TÄTIGKEITSBERICHT DATENSCHUTZ 2023

Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Hamburg

32. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

2023

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 (Kristian, KI-generiert)
Layout:	Gebr. Klingenberg & Rompel in Hamburg GmbH
Druck:	Beisner Druck GmbH & Co. KG

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

---

vorgelegt im April 2024
Thomas Fuchs
(Redaktionsschluss: 31. Dezember 2023)

INHALTSVERZEICHNIS

Vorwort

Kein Grund zur Langeweile, es gibt viel zu tun: Der Tätigkeitsbericht 2023 dokumentiert eine große Breite an Themen, mit denen sich unsere Behörde beschäftigt, einen neuen Höchststand an Prüfungen und Beratungen. Aus meiner Sicht ein gutes Zeichen, zeigt die Fülle der Aufgaben doch, dass die fortschreitende Digitalisierung ohne Datenschutz nicht mehr gedacht werden kann und die Verantwortlichen sich dessen immer mehr bewusst werden.

Dies mag auch mit der weiterhin angespannten Bedrohungslage bei Cyberangriffen zusammenhängen, die ein neuer Höchststand bei den gemeldeten Datenschutzverletzungen belegt. Nach 859 Fällen im Vorjahr stieg die Zahl der Data Breach-Meldungen auf insgesamt 925, die Zahl gemeldeter Hackerangriffe auf 235 (im Vorjahr 227). Nur zur Erinnerung: in 2019 hatten wir in Hamburg nur 74 gemeldete Hackerangriffe.

Zudem hat die Zahl der Beschwerdeverfahren wieder zugenommen und liegt mit 2537 deutlich über dem Vorjahreswert von 2160. Der Anstieg ist größtenteils auf eine wachsende Zahl von Beschwerden im Zusammenhang mit Produkten von Meta und Google und die federführende Rolle des HmbBfDI in Deutschland für diese Unternehmen zurückzuführen.

Aber wir arbeiten nicht nur reaktiv und verfahrensgeprägt. Immer stärker kommt die gestaltende Rolle eines auf Lösungen ausgerichteten Datenschutzansatzes zum Tragen und lässt sich an konkreten Projekten ablesen, die in diesem Bericht ausführlich dargestellt werden. Lassen Sie mich drei Beispiele herausgreifen:

Google beschloss im vergangenen Jahr, seinen Dienst **Google Street View** mit neuen Aufnahmen zu aktualisieren. Aufgrund großen

Widerstands gegen die Aufnahmen im Jahr 2010 war der Dienst in Deutschland seitdem nicht mehr erneuert worden, sodass Gebäude jüngeren Datums, wie beispielsweise die Elbphilharmonie, nicht auffindbar waren. Konnte dies nun unter Wahrung der Datenschutzrechte gelingen? Ja, weil wir mit Google frühzeitig klare Regeln vereinbarten, die das Recht der Bürger:innen auf informationelle Selbstbestimmung, in diesem Fall die Weigerung, das eigene Haus abbilden zu lassen, durch ein umfassendes frühzeitiges Widerspruchsrecht sicherten, und dem Unternehmen zugleich die Nutzung der geduldeten Bilder ermöglichten.

Ein zweites Beispiel: Die deutsche Datenschutzkonferenz, der Zusammenschluss der deutschen Aufsichtsbehörden, hat, basierend auf einem von Hamburg entwickelten Vorschlag, im letzten Jahr die Zulässigkeit sogenannter **Pur-Abo-Modelle** beschlossen, wenn diese auf klaren Rahmenbedingungen basieren. Dies ermöglicht Nutzer:innen den Zugang beispielsweise zu Angeboten von Zeitungsverlagen, ohne ihre personenbezogenen Daten zur Verarbeitung zu Werbezwecken preisgeben zu müssen. Das Modell wird nun auch in Europa diskutiert, insbesondere aufgrund der Einführung einer Variante durch Meta.

Drittens: Als erste Datenschutzaufsichtsbehörde hat der HmbBfDI eine **Checkliste für den Einsatz von LLM-Chatbots**, also ChatGPT und Co., herausgegeben. Viele Fragen beim Einsatz dieser Modelle sind noch offen, vom Datenschutz bis zum Urheberrecht. Aber die meisten Unternehmen und Behörden wollen mit dem Einsatz von LLM-Chatbots natürlich nicht warten, bis diese Fragen geklärt sind. Daher war es uns wichtig, auf Mindeststandards hinzuweisen, um den Schutz personenbezogener Daten bei der Verwendung dieser Modelle zu gewährleisten. Viele Unternehmen nutzen den Leitfaden inzwischen als Basis für interne Richtlinien.

Darüber hinaus haben wir Verbesserungen für Wohnungssuchende beim Umfang von Makler-Fragebögen, deutlich mehr Transparenz und Datenschutz bei großen Shopping-Portalen und nicht zuletzt eine datensparsamere Variante der Sicherheitskontrollen im Zusammenhang mit der Gruppenauslosung für die Fußball-Europameisterschaft 2024 in der Elbphilharmonie erreichen können.

Mir sind diese Beispiele wichtig. Verfahren und Bußgelder sind oft notwendig und stärken unsere Position, aber sie ersetzen nicht den ergebnisorientierten Dialog mit den Verantwortlichen. Ziel unserer Arbeit sind konkrete Verbesserungen für den Datenschutz, und damit für die Grundrechte der Hamburger:innen. Aber lesen Sie selbst!

Thomas Fuchs

I. EINLEITUNG

Einleitung

Und jetzt auch noch KI – Vom Recht auf Privatheit zum Schutz vor Kontrollverlust

Deutschland digitalisiert sich – noch mit Mühe. Während der Staat Faxgeräte entsorgt und bürgernahe Verwaltungsleistungen digitalisiert, lädt 2023 die „KI" zum radikalen Wandel ein.

Inmitten eines Diskurses um Weg und Ziel unserer digitalen Transformation werden Tatsachen geschaffen. Unternehmen und Behörden überlegen, planen und integrieren KI-Produkte in ihre Prozesse und Systeme – auch um die Versäumnisse einer lahmenden Digitalisierung zu überspringen. Die zentrale regulatorische Frage dieser Zeit ist, wie Bürger:innen vor den Gefahren des Fortschritts zu schützen sind, ohne dessen Potenzial zu ersticken: In welchem Rahmen sollte KI für Gesellschaft und Wirtschaft wirken dürfen?

Vollkommen neu ist das alles nicht: Vor knapp 30 Jahren regelte das europäische Datenschutzrecht schon die Zulässigkeit automatisierter Entscheidungssysteme; mit der DSGVO seit 2018 harmonisiert und unionsweit. In einer bis vor kurzem etwas unterschätzten Norm, Art. 22 DSGVO, steht in schönster Klarheit, dass niemand es hinnehmen muss, gegen seinen Willen automatisierten Entscheidungen ausgesetzt zu sein, die ihm oder ihr gegenüber rechtliche Wirkungen entfalten.

Die Beeinflussung durch automatisierte (Vor)-Entscheidungen

Der EuGH hat Ende 2023 in der sog. Schufa-Entscheidung dieser Regelung Wirkmacht verliehen. Der Gerichtshof hat klargestellt, dass dieses Verbot auch für prägende automatisierte Vorentscheidungen gilt. Wenn eigentlich der Algorithmus entscheidet und die nachgelagerte menschliche Entscheidung eine reine Formalität ohne eigene Kontrolle ist, greift das Datenschutzrecht gleichermaßen. Dies ist bei Schuldnerbewertungen („Scores") durch Auskunfteien im Regelfall anzunehmen. Es gilt aber ebenso, wenn Banken, Versicherungen oder Online-Händler:innen ausschließlich auf Basis eines maschinengesteuert erstellten Scores die Bonität potenzieller Kund:innen prüfen und davon ihre Entscheidung für den Vertragsschluss abhän-

gig machen. Auch in der Personalverwaltung dürfen Einstellungen nicht nur von einem abstrakten Score abhängig gemacht werden.

Es muss also noch eine eigene, menschliche Prüfung dazwischengeschaltet werden. Diese Stelle muss in der Lage sein, den vorangegangenen automatisierten Entscheidungsprozess zu verstehen, um zu beurteilen, ob die „Vorentscheidung" den konkreten Einzelfall angemessen auswertet. Sie muss erkennen können, ob ein zufälliger Systemfehler oder eine algorithmische Diskriminierung greifen – um diese im Notfall zu übersteuern. Diese Anforderungen sind kein Selbstzweck: Wenn Betroffene den weitläufigen datenschutzrechtlichen Auskunftsanspruch geltend machen, müssen Unternehmen wie Behörden in der Lage sein, Fragen nach der Logik und Tragweite der automatisierten Entscheidung zu beantworten.

Die Messlatte liegt hoch, ist aber bei solchen Scoring-Tools noch zu bewerkstelligen. Doch wie kann man die Logik und Tragweise eines Systems erläutern, das als sog. Blackbox funktioniert – wenn keiner im Einzelfall die Ursache für das Resultat auf eine bestimmte Anweisung nachvollziehen kann? Es wird darum gehen, Wissen und Nichtwissen über die Funktionsweise von Blackbox-Systemen wie Large Language Models transparent zu erläutern. Im Gleichlauf zu deren rasanter Entwicklung bedarf es der Aneignung profunder Kenntnisse, die notwendig sind, um die Funktionsweise der eingesetzten Sprachmodelle im Einzelfall nachzuzeichnen. Die Herausforderung für Unternehmen und Behörden, die ChatGPT oder Google Gemini nutzen, wird sein, diesen Einblick in proprietäre Systeme zu erhalten, die Informationen zu verstehen und ihren Einsatz risikogerecht anzupassen.

Insofern ist der leichtfertige Einsatz, insbesondere in Bezug auf konkrete Personen, äußerst kritisch zu sehen. In unserer Checkliste für die Nutzung von LLM-Chatbots heißt es deshalb, dass weder die Eingabe personenbezogener Daten noch die Ausgabe personenbezogener Daten beim Einsatz dieser Modelle rechtssicher möglich ist. Dies gilt auch für personenbeziehbare Daten. Es reicht also nicht, Namen

und Anschrift wegzulassen. Auch Informationen, die im Zusammenhang Rückschlüsse auf Betroffene zulassen, sind problematisch.

Die hinter diesen konkreten Fragestellungen stehende Abwägung von Grundrechtsschutz und Innovation prägt schon jetzt unsere Praxis im Gespräch mit Behörden und Unternehmen.

Die KI-Verordnung – wie wird sie die Praxis prägen?
Nun kommt mit der europäischen KI-Verordnung noch ein weiterer Rechtsrahmen dazu. Sie regelt den Marktzutritt sowie den Einsatz von KI-Systemen. Neben dem Verbot bestimmter KI-Systeme liegt das Hauptaugenmerk auf der Regulierung von zwei Arten von KI: Hoch-Risiko-Systeme in besonders grundrechtsensiblen Bereichen und universal einsetzbare KI-Systeme bzw. Modelle (etwa: Large Language Models und hierauf gebaute Chatbots). Hier sind bestimmte Regeln zu beachten.

