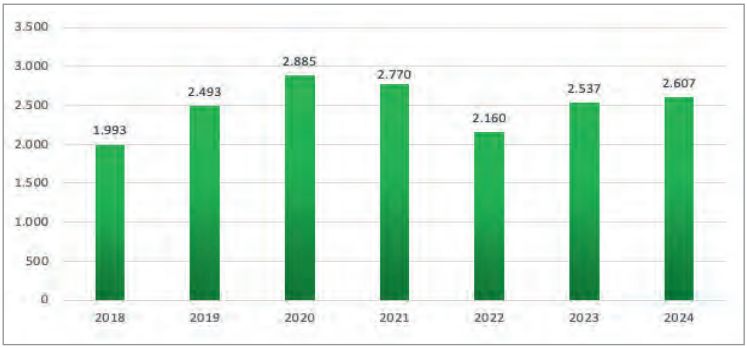
Die datenschutzrechtlichen Eingänge beim HmbBfDI[1] haben im Berichtsjahr 2024 mit 4.237 den entsprechenden Vorjahreswert (4.036) deutlich übertroffen. Ob Beschwerden, Beratungen oder „Datenpannen", die Anzahl der verschiedenen Vorgangsarten beim Datenschutzbeauftragten markierte 2024 Höchstwerte.

Art des Eingangs	Grundlage	Anzahl
Beschwerden Betroffener	Art. 57 Abs. 1 lit. f) DSGVO	2607
Hinweise nicht betroffener Personen		290
Meldungen von Verletzungen des Schutzes personenbezogener Daten	Art. 33 DSGVO	955
Beratung Personen	Art. 57 Abs. 1 lit. e) DSGVO	243
Beratung Verantwortlicher	Art. 57 Abs. 1 lit. f) DSGVO	102
Beratung Behörden	Art. 57 Abs. 1 lit. c) DSGVO	24
Geltungsmachung von Betroffenenrechte ggü. HmbBfDI	Ar. 15 DSGVO	16
		4.237

1.1 Beschwerden und Beratungen

Wie bereits im letzten Tätigkeitsbericht ausgeführt, sind die datenschutzrechtlichen Beschwerden der Kern der Tätigkeit der Beschäftigten des HmbBfDI (Tätigkeitsbericht 2023, Kapitel VIII 1.1). Dies gilt, durch die sich daraus oftmals ergebenen Bußgeld- und Gerichts- sowie den europäischen Verfahren, in qualitativer, insbesondere aber auch in quantitativer Hinsicht. In dieser Hinsicht wurde mit 2.607 Beschwerden im Jahr 2024 wieder ein Spitzenwert und damit das dritthöchste Ergebnis seit 2018 registriert.

[1] Schriftliche Eingänge auf Grundlage datenschutzrechtlicher Normen, d.h. einschließlich Meldungen nach Art. 33 DSGVO, ohne informationsfreiheitsrechtliche Vorgänge.



Beschwerden nach Art. 77 DSGVO beim HmbBfDI seit 2018

Im Vergleich zum Vorjahr sind 2024 auch die schriftlichen Beratungsanfragen von betroffenen Bürger:innen sowie von Behörden gestiegen, während die Anzahl der Beratungen von Unternehmen annähernd gleichgeblieben ist. Auf die prozentuale Verteilung der Beratungsgegenstände hatte das aber nur einen geringen Einfluss.

Schriftliche Beratungen von				
Jahr	**Betroffenen**	**Unternehmen**	**Behörden**	**Gesamt**
2024	243 (66%)	102 (28%)	24 (7%)	369
2023	211 (64%)	103 (31%)	15 (5%)	329

Wie die schriftlichen Beratungen von Unternehmen haben auch die telefonischen Beratungen 2024 mit insgesamt 934 Anrufen ein vergleichbares Niveau wie im Vorjahr (Tätigkeitsbericht 2023, Kapitel VIII 1.2).