Die Einführung und Nutzung solcher Systeme und die Einhaltung der Regeln unterliegen der behördlichen Aufsicht. Vor Markteintritt ist zu prüfen, ob ein System normkonform ist. Danach wird insbesondere ihre Anwendung in Unternehmen und Behörden durch „Marktaufsichtsbehörden" überwacht. Die KI-VO entwickelt damit den Schutz der DSGVO durch ein Marktüberwachungsregime fort. Die Aufsicht umfasst konkrete Risiken von KI-Produkten: Gefährdungen für Leben, Gesundheit, Berufsausübung und Freiheit sollen beobachtet und KI-Produkte ggf. vom Markt genommen werden.

Bis Mitte 2025 muss der deutsche Gesetzgeber diese Verordnung in großen Teilen umsetzen. Dabei ist unter anderem zu klären, wer für die Aufsicht zuständig ist. Meines Erachtens kommen für die Aufsicht über die Anwendung von KI-Systemen nur die Datenschutzaufsichtsbehörden in Betracht. Sie regulieren schon jetzt deren Einsatz, soweit die KI eine Variante der automatisierten Einzelfallentscheidung ist. Zudem sind KI-Anwendungen nur ein Produkt von vielen innerhalb der IT-Systemlandschaften von Unternehmen und Behörden. Sie werden nicht für sich alleinstehen und ohnehin Gegenstand von

Datenschutzfolgeabschätzungen sein. Das KI-Produktrisiko-Assessment wird hiervon nicht getrennt werden können. Diese Synergie sollte auf eine spiegelbildlich einheitliche Regulierung mit erfahrenen Ansprechpartner:innen treffen. Jedenfalls dürfte kein Unternehmen Interesse daran haben, eine weitere Aufsichtsbehörde neben der Datenschutzbehörde in seine Systeme blicken lassen zu müssen.

Grundrechtsschutz im Wege der Produktregulierung

Vor allem: Am Ende wird beim konkreten Einsatz von KI-Anwendungen über den Ausgleich von technologischer Innovation und Grundrechtsschutz der Bürger:innen entschieden. Zwar wird ein Produkt durch Marktüberwachung reguliert, doch dahinter steckt dieselbe Frage wie bei der automatisierten Einzelfallentscheidung: Wie können Menschen vor grundrechtsrelevanten Systemen geschützt werden, die sie nicht mehr nachvollziehen können? Marktüberwachung beim Einsatz von KI-Anwendungen ist also Grundrechtsschutz im Wege der Produktregulierung – der den Datenschutzaufsichtsbehörden bekannte Schutz der Privatheit ergänzt um Folgen für Leib, Leben und Freiheit. KI-Regulierung ist kein Selbstzweck: Ziel ist die Gewährleistung unserer Grundrechte in der fortschreitenden digitalen Transformation!

PRÜFUNGEN II.

Prüfungen

1. Prüfungen im Sicherheitsbereich

Im Berichtszeitraum 2022 hat der HmbBfDI mehrere beschwerdeunabhängige Prüfungen bei der Polizei Hamburg eingeleitet, durchgeführt und/oder abgeschlossen. Der HmbBfDI hat sich an einer gemeinsamen und koordinierten Kontrolle der Übermittlung von personenbezogenen Daten Minderjähriger ins europäische Ausland durch die Polizei angeschlossen (1.1). Im Jahr 2023 konnte der HmbBfDI die gesetzlich vorgeschriebenen turnusmäßigen Pflichtprüfungen, sowohl aus dem Gesetz über die Datenverarbeitung der Polizei (1.2) als auch aus dem Antiterrordateigesetz bzw. Rechtsextremismusdatei-Gesetz (1.3.) abschließen. Begonnen wurde mit der Prüfung im polizeilichen Auskunftssystem POLAS (1.4.).

1.1 Übermittlungen im Anwendungsprogramm SIENA

*Im Berichtszeitraum hat der HmbBfDI die Übermittlung von Daten Minderjähriger durch die Polizei Hamburg über das EUROPOL-Anwendungsprogramm SIENA (**S**ecure **I**nformation **E**xchange **N**etwork **A**pplication) geprüft. Bei dieser gemeinsamen und koordinierten Kontrolle mit anderen datenschutzrechtlichen Aufsichtsbehörden erhielt der HmbBfDI durch das LKA 19 einen umfassenden Einblick in den überstaatlichen polizeilichen Informationsaustausch.*

Der Europäische Datenschutzbeauftragte (EDSB) als Datenschutzaufsichtsbehörde über Europol ist an den Bundesbeauftragten für Datenschutz und die Informationsfreiheit (BfDI) und an den zuständigen Landesvertreter zum Thema Europol im Coordinated Supervision Committee (CSC) herangetreten mit der Bitte, die Übermittlung personenbezogener Daten Minderjähriger durch deutsche Behörden über SIENA zu prüfen.

Das von Europol gehostete Anwendungsprogramm SIENA kann zum polizeilichen Informationsaustausch mit anderen EU-Mitglied-

staaten, Europol sowie an das System angeschlossen Drittstaaten genutzt werden. Dabei dient das System der (ersten) Kontaktaufnahme im Hinblick auf Personen oder Sachverhalte. Es handelt sich dabei nicht um einen automatischen Zugang zu europäischen Datenbanken oder Erkenntnissen von anderen Polizeibehörden. Anfragen zum Zwecke der Straftatermittlung dürfen nur direkt an Europol gesendet werden, wenn die Anfragen in Verbindung mit Straftaten stehen, die in der Zuständigkeit von Europol liegen (vgl. Art. 3 Abs. 1 der Verordnung (EU) 2016/794 (Europol-Verordnung)).

Out-of-Europol-mandate-requests (d.h. Anfragen die in Verbindungen mit Straftaten stehen, die nicht in den Zuständigkeitsbereich von Europol fallen) können bilateral zwischen Mitgliedstaaten gemäß den nationalen gesetzlichen Bestimmungen des jeweiligen Mitgliedstaats erfolgen.

Um den einzelnen Aufsichtsbehörden eine Überprüfung der Nutzung von SIENA durch die Polizeibehörden zu ermöglichen, wurde seitens des EDSB die Statistik des webbasierten Nachrichtenportals SIENA zur Verfügung gestellt. Anhand der übermittelten Tabelle konnte nachvollzogen worden, ob mittels SIENA-Nachrichten Daten Minderjähriger aus Deutschland an andere Stellen übermittelt wurden. Gegenstand der gemeinsamen Kontrolle sollten die Daten Minderjähriger sein, die gemäß des Anhangs II B. der Europol-Verordnung als „Verdächtige“ oder „künftige potenzielle Straftäter“ eingestuft werden. Dabei waren die Richtigkeit der übermittelten Daten sowie die Überprüfung der Rechtmäßigkeit der Übermittlung Gegenstand der Kontrolle.

Anhand der Tabelle konnte festgestellt werden, dass auch von der Polizei Hamburg in mehreren Fällen Daten von vermeintlich Minderjährigen über das Anwendungsprogramm ins Ausland übermittelt wurden. Daten von Minderjährigen sind besonders sensibel, eine Weitergabe von diesen personenbezogenen Daten erfordert daher auch eine strenge Verhältnismäßigkeitsprüfung.

Nach Sichtung der Dokumentation und Erläuterungen durch die Polizei Hamburg konnten aber keine datenschutzrechtlichen Bedenken an der Übermittlung der personenbezogenen Daten festgestellt werden:

Im Rahmen der Prüfung stellte sich heraus, dass sämtliche Übermittlungen aus Hamburg vom LKA 19 veranlasst wurden. Beim LKA 19 handelt es sich um eine feste Dienststelle des Landeskriminalamtes, die aus der Sonderkommission „Castle" hervorgegangen ist und alleine der Bekämpfung und Ermittlung von Einbruchskriminalität in Hamburg dient.

Bei den vom HmbBfDI geprüften Fällen handelte sich allesamt um verdächtige Personen, die durch die Polizei Hamburg im Zusammenhang mit Einbruchdiebstählen aufgegriffen wurden und die teilweise nicht über Ausweispapiere verfügten. Dabei gaben die Verdächtigen zudem gegenüber der Polizei an, unter der Strafmündigkeitsgrenze von vierzehn Jahren zu liegen bzw. noch nicht volljährig zu sein. Die Polizei konnte gegenüber dem HmbBfDI darlegen, dass bei den Verdächtigen allerdings erhebliche und nachvollziehbare Zweifel an der Altersangabe bestanden. Dies und die Feststellung, dass es sich nicht selten um europaweit operierende Gruppen in diesem Deliktsbereich handelt, sei nach Angaben des LKA 19 keine selten anzutreffende Konstellation. Die Abfrage von europaweiten Kenntnissen sei somit essentiell für die Straftatermittlung im Bereich der Einbruchdiebstähle.

Da auch hier Anhaltspunkte vorlagen, dass die Personen ihren Wohnsitz bzw. ihren ständigen Aufenthalt in der Europäischen Union haben, wurde SIENA durch die Polizei Hamburg genutzt , um andere europäische Polizeibehörden (hier: Frankreich, Italien und Kroatien) zu kontaktieren, um die Einleitung/Fortführung von Ermittlungsverfahren voranzutreiben. Da die Betroffenen sich teilweise sogar in Untersuchungshaft befanden, war die Frage der Identitätsfeststellung auch besonders dringend, um eine beabsichtigte Zuführung der Person vor dem Amtsgericht Hamburg durchzuführen. Andere

Maßnahmen zur Altersbestimmung stellen dabei kein milderes Mittel dar. Auch wurden lediglich an die Staaten personenbezogene Daten übermittelt, bei denen ein Hinweis über Informationen vorlag. Eine pauschale europaweite Übermittlung ist nicht erfolgt.

1.2 ATD und RED Kontrolle

Der HmbBfDI hat bei der Polizei Hamburg (LKA 7 – Staatschutzabteilung) eine Vor-Ort-Prüfung der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) durchgeführt. Neben der Prüfung der technischen Rahmenbedingungen 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 am 5.9.2023 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 (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 sehr schwach ausgestaltet sei. Dies werde durch aufsichtsrechtliche Kontrolle kompensiert. 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 dritte Prüfung des HmbBfDI der fraglichen Dateien beim LKA Hamburg.

Sowohl bei der ATD als auch der RED handelt es sich um gemeinsame, standardisierte und zentrale Dateien, die jeweils von verschiedenen Sicherheitsbehörden des Bundes sowie der Landes-

kriminalämter und der Verfassungsschutzbehörden der Länder 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, trägt die Behörde, die die Daten eingegeben hat (vgl. § 9 Abs. 1 Satz 1 RED-G bzw. § 8 Abs. 1 Satz 1 ATDG).

Bei den (stichprobenhaft) geprüften betroffenen Personen aus der RED und der ATD wurden Voraussetzungen für deren Speicherungen dargelegt und erläutert. 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 konnten nicht festgestellt werden. Aufgrund des Geheimhaltungsgrads sind detaillierte Ausführungen über den Inhalt der Dateien nicht möglich.

Ähnlich wie der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) gelangt der HmbBfDI im Rahmen seiner Prüfung aber wiederholt 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 (vgl. BfDI 28. Tätigkeitsbericht, S. 52 ff.).

1.3 Abschluss der Pflichtprüfung von verdeckten und eingriffsintensiven Maßnahmen nach dem PolDVG

Der HmbBfDI konnte die im Jahr 2022 begonnenen Prüfungen der heimlichen und eingriffsintensiven Maßnahmen für die Jahrgänge 2019 bis einschließlich 2022 im Laufe des Jahres 2023 nunmehr abschließen. Wie schon im vorigen Bericht angedeutet, stellte der HmbBfDI hierbei keine gravierenden materiellen Mängel fest: Bei den geprüften Einzelmaßnahmen drängte sich in keinem Fall der Verdacht auf, dass diese insgesamt rechtswidrig sind.

Nach § 73 PolDVG hat der HmbBfDI die Einhaltung der gesetzlichen Vorschriften über die Verarbeitung von personenbezogenen Daten nach den §§ 20 bis 31 und 50 PolDVG (verdeckte Maßnahmen zur Gefahrenabwehr wie z.B. die Observation und die Telekommunikationsüberwachung) im Abstand von höchstens zwei Jahren bei der Polizei Hamburg zu kontrollieren. Aufgrund der seit dem 24.12.2019 geltenden Übergangsbestimmungen in § 78 Abs. 3 PolDVG hatte der HmbBfDI zum 1.1.2022 erstmals mit der Prüfung begonnen. Die Prüfungen wurden durch gravierende Mängel bei der Protokollierung der verdeckten Maßnahmen erheblich erschwert. Eine Prüfung der einzelnen Maßnahmen konnte im Berichtszeitraum 2022 daher nicht beendet werden. Auch eine Prüfung des neu etablierten Protokollierungsprozesses und der Benachrichtigung der Betroffenen stand noch aus (vgl. 31. TB Datenschutz 2022, S. 18 ff.).

Während der im Jahr 2023 durchgeführten Nachkontrollen wurden Maßnahmen aus dem Zeitraum 1.7.22 bis 31.12.22 geprüft, um einen vollständigen Überblick über das Jahr 2022 zu erhalten. Hierfür wurden neben der Sichtung zahlreicher Unterlagen auch zwei Vor-Ort-Termine durch Mitarbeitende des HmbBfDI im Polizeipräsidium wahrgenommen, bei denen ebenfalls die neue Papierprotokollierung in Augenschein genommen wurde und im zweiten Termin

dann eine daraus gebildete Stichprobe gesichtet wurde. Bei dieser Gelegenheit konnten auch Unstimmigkeiten hinsichtlich einiger gesichteter Anordnungen zu Maßnahmen aus dem ersten Halbjahr 2022 durch Einsicht in die Akten ausgeräumt werden.

Insbesondere wurde bei der Stichprobenziehung für das zweite Halbjahr 2022 darauf Wert gelegt, dass diese auch Bestandsdatenauskünfte des LKA enthielt. Diese wären durch die Polizei Hamburg mangels Protokollierung für das erste Halbjahr 2022 nur mit händischer Nachsuche auffindbar gewesen. Im zweiten Halbjahr zeigten sich bei den geprüften Maßnahmen keine berichtenswerten Auffälligkeiten.

Nachdem die Polizei Hamburg im Zeitraum vom 24.12.2019 bis 30.6.2022 ihrer Pflicht zur Protokollierung der Maßnahmen nach § 64 PolDVG nicht nachkam, wurden für den Zeitraum 1.1.2022 bis 30.06.2022 für einige Maßnahmen nachträglich Protokollierungen angefertigt und für den Zeitraum ab 1.7.2022 eine Protokollierung in Papierform durch manuelle Erstellung von Formularen und deren Sammlung an zentraler Stelle vorgenommen.

Der HmbBfDI geht jedoch auch weiterhin davon aus, dass die Regelung des § 64 PolDVG ihrem Sinn und Zweck nach zur Sicherstellung von Revisionsfähigkeit und Vollständigkeit eine digitale Lösung verlangt und die Papierlösung allenfalls ein Provisorium darstellt, das den Vorgaben des Rechts weiterhin nicht umfassend genügt (vgl. 31. TB Datenschutz 2022, S. 20 ff.)

Ebenfalls datenschutzrechtlich bedenklich stellte sich im Berichtszeitraum 2022 die Benachrichtigung der Polizei Hamburg gegenüber den Betroffenen dar. Nach Abschluss der verdeckten Maßnahmen durch die Polizei sind die Betroffenen in den gesetzlich vorgeschriebenen Fällen in der Regel über die Maßnahmen zu unterrichten. Die Benachrichtigungen genügten jedoch mit dem verwendeten Formular K170d nicht den gesetzlichen Vorgaben des § 68 PolDVG (vgl. 31. TB Datenschutz 2022, S. 26 ff.). Dies dürfte zumindest den

Zeitraum 24.12.2019 bis 30.6.2022 betreffen. Die finale Neubearbeitung des Formulars wurde dem HmbBfDI nach Fertigstellung am 7.9.23 vorgelegt. Es schafft deutliche Verbesserungen, enthält aber weiter diskussionswürdige Formulierungen. Dies wurde der Polizei Hamburg bereits mitgeteilt und ein Austausch für die weitere Überarbeitung angeboten. Als problematisch kann weiterhin das Fehlen der Kontaktdaten des HmbBfDI angesehen werden: Hier wurde sich für eine Linklösung entschieden. Das Formular verweist pauschal auf die Website der Polizei Hamburg und die Möglichkeit, dort die Datenschutzbestimmungen aufzurufen. § 68 Abs. 1 Nr. 1 lit. e) PolDVG verlangt aber sehr konkret Angaben zur „Erreichbarkeit der oder des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit". Diskutabel ist zudem, wie genau für den Adressaten die Art der Maßnahme zu umschreiben ist. § 66 Abs. 1 PolDVG verlangt als Umsetzung der Transparenzanforderungen aus Art. 12 Richtlinie (EU) 2016/680 eine klare, verständliche Sprache. Da das überarbeitete Formular neben der Nennung der jeweiligen Überschrift der Norm auch noch ein erläuterndes Freitextfeld vorsieht, wird auf die Verwendung dieses Felds ein besonderer Fokus in den zukünftigen Prüfungen zu legen sein.

1.4 Prüfung POLAS

Im Berichtszeitraum hat der HmbBfDI mit der Prüfung des Polizeilichen Auskunftssystems POLAS begonnen. Schwerpunkt sollen u.a. die Voraussetzungen der Speicherung und die sog. Personengebundenen Hinweise (PHW) darstellen.

Das Polizeiliche Auskunftssystem POLAS dürfte (neben dem reinen Vorgangsbearbeitungssystem der Polizei) die wohl größte und meistgenutzte Datei der Polizei Hamburg darstellen. Es 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.

Voraussetzung für die suchfähige Speicherung einer Person in POLAS für die Dauer von zwei Jahren ist, dass gegen diese Person ein strafrechtliches Ermittlungsverfahren eingeleitet worden ist. Entfällt der dem Ermittlungsverfahren zugrundeliegende Verdacht, sind die Daten zu löschen. Eine weitere Speicherung über die zwei Jahre hinaus ist nur zulässig, soweit eine Negativprognose hinsichtlich der Begehung weiterer Straftaten gestellt werden kann (§ 36 Abs. 2 Satz 4 PolDVG). Diese Negativprognose ist vom Sachbearbeitenden der Kriminalpolizei zu erstellen und hinreichend darzulegen. Hierbei muss durch konkrete Tatsachen belegt werden, dass der Beschuldigte nach kriminalistischer Erfahrung erneut strafrechtlich in Erscheinung treten wird.

Hier kam es hier bereits in der Vergangenheit zu erheblichen Problemen (vgl. 26. TB Datenschutz 2016/2017, S. 32 – zu § 16 PolDVG a.F.). Bei einem nicht unwesentlichen Teil der dort überprüften Stichproben lag die für die Speicherung erforderliche Negativprognose nicht oder nicht ausreichend vor oder war nicht ausreichend dokumentiert. Zudem wurde der Ausgang des Strafverfahrens bzw. der Wegfall des Verdachts bei mehreren Einträgen nicht berücksichtigt. Nicht endgültig aufklärbar war im Rahmen dieser Prüfung, ob dafür letztendlich organisatorische Mängel bei der Polizei Hamburg oder die Übermittlung durch die Staatsanwaltschaft Hamburg ausschlaggebend gewesen ist (26. TB Datenschutz 2016/2017, S. 33 f.).

Im Berichtszeitraum wurden nun durch den HmbBfDI zunächst Informationen zur Weiterentwicklung der Schnittstellen zwischen Staatsanwaltschaft und Polizei seit der letzten Prüfung angefordert. Dem HmbBfDI wurde abstrakt eine erhebliche Verbesserung sowohl der Schnittstelle als auch der Einzelfallprüfung geschildert: Es soll ein neues technisches Verfahren die sog. „Arbeitsrate POLAS/KAQS“ geschaffen worden sein. Durch Änderungen an den Schnittstel-

len wird seit dem 1.1.2018 bei Verfahrenseinstellungen durch die Staatsanwaltschaft Hamburg neben der Einstellungsentscheidung auch eine von insgesamt zehn Untererledigungsarten mitgeteilt, die über die weitere Speicherung entscheiden.

Ausgehend hiervon wurde durch den HmbBfDI in eine Prüfung der einzelnen konkreten Speicherungen von Personen übergeleitet. Dabei wurde ein weiter gefasster Prüfungsansatz gewählt, da die Bildung einer geeigneten Stichprobe aufgrund der Masse an gespeicherten Einstellungsentscheidungen Schwierigkeiten bereitet. Ansatzpunkt für die Stichprobe waren daher zunächst nicht die Speicherungen nach § 36 Abs. 2 Satz 4 PolDVG selbst, sondern die sog. Personengebundenen Hinweise (PHW).

Personengebundene Hinweise sind Hinweise auf Besonderheiten einer natürlichen Person, wie z.B. „Gewalttätig“ oder „Bewaffnet“, aber auch „Ansteckungsgefahr“ und „Psychische und Verhaltensstörung“, die bei Abruf einer Person im bundesländerübergreifenden Informationssystem der Polizeien (INPOL) und/oder dem landesrechtlichen polizeilichen Auskunftssystem (hier: POLAS) gut sichtbar und hervorgehoben angezeigt werden. Diese Warnhinweise sollen ausschließlich dem Schutz des Betroffenen und der Eigensicherung von Polizeibediensteten dienen und nicht lediglich auf gegebenenfalls vorliegende Vorstrafen hinweisen. 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 BKA für die Vergabe der PHW ein bundeseinheitlicher Leitfaden vergeben, 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).

Der HmbBfDI hat sich nun in einem ersten Schritt entschieden, die PHW „Psychische und Verhaltensstörung“, „Gewalttätig“ und „Betäubungsmittelkonsument“ zu überprüfen.

Insbesondere die Eintragung „Psychische und Verhaltensstörungen“ erfolgte nach Erkenntnissen anderer Aufsichtsbehörden bei vielen Länderpolizeien vorschnell: Derartige Eintragungen verlangen die Erfüllung festgelegter Vergabekriterien, die bundeseinheitlich in einem Leitfaden des Bundeskriminalamtes definiert werden. Auch die anderen beiden genannten PHW sind problembehaftet, hier jedoch nicht wegen der hohen Eintragungsvoraussetzungen, sondern gerade wegen der Auslegungsspielräume zur Frage der Eigensicherung von Beamten. So darf der PHW „Betäubungsmittelkonsument“ nur dann vergeben werden, wenn die zu diesem PHW festgeschriebenen Kriterien erfüllt sind. 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 BtM gefunden wurden, die geschluckt oder geraucht werden.