1.2 Meldepflicht nach Art. 33 DSGVO

Die Berichterstattung zur Entwicklung der Meldungen von Verletzungen des Schutzes personenbezogener Daten gleicht sich Jahr für Jahr. Grund dafür ist, dass den HmbBfDI in jedem Jahr mehr Meldungen erreichen als im Vorjahr. Die Zahl steigt kontinuierlich an und auch im Jahr 2024 hat sie mit 955 einen neuen Höchststand erreicht. Dabei entstanden die häufigsten „Datenpannen" wieder durch

den sogenannten Falschversand (311 Meldungen), also den Versand eines Briefes oder einer E-Mail an die falsche Person, und vor allem durch erfolgreiche Hackerangriffe, die mit 288 Meldungen 2024 schon rund 30% der Meldungen nach Art. 33 DSGVO ausmachten (im Vorjahr 26%, Tätigkeitsbericht 2023, Kapitel VIII 1.2).

1.3 Abhilfemaßnahmen

Auch in diesem Berichtszeitraum hat der HmbBfDI wieder von seinen verschiedenen Abhilfebefugnissen (Art. 58 Abs. 2 DSGVO) Gebrauch gemacht. Im Einzelnen wurden im Jahr 2024 folgende Maßnahmen ergriffen:

Maßnahme	Rechtsgrundlage	Anzahl 2024
Verwarnungen	Art. 58 Abs. 2 lit. b	22
Anweisungen und Anordnungen	Art 58. Abs. 2 lit. c-g und j	1
Geldbußen	Art. 58 Abs. 2 lit. i	20
Widerruf von Zertifizierungen	Art. 58 Abs. 2 lit. h	1

1.4 Europäische Verfahren

Insbesondere aus datenschutzrechtlichen Beschwerden können sich, wie oben erwähnt, grenzüberschreitende, d.h., europäische Verfahren entwickeln, wenn ein Sachverhalt die Bürger:innen mehrerer europäischer Mitgliedstaaten betrifft. Die Datenschutzaufsichtsbehörde, in deren Land die verantwortliche Stelle ihren Hauptsitz hat, übernimmt dabei – als sogenannte „lead authority" – die Federführung, andere Aufsichtsbehörden, die ebenfalls betroffen sind, werden als „concerned authority" am Verfahren beteiligt.

Im Berichtsjahr 2024 war der HmbBfDI insgesamt an 51 grenzüberschreitenden Fällen beteiligt, davon in 11 Fällen federführend und in 40 Fällen als „concerned authority". Während also die Zahl der Federführungen auf europäischer Ebene im Vergleich zum Vorjahr konstant blieb (Tätigkeitsbericht 2023, Kapitel VIII 1.4), ist die Zahl der Beteiligungen deutlich gestiegen. Die Gesamtzahl der europäi-

schen Verfahren, an denen der HmbBfDI innerhalb eines Jahres beteiligt war, war damit 2024 so hoch wie nie zuvor.

1.5 Stellungnahmen in Gesetzgebungsverfahren (Förmliche Begleitung bei Rechtsetzungsvorhaben)

Auch die Zahl der Stellungnahmen in Gesetzgebungsverfahren hat sich im Berichtszeitraum gegenüber den Vorjahren wieder leicht erhöht (vgl. Tätigkeitsbericht 2023, Kapitel VIII 1.5). Im Jahr 2024 wurde der HmbBfDI im Rahmen von 106 sogenannten Senatsdrucksachenabstimmungen, von denen 54 Rechtsetzungsverfahren zum Gegenstand hatten, um seine Stellungnahme gebeten.

ABKÜRZUNGSVERZEICHNIS
STICHWORTVERZEICHNIS

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für Datenschutz und Informationsfreiheit
BGH	Bundesgerichtshof
BVerfG	Bundesverfassungsgericht
DA	Data Act
DAkkS	Deutsche Akkreditierungsstelle
DDG	Digitale-Dienste-Gesetz
DGA	Digital Governance Act
DSA	Digital Services Act
DSGVO	Datenschutzgrundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DMA	Digital Markets Act
EDSA	Europäischer Datenschutzausschuss
EuGH	Europäischer Gerichtshof
HmbDSG	Hamburgisches Datenschutzgesetz
HmbBfDI	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
IDPC	Irish Data Protection Commission
IMI	Internal Market Information System
OSS	One Stop Shop Mechanismus
OZG	Online-Zugangsgesetz
PolDVG	Gesetz über die Datenverarbeitung der Polizei
SK	Senatskanzlei Hamburg
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UKE	Universitätsklinikum Eppendorf

Stichwortverzeichnis

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z