Durch die Polizei Hamburg wurde für den HmbBfDI zunächst eine Liste derjenigen Personen erstellt, die in POLAS mit den genannten PHW hinterlegt sind.

Zu einer ersten Stichprobe von 89 Personen (ca. 1% der Speicherungen) wurden sodann bei der Polizei Hamburg diverse weitergehende Informationen angefordert.

Aufgrund der Menge der Unterlagen ist mit einer Übersendung durch die Polizei Hamburg erst im Frühjahr 2024 zu rechnen. Über den Weitergang der Prüfung wird der HmbBfDI zukünftig berichten.

2. Data Breach bei der Hochschule für Angewandte Wissenschaften (HAW)

Zunehmende Cyber-Angriffe stellen verantwortliche Stellen vor Herausforderungen in Bezug auf die Sicherheit personenbezogener Daten und werfen verschiedene Fragen der datenschutzrechtlichen und technischen Bewältigung der Folgen auf.

Wie aus der Presse bekannt, wurde die Hochschule für Angewandte Wissenschaften (HAW) zwischen den Jahren 2022 und 2023 Opfer eines Ransomware-Angriffs. In dessen Folge wurden personenbezogene Daten von Studierenden, Beschäftigten, Bewerbenden und weiteren Betroffenen durch die Angreifer unzugänglich gemacht. Im Zuge des Ransomware-Angriffs erfolgte auch ein Datenabfluss von nicht genau bekanntem Umfang. Teile der so abgeflossenen Daten wurden später im Darknet veröffentlicht.

Um die Betroffenen über die individuellen und konkreten Risiken aus der Darknet-Veröffentlichung gemäß Art. 34 DSGVO zu benachrichtigen, sah es die HAW zunächst als geboten an, die Darknet-Veröffentlichungen zur Feststellung der Art der Daten sowie der jeweils konkret Betroffenen zu sichten. Dies schien erforderlich, da ohne weiteres nicht bekannt war, welche Daten veröffentlicht wurden. Die Art der Daten war auch deshalb nicht abzuschätzen, da unter den vom Ransomware-Angriff betroffenen Daten auch solche aus persönlichen Laufwerken waren, und somit von potentiell unbekannten Daten und Daten aus privater Nutzung ausgegangen werden musste. Der HAW ging es dabei auch um die Identifizierung von Daten hochschulfremder Dritter in den privaten Datensammlungen, die ggf. ebenfalls als Betroffene zu behandeln und zu informieren gewesen wären. Damit waren beispielsweise personenbezogene Daten Dritter gemeint, die in privaten E-Mails von Beschäftigten der Hochschule enthalten und auf den persönlichen Laufwerken von Beschäftigten oder Studierenden abgelegt waren.

In intensivem Austausch zwischen HmbBfDI und HAW wurde der Umfang der Benachrichtigungspflicht erörtert und die Frage diskutiert, ob die HAW als Verantwortliche abgeflossene Daten für eine Benachrichtigung nach Art. 34 DSGVO inhaltlich untersuchen muss und darf.

Der HmbBfDI sieht grundsätzlich die Auswertung von Daten kritisch, die definitiv oder potentiell aus persönlichen Dateiablagen stammen, auf die seitens der Hochschule im regulären Nutzungszustand kein uneingeschränktes Zugriffsrecht besteht. Hat der Verantwortliche den Betroffenen auch eine Nutzung der IT-Systeme zu privaten Zwecken gestattet, so ist im Falle eines Data Breach für diese Daten besonders zu verfahren und insbesondere die unberechtigte Kenntnisnahme dieser Inhalte bei der Incident Response zu vermeiden.

Generell sollten alle Daten, deren Art und Inhalt ein Verantwortlicher nicht bestimmt oder kontrolliert, in diesem Sinne behandelt werden, das heißt die insbesondere auch nicht Gegenstand einer ordentlichen Verfahrensdokumentation i.S.d. Art. 30 DSGVO sind.

Insbesondere zeichnen sich diese Daten dadurch aus, dass der Verantwortliche regelhaft weder Kenntnis hat über die Art der personenbezogenen Daten, den Zweck der Verarbeitung oder die Kategorien der Betroffenen – hier kann es sich um mögliche Dritte handeln, die in keinem Verhältnis zum Verantwortlichen selbst stehen. Im Sinne von Art. 11 Abs. 1 DSGVO wäre der Verantwortliche auch nicht verpflichtet, sich diese Kenntnis allein zum Zweck einer individualisierten Benachrichtigung nach Art. 34 DSGVO zu verschaffen.

Davon zu differenzieren sind Daten aus „ordentlichen" Verfahren des Verantwortlichen, über deren kategorischen Inhalt der Verantwortliche allein schon zur Erfüllung der Pflichten nach Art. 30 DSGVO Kenntnis haben muss. Sind solche Daten von einem Leak betroffen, sollte dem Verantwortlichen in der Regel bereits bekannt sein, welche Kategorien von Daten umfasst sind und welche Risiken für den Betroffenen aus dem Leak erwachsen können. Im Einzelfall mag es

dennoch geboten sein, in solchen Fällen eine Sichtung vorzunehmen. Etwaige entgegenstehende Bedenken eines unzulässigen Zugriffs bestehen hier in der Regel nicht.

Im Ergebnis verneinte der HmbBfDI eine Pflicht der Hochschule zur individuellen Benachrichtigung von Betroffenen im eingangs beschriebenen Sinne, d.h. von Personen, deren Daten sich in den Laufwerken von Nutzerinnen und Nutzer der HAW befanden, über die Veröffentlichung von Daten im Darknet, sofern dazu eine Sichtung von Daten erforderlich wäre, die ansonsten vor dem Zugriff der HAW geschützt wären (z.B. Daten in persönlichen Ordnern bzw. Laufwerken). An die Stelle der individuellen Benachrichtigung tritt dann die öffentliche Bekanntmachung oder eine ähnliche Maßnahme im Sinne des Art. 34 Abs. 3 lit. c DSGVO. Davon unberührt bleibt selbstverständlich die Pflicht, eindeutig identifizierbare Betroffene, wie z.B. Beschäftigte und Studierende der Hochschule ggf. individuell zu benachrichtigen, die wiederum durch die individuelle Benachrichtigung in die Lage zu versetzen sind, die von ihren persönlich-privaten Datensammlungen inhaltlich betroffenen Dritten zu informieren.

3. Sichere Kommunikation mit den Jugendhilfe-Trägern

Das Projekt zur Absicherung der E-Mail-Kommunikation ist weiterhin ohne absehbare Lösung, nachdem bisherige Ansätze verworfen wurden. Hoffnungen ruhen jetzt auf einem neuen Verschlüsselungsgateway, das allerdings noch viele Fragen aufwirft.

Bereits 2017 hat der HmbBfDI die E-Mail-Kommunikation mit externen Stellen durch den Allgemeinen Sozialen Dienst (ASD) des Fachamtes Jugend- und Familienhilfe im Bezirksamt Wandsbek geprüft. Hierbei wurde festgestellt, dass in ausnahmslos allen kontrollierten Fällen nicht hinreichend verschlüsselte E-Mails auch und gerade mit sensiblen personenbezogenen Sozialdaten von Kindern

und Jugendlichen versendet wurden. Ende 2021 war der HmbBfDI verhalten optimistisch, dass nach der erfolgreichen Pilotierung einer Ende-zu-Ende-Verschlüsselung der Rollout in 2022 abgeschlossen sein würde (vgl. 30. TB Datenschutz 2021, Kap. II 2).

Im 31. TB Datenschutz 2022 wurde berichtet, dass die Vorbereitungen eines Rollouts nicht abgeschlossen waren, da sowohl die Einbindung der Jugendhilfe-Träger nicht ausreichend vorangetrieben wurde, als auch die Abläufe zur Erzeugung und Verwaltung der Verschlüsselungszertifikate nicht geklärt waren (vgl. 31. TB Datenschutz 2022, Kap. II 4.2).

Diese Ausgangsituation veranlasste die Lenkungsgruppe im Mai 2023 einer Re-Evaluation der Optionen zuzustimmen, nicht zuletzt, da mit dem sogenannten „zentralen Mailgateway" (ZGW) eine neue Lösungsoption von Dataport herangetragen wurde. Diese stellte einen erheblich verringerten Aufwand für persönliche Verschlüsselungszertifikate in Aussicht.

Um bis zur Verfügbarkeit des ZGW eine Zwischenlösung zu finden, wurde der Einsatz von GnuPG erörtert. Diese Pläne wurden jedoch nicht weiterverfolgt, da Stand Juni eine Umsetzung des ZGW Ende 2023 / Anfang 2024 angedeutet wurde. Vor dem Hintergrund dieser relativ kurzen Übergangszeit bewertete die Projektleitung eine Zwischenlösung mit GnuPG als zu aufwändig. Im Juli 2023 beschloss die Lenkungsgruppe ohne Übergangslösung auf das ZGW zu warten.

Bezüglich des ZGW wies der HmbBfDI bereits im Juni auf technische Bedenken im Zusammenhang mit den sogenannten Domänenzertifikaten hin. Diese Domänenzertifikate sollen als Kernfunktion des ZGW personalisierte S/MIME-Zertifikate einsparen, indem stattdessen ein einzelnes domänenweites Zertifikat für alle E-Mail-Identitäten verwendet wird (bspw. info@example.com). Damit weicht das ZGW vom standardisierten Verhalten eines S/MIME-Clients ab, wodurch keine Kompatibilität mit anderen Clients gegeben ist. Diese Einschätzung des HmbBfDI wurde im August 2023 auch durch

Dataport bestätigt. Domänenzertifikate seien für die Kommunikation zwischen ZGWs gedacht. Als Konsequenz soll im Projekt der Rollout des ZGWs auch auf Trägerseite geprüft werden. In diesem Zusammenhang wurde erstmals eine Umfrage unter den Trägern gestartet, um u.a. deren IT-Ausstattung abzuschätzen.

Im Oktober wandte sich die Projektleitung an das Amt für IT und Digitalisierung (ITD) mit der Bitte um Unterstützung im Aufbau einer FHH-weiten Lösung auf Basis des ZGW. Im November 2023 wurde bekannt, dass sich bereits die Ausschreibung des ZGW weiter verzögert. Zudem ergab die Träger-Umfrage, dass ein geringeres E-Mail-Volumen als angenommen betroffen ist. Vor diesem Hintergrund regt der HmbBfDI an, zuvor als zu aufwändig ausgeschlossene Lösungen neu zu betrachten.

Die nunmehr über 6 Jahre andauernde Lösungssuche zeigt aus Sicht des HmbBfDI die Überforderung eines isolierten Projekts wie dem ASD mit der komplexen Aufgabe, eine Infrastruktur zur verschlüsselten E-Mail-Infrastruktur aufzubauen. Der HmbBfDI wertet dies als weiteres klares Zeichen, dass dringend eine FHH-weite Lösung zur verschlüsselten E-Mail-Kommunikation auch und gerade mit Externen vorangetrieben werden muss (vgl. die Beiträge III 3 und III 4 in diesem TB).

4. Technische Analyse von Webseiten und Apps

Der HmbBfDI erhält regelmäßig Beschwerden über die unzulässige Nutzung von sog. Cookies und anderen Technologien auf Webseiten. Häufig geht es um das Setzen von Cookies auf den Endgeräten der Nutzer:innen ohne deren vorherige Einwilligung. Der Einsatz von sog. Cookies ist nicht per se unzulässig, sie werden jedoch von Webseitenbetreibern u.a. für die Nachverfolgung von Nutzer:innenverhalten auf Webseiten und Apps gesetzt und sind in diesen Fällen einwilligungsbedürftig.

Vor diesem Hintergrund hat der HmbBfDI beschwerdegebundene sowie anlasslose Prüfungen von Webseiten auf den datenschutzkonformen Einsatz von Cookies und ähnlichen Technologien durchgeführt (siehe hierzu auch Kap. II 11 in diesem TB).

Für die Durchführung dieser Prüfungen wurde u.a. ein Framework eingesetzt, das als Ergänzung zu dem vom Europäischen Datenschutzbeauftragten (EDPS) entwickelten Softwaretool „Website Evidence Collector" (https://github.com/EU-EDPS/website-evidence-collector) eigens programmiert wurde. Es ermöglicht bei Aufruf einer Webseite halbautomatisiert die Dokumentation und Analyse des HTTP-Datenflusses zwischen Browser und Webservern.

Die im Endgerät abgelegten Cookies werden dabei analysiert, um Erkenntnisse über den mutmaßlichen Zweck der Speicherung zu erlangen. Durch dieses Verfahren können Einträge, die nach § 25 Abs. 2 Nr. 2 TTDSG als technisch unbedingt erforderlich zu bewerten sind, von solchen Einträgen unterschieden werden, für die nach § 25 Abs. 1 TTDSG eine den Anforderungen der DSGVO genügende Einwilligung eingeholt werden muss. Die in den Prüfläufen erstellten Ergebnisse wurden nach deren Abschluss und einer sich anschließenden weiteren manuellen Analyse in einen detaillierten Prüfbericht übertragen. Dieser schließt zusammen mit den in eine Archivdatei überführten Prüfungsartefakte die technische Dokumentation der Prüfung ab.

Im Rahmen der Prüfung von Applikationen (Apps) wurde der dafür eingerichtete Teststand mit den Softwareprodukten „tweasel-cli" (https://github.com/tweaselORG) und „PiRogue tool suite" (https://pts-project.org/) angereichert, die die Analyse und Dokumentation von Datenflüssen von Applikationen und Webservern ermöglichen.

Diese technisch fortschrittlichen Analysemethoden versetzen den HmbBfDI in die Lage, auch komplexe Webangebote und Apps zu analysieren und eventuelle Verstöße gegen datenschutzrechtliche Vorschriften festzustellen und verfahrenssicher zu dokumentieren.

Den Autor:innen dieser weitgehend quelloffen bereitgestellten Softwarewerkzeuge spricht der HmbBfDI ausdrücklich seinen Dank aus.

5. Umsetzung des Onlinezugangsgesetzes

Der HmbBfDI begleitet die Umsetzung des Onlinezugangsgesetzes in der FHH. Er prüft dabei die in Hamburg entwickelten Onlinedienste zum Online-Zugang zu Verwaltungsleistungen.

Insgesamt wurden in Hamburg 23 Onlinedienste für unterschiedliche Verwaltungsleistungen, u.a. aus den Bereichen Veranstaltungsanmeldung, Arbeitnehmerschutz und Sicherheitsprüfungen entwickelt. Der HmbBfDI wurde in die datenschutzrechtliche Prüfung eingebunden.

Der Prüfgegenstand bestand bzw. besteht fast ausschließlich aus den sogenannten Onlinediensten. Dieser Begriff findet erst mit dem derzeit geplanten Änderungsgesetz Eingang in das Onlinezugangsgesetz, das einen Online-Zugang zu Verwaltungsleistungen bietet. Der Onlinedienst übernimmt dabei nur die Schnittstellenfunktion zum etablierten Fachverfahren. Nutzenden steht durch den Onlinedienst ein Web-Formular zur Verfügung, bei dem die Eingaben zur weiteren Bearbeitung an das Fachverfahren weitergereicht werden. Insofern umfassen die hier beschriebenen Prüfungen bis auf wenige Ausnahmen ausdrücklich nicht das nachgelagerte Fachverfahren, sondern lediglich die Online-Formular-Schnittstelle zur Datenerfassung.

Diese von der FHH entwickelten Onlinedienste basieren in der Regel auf der Online-Service-Infrastruktur (OSI), einem von Dataport entwickelten Framework, das aber selbst noch nicht durch den HmbBfDI geprüft wurde.

Abweichend umfassen einzelne Onlinedienste komplexere Verfahren mit komplexeren IT-Systemen, deren Prüfung durch den HmbBfDI

noch über das Berichtsjahr 2023 andauert. Als Beispiel wäre hier der Onlinedienst „Hinweise auf Verstöße im Rahmen der Geldwäscheaufsicht mitteilen (Whistleblower-System)“ zu nennen, der unter anderem Funktionalitäten zur Kommunikation mit Hinweisgebenden enthält.

Die Datenschutzdokumentation liegt dem HmbBfDI zur Prüfung vor und wurde zum größten Teil vollständig gesichtet. Hinsichtlich der dargelegten technischen und organisatorischen Maßnahmen wurde vielfach eine Nachschärfung gefordert, da gemachte Angaben unvollständig oder zu abstrakt waren.

Allen geprüften Onlinediensten war gemein, dass eine Einstufung des erforderlichen Vertrauensniveaus i.S.d. Art. 8 Abs. 2 eIDAS-Verordnung hinsichtlich der Authentifizierung der Nutzenden versäumt wurde. Eine Verpflichtung des Betreibenden eines Onlinedienstes zur Erstellung einer sogenannten Bedarfsfeststellung ergibt sich unter anderem aus Ziffer 2.4 der Technischen Richtlinie 03107-1 des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Der HmbBfDI merkte an, dass diese Einstufung unverzüglich nachzuholen ist. Hintergrund dieses Vertrauensniveaus ist die Frage, inwieweit Nutzende eines Onlinedienstes zweifelsfrei identifiziert und authentifiziert sein müssen. Ein Onlinedienst müsste hier entsprechend der jeweiligen Anforderungen und Schutzbedarfe festlegen und dokumentieren, ob beispielsweise eine Authentifizierung über die eID-Funktion des Personalausweises notwendig ist.

Ein allgegenwärtiges Problem bei der Einrichtung der Onlinedienste war die Klärung der datenschutzrechtlichen Verantwortlichkeit. Das bisherige Onlinezugangsgesetz sieht hierzu keine Regelungen vor. Individuelle Vereinbarungen würden einen hohen Verwaltungsaufwand erzeugen, da die Onlinedienste im Rahmen des „Einer für Alle“-Verfahrens auch Behörden in anderen Bundesländern als Dienst angeboten werden sollen. Das Änderungsgesetz sieht hierfür eine gesetzliche Regelung vor. Der HmbBfDI hat die Lösung der FHH insoweit akzeptiert, die Verantwortlichkeit im Sinne der kommenden

Regelung zu gestalten, anstatt aufwändige Übergangslösungen zu finden.

6. Callcenter Emotionsanalyse

Beschäftigte in Callcentern sind oftmals einer relativ intensiven Überwachung ihrer Arbeitsprozesse ausgesetzt. Eine neue Dimension ist erreicht, wenn auch ihre Emotionen durch KI erfasst und ausgewertet werden.

Eine Emotionsanalyse von Gesprächen in Callcentern durch den Einsatz von künstlicher Intelligenz (KI) ist eine Technologie, die es ermöglicht, die Emotionen von Anrufenden und Callcenter-Mitarbeitenden während eines Gesprächs zu erkennen und zu analysieren. Die KI-gestützte Analyse wertet geschriebene Texte Wort für Wort aus, um eine positive, negative oder neutrale Stimmung zu erkennen und daraus Schlüsse zu ziehen. Die KI ist zudem in der Lage, menschliche Emotionen zu erfassen, zu interpretieren und entsprechend darauf zu reagieren. Dazu analysiert sie verschiedene Daten und Muster, die Signale für Emotionen wie Freude, Trauer, Wut oder Verwirrung sind. Das können ein bestimmter Tonfall in der Stimme oder andere sicht- oder hörbare Signale sein. Der Einsatz dieser Technik soll dazu beitragen, die Kundenzufriedenheit zu erhöhen und die Qualität der eigenen Dienstleistung sicherzustellen bzw. zu optimieren.

Der HmbBfDI hat von einer Journalistin den Hinweis bekommen, dass ein Logistikunternehmen eine automatisierte Gesprächsauswertung in seinen Callcentern einsetzen würde. Hierbei könnten über den Einsatz eines Tools die Sprache und Emotionen der Mitarbeiter:innen und Kund:innen automatisch ausgewertet werden. Für die Gesprächsauswertung sei die Software eines Dienstleisters eingesetzt bzw. eingekauft worden. Auf der Website des Dienstleisters waren ebenfalls Berichte über die Partnerschaft mit dem Verantwortlichen zu finden.

Der Einsatz von KI bzw. automatisierter Entscheidungsfindung stellt die Aufsichtsbehörden und Verantwortliche regelmäßig vor besondere Herausforderungen. Insbesondere ist es schwierig, die Betroffenen über die genauen Verarbeitungen zu informieren und abzugrenzen, ob eine vollautomatische Entscheidungsfindung erfolgt.

Der HmbBfDI hat aufgrund des Hinweises die Ermittlungen von Amts wegen aufgenommen und den Verantwortlichen zu einer Stellungnahme und Beantwortung eines Fragenkatalogs aufgefordert. Der Verantwortliche erklärte in der Folge, dass der ergangene Hinweis unzutreffend sei und konnte belegen, dass diese Software in der Art nie eingesetzt wurde.

Ein Datenschutzverstoß musste in der Folge nicht festgestellt werden. Der Hinweis führte aber dazu, dass innerhalb der Ermittlungen wertvolle Erkenntnisse gewonnen und ein Fragenkatalog zu dem Themengebiet der Emotions- und Sprachanalyse durch KI entwickelt werden konnten. Es kann davon ausgegangen werden, dass Beschwerden oder Prüfungen dieser Art in der Zukunft vermehrt vorkommen könnten. Der HmbBfDI begrüßt alle Formen von Hinweisen zu vermeintlichen datenschutzrechtlichen Verstößen, weil diese, unabhängig vom tatsächlichen Vorliegen eines Verstoßes, dazu beitragen, potenzielle Verstöße abzustellen und das allgemeine Persönlichkeitsrecht aller Betroffenen zu wahren.

7. Prüfung von Videokonferenzsystemen beim IT-Dienstleister Dataport

Der HmbBfDI führte im Berichtszeitraum weitere Gespräche mit Dataport zu den dort betriebenen Videokonferenzsystemen und war auch mit anderen Verantwortlichen in der FHH im Austausch, die diese Systeme einsetzen bzw. dies anstreben. Mittlerweile ist der Stand der Dokumentationen und die damit verbundene Transparenz der Dienste deutlich verbessert und im Endergebnis bleiben keine gravierenden datenschutzrechtlichen Mängel bestehen.

Der HmbBfDI konnte seine Teilprüfungen und Beratungen bezüglich der quelloffen entwickelten Videokonferenzsoftware dOnline-Zusammenarbeit (dOZ) 1.0 und 2.0 im Berichtszeitraum weitestgehend abschließen. Es verbleiben kleinere offene Fragestellungen und grundsätzliche Unklarheiten bezüglich der internen Organisation des Dienstleisters. Für die Teilprüfung des proprietären Produktes dVideokommunikation (dVK) wurde die Prüfung mittlerweile vollständig abgeschlossen.

Im vergangenen Jahr stellte der HmbBfDI die Mängel der einzelnen Videokonferenzsysteme dar (vgl. 31. TB Datenschutz 2022, Kap. II 3). Es wurde damals auf einige Aspekte verwiesen, die erst im Verlaufe des Berichtszeitraums fertiggestellt werden sollten. Unter anderem bezogen sich diese Merkposten auf sog. Sicherheitskonzepte, aus denen hervorgeht, mit welchen Maßnahmen die IT-Sicherheits-Ziele und -Strategien verfolgt werden. Sicherheitskonzepte stellen eine Kernkomponente einer modernen – an den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientierten – IT-Tätigkeit dar und sind für Verantwortliche wertvoll, um abschätzen zu können, ob die genutzten Systeme die eigenen technischen Anforderungen in Bezug auf die Schutzziele der Informationssicherheit und dadurch auch des Art. 32 DSGVO überhaupt erfüllen können. Da Verantwortliche diese Betrachtung nicht vollständig selbst durchführen können, sondern stets auf die Mitwirkung ihrer Dienstleister angewiesen sind, fällt diesen Dienstleistern hier eine wichtige Aufgabe zu.

Die an der Prüfung beteiligten Aufsichtsbehörden haben daher einen Fokus auf die Mitwirkung von Dataport gelegt, um zu überprüfen, ob bestehende und künftige Kund:innen ausreichend über die Umstände der Verarbeitung bei Dataport informiert werden und somit als datenschutzrechtlich Verantwortliche belastbar abschätzen können, inwiefern die angebotenen Dienstleistungen ihren Ansprüchen genügen (können).

Dataport konnte nach ersten Verzögerungen im Laufe des Berichtsjahres aktualisierte Unterlagen für dOZ zur Verfügung stellen.

Allerdings wurden die ursprünglich in Aussicht gestellten Fristen teilweise deutlich überschritten. So konnte Dataport zwar Mitte des Jahres die Sicherheitskonzepte für dOZ1.0 vorlegen, musste aber für dOZ2.0 mitteilen, dass diese erst Ende des Jahres zur Verfügung stehen werden. Dies ist auch vor dem Hintergrund bemerkenswert, als dass sich dOZ2.0 in der weitaus flächendeckenderen Nutzung befindet als Version 1.0 und daher mehr Kunden von den dokumentierten Rahmenbedingungen und Maßnahmen abhängig sind. Die Verzögerungen wurden teilweise mit internen Schwierigkeiten begründet, bei der Dokumentation der Verfahren mit der technischen Entwicklung Schritt zu halten. Die an der Prüfung beteiligten Aufsichtsbehörden haben deutlich gemacht, dass aus ihrer Sicht alle (potentiellen) Kund:innen über die gesamte Funktionalität sowie die damit einhergehenden Risiken aus Betriebssicht von Dataport zu informieren sind. Nur so können die Kund:innen, also die datenschutzrechtlich Verantwortlichen, fundiert und belastbar entscheiden, ob sie das jeweilige Verfahren für die eigenen Zwecke nutzen können.

Die Verzögerung ist auch deshalb erstaunlich, da dem HmbBfDI im Rahmen einer Beratung Dokumente vorgelegt worden sind, die eindeutig für den Einsatz von dOZ2.0 Aussagen zu Sicherheitskonzepten und Risikoanalysen trafen. Die dort zu Beginn der zweiten Jahreshälfte vorgelegten Unterlagen lieferten Aussagen zu konkreten, mit dem Betrieb bei dOZ2.0 einhergehenden Risiken, Datensicherungs-, Lösch-, Protokollierungs-, Rollen- und Rechte-Konzepten sowie zum Aufbau der Mandantentrennung im Verfahren als auch zu technischen und organisatorischen Maßnahmen bei Unterauftragnehmern. Diese Informationen hätten die an der Prüfung beteiligten Aufsichtsbehörden auch direkt nach Erstellung von Dataport erwartet. Weshalb es hier zu einer erheblichen Verzögerung gekommen ist, konnte bislang von Dataport nicht beantwortet werden. Es besteht der Eindruck, dass Dataport seine internen Prozesse nicht optimal aufgestellt hat und Freigaben von Unterlagen nicht zentral gesteuert werden.

Für dVK wurden die eingeforderten Maßnahmen und Prozesse im Berichtszeitraum umgesetzt. Grundsätzliche Fragestellungen im Hinblick auf Drittstaatenübermittlungen zum Zwecke des Supports konnten in Anbetracht des EU-US Data-Privacy-Framework ebenfalls abgeschlossen werden.

Der HmbBfDI wird die Entwicklung von Verfahren zur Videokonferenz bei Dataport weiter aufmerksam verfolgen. Klar ist, dass diese Technologien seit der Corona-Pandemie absolut etabliert sind und sich deren Nutzung verstetigen wird. Vor dem Hintergrund weiterer technischer und rechtlicher Anforderungen werden sicherlich weitere Entwicklungen zu verzeichnen sein. Insbesondere die Nutzbarmachung von Videokonferenzen im Kontext der Bearbeitung von hohen Schutzbedarfen und/oder Bearbeitung von Verschlusssachen wird der öffentlichen Verwaltung auch künftig abverlangen, kontrollierbare und belastbare Videokonferenzsoftware einzusetzen. Bei dieser Entwicklung steht der HmbBfDI gerne jederzeit für Beratungen bereit.

8. Hinweisgeberschutz bei der Sozialbehörde

Im Rahmen einer Beschwerde gegen die Sozialbehörde als Rechts- und Fachaufsichtsbehörde stellte sich heraus, dass keine ausreichend bereichsspezifische Rechtsgrundlage für die Offenlegung der Identität eines Whistleblowers bestand.

Im Jahr 2023 konnte der HmbBfDI ein umfangreiches Beschwerdeverfahren eines sog. Whistleblowers abschließen. Die Regelungen der sog. „Whistleblower-Richtlinie“ (EU/2019/1937) fanden bei der Bearbeitung durch den HmbBfDI keine Berücksichtigung, weil es zum Zeitpunkt der Datenschutzverletzung keinen anwendbaren nationalen Umsetzungsakt der Richtlinie gab. Eine unmittelbare vertikale Anwendung der Richtlinie kam nicht in Betracht, da deren Umsetzungsfrist noch nicht abgelaufen war.

Der gegen die Sozialbehörde gerichteten Beschwerde lag folgender Sachverhalt zugrunde: Die Asklepios Klinik Nord/Ochsenzoll ist gemäß § 4 Abs. 1 des Hamburgischen Maßregelvollzugsgesetzes (HmbMVollzG) eine Einrichtung des Maßregelvollzugs. Sie setzt für einige Bereiche, welche ihre Aufgabe als Beliehene nicht unmittelbar betreffen, privatrechtlich organisierte Dienstleister ein. Ein Mitarbeiter dieser Dienstleister verfasste eine mehrere Hundert Seiten umfangreiche Dokumentation mit – seiner Auffassung nach – zahlreichen Missständen in der Klinik. Diese verschickte der Mitarbeiter, teils in gekürzter Fassung, an eine große Zahl von öffentlichen und nichtöffentlichen Stellen, u.a. an mehrere Staatsanwaltschaften und die Sozialbehörde, welche gemäß § 4 Abs. 4 HmbMVollzG die Rechts- und Fachaufsicht über die Maßregelvollzugseinrichtung führt. Seine E-Mail an die Sozialbehörde hatte den Betreff „Bitte streng vertraulich behandeln". Im Rahmen ihrer Aufsichtstätigkeit leitete die Sozialbehörde die Dokumentation, welche den Verfasser leicht erkennen lässt, ungeschwärzt an die Klinik weiter. Nach Auffassung der Sozialbehörde konnte die Dokumentation nur unter Missachtung grundlegender Sicherheitsvorschriften der Maßregelvollzugseinrichtung erstellt werden, weshalb von dieser die erforderlichen Maßnahmen zu treffen waren, um künftige Verstöße verhindern. Hierzu gehörte – trotz der damit verbundenen Gefährdung des Arbeitsverhältnisses des Mitarbeiters – ein Hinwirken darauf, dass eben dieser in der Maßregelvollzugsanstalt nicht mehr eingesetzt würde.

Nachdem das Arbeitsverhältnis des Mitarbeiters durch den Dienstleister daraufhin tatsächlich gekündigt wurde, erhob dieser beim HmbBfDI Beschwerde gegen die Sozialbehörde wegen der identitätsoffenlegenden Weiterleitung seiner Dokumentation an die Maßregelvollzugseinrichtung.

Der HmbBfDI kam zu dem Ergebnis, dass die Offenlegung der Identität des Beschwerdeführers ohne Rechtsgrundlage erfolgte und daher unzulässig war, Art. 6 Abs. 1 DSGVO. Es fehlte eine entsprechend bereichsspezifische Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Rechts- und Fachaufsicht.

Grundsätzlich wäre eine Rechtfertigung durch Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 4 HmbDSG in Verbindung mit § 4 Abs. 4 S. 1 HmbMVollzG denkbar gewesen. Der mit der Offenlegung der Identität des Beschwerdeführers verbundene Eingriff ist aber als besonders intensiv zu bewerten, nicht zuletzt, weil die Offenlegung darauf abzielte, einen Dritten dazu zu veranlassen, das Arbeitsverhältnis mit dem Beschwerdeführer zu beenden. Generalklauseln wie § 4 HmbDSG sind jedoch nicht dazu geeignet, schwerwiegende Grundrechtsbeeinträchtigungen zu rechtfertigen. Dies folgt daraus, dass sie keine Abwägung zwischen den betroffenen Interessen vorsehen oder diese selbst vornehmen. Mithin können nur niedrigschwellige Eingriffe über § 4 HmbDSG in Verbindung mit einer Vorschrift des Fachrechts gerechtfertigt werden.

Die Identitätsoffenlegung war auch nicht aufgrund von Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 40 Abs. 1 S. 1 oder S. 2 HmbMVollzG gerechtfertigt. Denn diese Vorschriften regeln ausschließlich die Verarbeitung personenbezogener Daten von untergebrachten Personen.

Zuletzt kam auch Art. 6 Abs. 1 lit. d DSGVO als Rechtsgrundlage nicht in Betracht, da das Verhalten des Beschwerdeführers selbst keine unmittelbare Gefahr lebenswichtiger Interessen darstellte.

Der vorliegende Fall mag dazu dienen, den Gesetzgeber daran zu erinnern, im Fach- und Aufsichtsrecht hinreichend bereichsspezifische Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu schaffen. Denn über eine Generalklausel wie § 4 HmbDSG können besonders intensive Eingriffe in das Recht auf informationelle Selbstbestimmung nicht gerechtfertigt werden.

9. Nutzung der IT-Infrastruktur des Arbeitgebers durch den Betriebsrat

Die Mitbenutzung der IT-Infrastruktur des Arbeitgebers durch den Betriebsrat ist datenschutzrechtlich in engen Grenzen möglich, soweit angemessene technische und organisatorische Maßnahmen ergriffen werden!

Der HmbBfDI hat sich im Rahmen einer Beschwerde mit der Frage befasst, ob und unter welchen Voraussetzungen die Nutzung der IT-Infrastruktur des Arbeitgebers durch den Betriebsrat mit dem Datenschutzrecht vereinbar ist.

Nach dem Leitbild des § 2 Abs. 1 des Betriebsverfassungsgesetzes (BetrVG) arbeiten Betriebsräte und Arbeitgeber vertrauensvoll zusammen. Gemäß § 79a S. 3 BetrVG unterstützen sie sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften. Zugleich haben beide Betriebsparteien häufig gegenläufige Interessen. Als Interessenvertretung der Arbeitnehmer:innen erlangt der Betriebsrat regelmäßig Kenntnisse, welche – insbesondere in arbeitsrechtlichen Streitigkeiten – auch für den Arbeitgeber von großem Interesse sind. Ein Betriebsrat ist daher gut beraten, die von ihm verarbeiteten Daten hinreichend zu schützen.

Trotzdem nutzen in der Praxis Betriebsräte häufig die vom Arbeitgeber zur Verfügung gestellte IT-Infrastruktur (z.B. Netzwerkspeicher und E-Mailkonten). Grund hierfür könnte die arbeitsgerichtliche Rechtsprechung sein, nach welcher ein arbeitsrechtlicher Anspruch auf eine eigene IT-Ausstattung des Betriebsrats nicht bestehe. Dies gelte auch für einen eigenen Internet- und Telefonanschluss (BAG, Urteil vom 20.04.2016, Az. 7 ABR 50/14). Die Nutzung der IT-Infrastruktur des Arbeitgebers birgt für den Betriebsrat die Gefahr, dass sich der Arbeitgeber durch sein (technisches) Administratorenrecht Zugriff auf die Daten des Betriebsrats verschaffen könnte, selbst

wenn der Zugang eigentlich auf Betriebsratsmitglieder beschränkt ist. Dieses Risiko besteht insbesondere bei E-Mailkonten des Betriebsrats, welche über den vom Arbeitgeber betriebenen E-Mailserver laufen (z.B. „betriebsrat@unternehmen-xy.de"). Entsprechend begründete Beschwerden von Betriebsratsmitgliedern erreichen den HmbBfDI immer wieder. Eine Lösung könnte die Anwendung einer vom Betriebsrat kontrollierten Verschlüsselung sein, solange der Schlüssel dem Arbeitgeber nicht bekannt ist. Für die E-Mail-Kommunikation könnte beispielsweise eine durchgängige PGP-Verschlüsselung hilfreich sein, vorausgesetzt alle Beteiligten setzen sie ein. Dennoch blieben Meta-Daten wie die Identität der den Betriebsrat kontaktierenden Mitarbeiter:innen für den Arbeitgeber zugänglich, falls dieser seine administrativen Rechte ausnutzt. Nicht ohne Grund wird in der Literatur zum Teil die Auffassung vertreten, dass ein Anspruch des Betriebsrats gegen den Arbeitgeber auf Zurverfügungstellung oder Finanzierung einer Verschlüsselungssoftware bestehen müsse.

Im Berichtszeitraum hat der HmbBfDI die Beschwerde eines Mitarbeiters geprüft, dessen personenbezogene Daten vom Betriebsrat verarbeitet wurden. Der Beschwerdeführer war der Meinung, seine Daten seien nicht ausreichend vor Einblicken des Arbeitgebers geschützt. Der HmbBfDI stellte im Rahmen der Prüfung fest, dass die Daten des Betriebsrats ohne Einsatz einer von ihm kontrollierten Verschlüsselung auf einem vom Arbeitgeber bereitgestellten Netzwerklaufwerk gespeichert wurden. Ein technisches Zugriffsrecht wurde nur den Betriebsratsmitgliedern eingeräumt. Die Administratorenrechte lagen im vorliegenden Fall nicht beim Arbeitgeber, sondern ausschließlich bei dem für die IT-Verwaltung zuständigen Mitarbeiter. Zwischen dem Betriebsrat und dem Arbeitgeber wurde in einem arbeitsgerichtlichen Vergleich zudem vereinbart, dass sich der Arbeitgeber die Administratorenrechte bis zum Ablauf einer festgelegten Frist nicht einräumen lassen und auch nicht den IT-verantwortlichen Mitarbeiter anweisen darf, ihm Zugang zu den Betriebsratsdaten zu gewähren.

Ein Verstoß gegen das Datenschutzrecht wurde in diesem Fall nicht festgestellt. Bei der Auswahl der technischen und organisatorischen Maßnahmen zum Schutz der Betriebsratsdaten muss die bisherige arbeitsgerichtliche Rechtsprechung zur vertrauensvollen Zusammenarbeit berücksichtigt werden. Ebenso ist zu beachten, dass der Arbeitgeber gemäß § 79a S. 2 BetrVG datenschutzrechtlich für die Verarbeitung der Betriebsratsdaten verantwortlich ist. Eine vom Betriebsrat kontrollierte Verschlüsselung oder eine separate IT-Infrastruktur sind nicht in jedem Falle zwingend erforderlich. Der vorliegende Fall zeigt, dass es auch ungewöhnliche Lösungen gibt, um die von Art. 32 DSGVO aufgestellten Anforderungen risikoangemessener Maßnahmen zu erfüllen. Um die Vertraulichkeit der vom Betriebsrat verarbeiteten personenbezogenen Daten bestmöglich zu gewährleisten, ist eine von diesem kontrollierte Verschlüsselung gleichwohl vorzugswürdig. Dies erhöht nicht nur die Vertraulichkeit, sondern schützt auch den Arbeitgeber vor dem Verlust administrativer Rechte, sollte das Arbeitsverhältnis mit dem IT-verantwortlichen Mitarbeiter enden, ohne dass eine Nachfolgeregelung getroffen wurde.

10. Datenlöschung vor Ablauf der Aufbewahrungsfrist

In der Regel stellt die Unterschreitung einer gesetzlichen Aufbewahrungsfrist einen Datenschutzverstoß dar. Der HmbBfDI befasst sich damit im Rahmen von Beschwerden gemäß Art. 77 DSGVO jedoch nur, wenn die verletzte Aufbewahrungspflicht jedenfalls auch dem Schutz der betroffenen Person dient.

Im Rahmen einer Beratungsanfrage hatte sich der HmbBfDI mit der Frage zu befassen, ob die Löschung personenbezogener Daten vor Ablauf einer gesetzlichen Aufbewahrungsfrist einen Verstoß gegen die DSGVO darstellen und ob ein solcher Verstoß im Wege einer Beschwerde gemäß Art. 77 DSGVO verfolgt werden kann. Während

bei einer Überschreitung von gesetzlichen Aufbewahrungsfristen regelmäßig eine Verarbeitung ohne Rechtsgrundlage (Art. 6 Abs. 1 DSGVO) und ein Verstoß gegen die Pflicht zur Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO sowie Art. 17 Abs. 1 DSGVO) vorliegen, welche selbstverständlich mit einer Beschwerde bei einer Aufsichtsbehörde verfolgt werden können, könnte man meinen, eine kürzere Verarbeitungsdauer von personenbezogenen Daten wäre im Sinne des Datenschutzrechts und könne daher keinen Datenschutzverstoß darstellen. Doch die Rechtslage ist komplexer, wenn gesetzliche Aufbewahrungsfristen unterschritten werden:

Gemäß Art. 6 Abs. 1 DSGVO bedarf jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage. Neben etwa dem Erheben, der Speicherung oder der Offenlegung stellt gemäß Art. 4 Nr. 2 DSGVO auch das Löschen personenbezogener Daten eine Verarbeitung dar. Rechtsgrundlage für die Löschung zum Zeitpunkt des Ablaufs einer gesetzlichen Aufbewahrungsfrist ist regelmäßig Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit Art. 17 Abs. 1 DSGVO.

Im Falle der Unterschreitung einer gesetzlichen Aufbewahrungsfrist liegen die Voraussetzungen dieser Vorschriften nicht vor. Als Rechtsgrundlage kommt aber eine Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO in Betracht. Dass eine Löschung auch auf berechtigte Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO gestützt werden kann, erscheint indes zweifelhaft. Denn bei einer gesetzlichen Aufbewahrungspflicht dürfte regelmäßig kein dieser gegenläufiges berechtigtes Interesse bestehen.

Im Ergebnis wird damit in den meisten Fällen durch die Unter- oder Überschreitung einer gesetzlichen Aufbewahrungsfrist ein Verstoß gegen die DSGVO vorliegen.

Hinsichtlich des Beschwerderechts gemäß Art. 77 DSGVO ist weiter zu differenzieren. Das Beschwerderecht setzt nach seinem Wortlaut lediglich voraus, dass die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen

die DSGVO verstößt. Daneben muss auch eine Verletzung der beschwerdeführenden Person in ihren eigenen Rechten jedenfalls möglich erscheinen („Beschwerdebefugnis"). Bei einer Unterschreitung der Aufbewahrungsfrist ist entscheidend, ob die verletzte Aufbewahrungspflicht zumindest auch dem Schutz der betroffenen Person dient. Wenn dies der Fall ist, wie z.B. bei der Aufbewahrungspflicht einer Patienten- oder Anwaltsakte, liegt die erforderliche Beschwerdebefugnis vor. Bei einer steuerrechtlichen Vorschrift wie § 147 der Abgabenordnung ist indes nicht der Schutz der betroffenen Person bezweckt, sondern die Möglichkeit der Überprüfung durch ein Finanzamt. Bloße Verletzungen von Rechtsnormen, welche nicht auch dem Schutz der betroffenen Person dienen, können somit nicht im Wege der Beschwerde gemäß Art. 77 DSGVO verfolgt werden. Eine Verfolgung der gleichwohl vorliegenden Datenschutzverletzung durch den HmbBfDI von Amts wegen bleibt jedoch möglich.

11. Prüfung von Dienstanbietern nach TTDSG

Der HmbBfDI ist gemäß § 19 Abs. 7 des Hamburgisches Datenschutzgesetzes (HmbDSG) Aufsichtsbehörde für Telemedien (das sind vor allem Webseiten und Apps) im Sinne des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG). Durch eine klarstellende Änderung des HmbDSG wurde dem HmbBfDI ausdrücklich die Befugnis übertragen, Bußgelder bei Verstößen gegen die Vorgaben des § 25 TTDSG verhängen zu können (siehe 31. TB Datenschutz 2022, Kap. III 2).

§ 25 TTDSG setzt auf nationaler Ebene Art. 15 Abs. 3 der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG, zuletzt geändert durch die Richtlinie 2009/136/EG, sogenannte Cookie-Richtlinie) um, wonach die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der Nutzer auf der Grundlage von klaren und

umfassenden Informationen eingewilligt hat. Ohne eine vorherige Einwilligung können Cookies oder ähnliche Technologien nur dann eingesetzt werden, wenn dies unbedingt erforderlich ist, um ausdrücklich gewünschte Dienste zur Verfügung stellen zu können.

Die nunmehr klare Rechtslage wird von vielen Webseitenanbietern mittlerweile berücksichtigt. Dennoch bestehen bei einzelnen Anbietern weiterhin Defizite, die ihre Webseiten oder Apps nicht im Einklang mit den gesetzlichen Vorgaben betreiben. Der Einsatz von sogenannten Cookie-Bannern, über die eine Einwilligung für das Speichern oder Auslesen von Informationen aus dem Endgerät abgefragt wird, ist nur dann erforderlich, wenn über das unbedingt erforderliche Maß hinaus Datenverarbeitungen mittels Cookies stattfinden sollen. Webseitenbetreiber sind also in vielen Fällen nicht daran gehindert, eine Webseite auch ohne Cookie-Banner auszuspielen.

Ein häufig festgestelltes Fehlverhalten der Anbieter ist eine (teilweise offensichtlich) fehlerhafte Einteilung in erforderliche und nicht erforderliche Cookies, d. h. in solche, die richtigerweise als erforderlich angesehen und damit ohne vorherige Einwilligung eingesetzt werden dürfen, und solche, die zu anderen Zwecken eingesetzt werden sollen und daher nicht ohne vorherige Einwilligung eingesetzt werden dürfen. Der HmbBfDI hat Verantwortlichen in vielen Fällen Hilfestellung gegeben, auch um die Vorgaben aus der Orientierungshilfe Telemedien der DSK (https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf) klarstellend zu ergänzen und zu erläutern.

Im Berichtszeitraum hat der HmbBfDI eine Reihe von Webseitenbetreibern auf den rechtskonformen Einsatz von Cookies und ähnlichen Technologien überprüft. Der Fokus lag dabei auf reichweitenstarken Webangeboten und solchen, zu denen Beschwerden vorlagen. Weit überwiegend haben sich die Betreiber sehr kooperativ gezeigt und die monierten Prozesse auf ihren Webseiten angepasst, so dass ein Großteil der Verfahren mit entsprechenden Verbesserungen für die Nutzer:innen abgeschlossen werden konnte. Die Prüfungen wurden

mit technischen Prüftools durchgeführt, die eine teilautomatisierte Analyse der geprüften Webseiten ermöglichen (siehe dazu Kap. II 4 in diesem TB).

12. Makler-Prüfaktion

Im Rahmen der Prüfaktion des HmbBfDI in der Wohnungswirtschaft wurde die Datenerhebung von Mietinteressent:innen durch Maklerunternehmen und dabei insbesondere die verwendeten Selbstauskunftsformulare untersucht. Dabei zeigten sich in fast allen Fällen der überprüften Unternehmen Mängel in der Praxis der Datenbeschaffung bei Mietbewerber:innen.

Die systematische Prüfung von Immobilienmaklern wurde im letzten Tätigkeitsbericht bereits für 2023 angekündigt. Leitlinie und Prüfungsmaßstab für die datenschutzkonforme Datenerhebung anhand von Selbstauskünften ist die „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen", die die Datenschutzkonferenz (DSK) im Jahr 2018 veröffentlichte (https://www.datenschutzkonferenz-online.de/media/oh/20180207_oh_mietauskuenfte.pdf).

Bei fast allen im Berichtszeitraum überprüften Unternehmen wurde entweder auf dem Formular der Selbstauskunft oder in den Datenschutzerklärungen auf eine Einwilligung der Mietinteressent:innen zur Preisgabe ihrer Daten im Zusammenhang mit der Bewerbung für eine Wohnung abgestellt. Die im Einzelnen abgefragten Daten und Nachweise wurden dabei zumeist als freiwillige Angaben bezeichnet. Raum dafür, Datenerhebungen von Mietinteressent:innen auf eine Einwilligung zu stützen, besteht regelmäßig jedoch nicht. Bei der Bewerbung um eine Mietwohnung fehlt es an der für eine wirksame Einwilligung nach Art. 4 Nr. 11 DSGVO notwendigen Freiwilligkeit im Hinblick auf die Preisgabe der Daten durch den Mietinteressent:innen im Rahmen einer Selbstauskunft. Aufgrund der strukturellen Unterlegenheit von Bewerber:innen um eine Mietwohnung gegen-

über Vermieter- und Maklerseite und der erheblich angespannten Angebotssituation für Mietwohnungen in Hamburg werden die dort geforderten Angaben gerade nicht im Rahmen einer freien Entscheidung von den Betroffenen mitgeteilt. Hinweise in Selbstauskunftsformularen auf eine „freiwillige Selbstauskunft" oder „Alle Angaben in der Selbstauskunft wurden freiwillig gemacht", sind irreführend und geben eine unzutreffende Rechtsgrundlage wieder.

Auch wurde nicht zwischen den nach der Orientierungshilfe maßgeblichen, unterschiedlichen Zeitpunkten im Vermietungsprozess unterschieden. So wurden Daten wie Einkommensnachweise und Bonitätsauskünfte bereits bei bestehendem Anmietungsinteresse erhoben, ohne dass zu diesem Zeitpunkt eine Entscheidung für den bestimmten Bewerber als neuem Mieter getroffen wurde. Einkommensnachweise dürfen jedoch erst bei beabsichtigtem Vertragsschluss mit einem/einer konkreten Bewerber:in erhoben werden. Zu beanstanden war weiterhin, schon vor Besichtigungsterminen Angaben zum Arbeitgeber und zum Einkommen abzufragen, ohne dass ein Anmietungsinteresse überhaupt feststand.

Bei der Nachprüfung eines Unternehmens hat sich herausgestellt, dass entgegen dessen anders lautender Ankündigung, die für die Datenerhebung eingesetzte Software werde so angepasst, dass vor einem Besichtigungstermin nur Kontaktdaten erhoben würden, dies tatsächlich nicht umgesetzt wurde. Die weitere Nachprüfung der Webseite des Unternehmens durch den HmbBfDI hat ergeben, dass die Anpassungen vom verantwortlichen Immobilienmakler nunmehr realisiert wurden.

Im Rahmen der Prüfaktion konnte der HmbBfDI bei den geprüften Maklerunternehmen datenschutzkonforme Anpassungen der Selbstauskunftsformulare erreichen. Die Prüfaktion im Bereich der Immobilienwirtschaft wird im Jahr 2024 fortgesetzt.

13. Immobilieninserate mit Fotos eingerichteter Wohnungen

Bei der Veröffentlichung von Fotos bewohnter Wohnungen durch Eigentümer:innen, Vermieter:innen und Makler:innen im Rahmen von Immobilien- bzw. Wohnungsinseraten sollte eine schriftliche Einwilligung der Bewohner:innen eingeholt werden, um Streitigkeiten vorzubeugen und der Nachweispflicht des Art. 7 Abs. 1 DSGVO zu entsprechen.

Im Berichtsjahr 2023 erreichten den HmbBfDI wiederholt Beschwerden von Bürger:innen, deren Mietwohnungen für Wohnungsinserate fotografiert wurden. Verkäufer:innen, Vermieter:innen bzw. deren Makler:innen erstellen mit diesen Fotos Immobilien- oder Wohnungsinserate, welche in der Regel auf deren Webseite sowie in Immobilienportalen veröffentlicht werden. Ein besonders häufiger Streitpunkt der Beschwerden war der Nachweis einer nur mündlich erteilten Einwilligung. Dies ist zwar grundsätzlich zulässig, birgt für Verantwortliche jedoch die Gefahr, ihre Nachweispflicht aus Art. 7 Abs. 1 DSGVO nicht erfüllen zu können.

Fotos von bewohnten Wohnräumen enthalten regelmäßig personenbezogene Daten. Denn durch die auf den Fotos sichtbaren Einrichtungsgegenstände können die Bewohner:innen identifiziert werden (Art. 4 Nr. 1 DSGVO). Dies gilt erst recht, wenn auf den Fotos Briefe mit Adresse oder gar Bilder der Bewohner:innen selbst sichtbar sind. Zudem können Rückschlüsse auf deren Lebensgewohnheiten, den Geschmack und ggf. die Interessen möglich sein.

In den allermeisten Fällen stellt bereits die Anfertigung, jedenfalls aber das Veröffentlichen der Fotos, eine Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DSGVO dar. Gemäß Art. 6 Abs. 1 DSGVO bedarf jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage. Da der Eingriff in die Privatsphäre der Bewohner:innen durch das Veröffentlichen von Fotos der von ihnen

bewohnten Räume als intensiv anzusehen ist, dürfte ein berechtigtes Interesse der Verantwortlichen gemäß Art. 6 Abs. 1 lit. f DSGVO als Rechtsgrundlage in aller Regel ausscheiden. Diese Wertung hat auch das Amtsgericht Steinfurt (Teilurteil vom 10.04.2014 – 21 C 987/13) vorgenommen, indem es feststellte, dass ein mietrechtlicher Anspruch des Vermieters auf Duldung der Anfertigung von Fotos der bewohnten Wohnung nicht bestehe. Weder das Anfertigen, noch das Veröffentlichen von Wohnungsfotos ist für die Durchführung eines Wohnraummietverhältnisses erforderlich, sodass auch Art. 6 Abs. 1 lit. b DSGVO als Rechtsgrundlage nicht in Betracht kommt. Für Verantwortliche verbleibt somit nur eine Einwilligung der Bewohner:innen als mögliche Rechtsgrundlage, Art. 6 Abs. 1 lit. a DSGVO, Art. 7 DSGVO. Eine wirksame Einwilligung erfordert unter anderem, dass die Bewohner:innen umfassend über die beabsichtigte Verarbeitung informiert sind und sie ihre Zustimmung freiwillig erteilen.

Es wird empfohlen, dass Verantwortliche ihre Absicht, aktuelle Fotos der bewohnten Wohnung veröffentlichen zu wollen, frühzeitig ankündigen, um die Bewohner:innen nicht zu überraschen und somit möglicherweise die Freiwilligkeit der Einwilligung zu gefährden. Eine Einwilligung sollte zudem zur Gewährleistung der Nachweispflicht aus Art. 7 Abs. 1 DSGVO schriftlich eingeholt werden. In jedem Fall müssen Verantwortliche vor der Verarbeitung über die geplanten Veröffentlichungskanäle, die Freiwilligkeit der Einwilligung und deren Widerruflichkeit informieren. Besonders persönliche Gegenstände sollten aus dem Bildbereich entfernt oder auf den Fotos unkenntlich gemacht werden. Wird von den Bewohner:innen keine Einwilligung erteilt, verbleibt den Verantwortlichen, Fotos der Wohnung im unbewohnten Zustand zu verwenden.

14. Weitergabe von Mieterdaten an die Polizei

Vermieter oder Hausverwaltungen dürfen Mieterdaten nur unter bestimmten Bedingungen an die Polizei weitergeben. Bei Anfragen sollten sie die Voraussetzungen genau prüfen, im Zweifel Rückfragen stellen und alle relevanten Informationen dokumentieren, bevor sie Daten weitergeben.

Ein Bürger beschwerte sich beim HmbBfDI darüber, dass seine Hausverwaltung personenbezogene Daten aus seiner Mieterakte ohne seine Zustimmung an die Polizei weitergegeben hatte. Der Beschwerdeführer gab an, dass die Polizei gegen ihn ermittelt habe und einen Handschriftenvergleich durchführen wollte. Die Ermittlungen gegen ihn seien jedoch eingestellt worden. Die Sachverhaltsaufklärung im Beschwerdeverfahren ergab, dass gegen den Betroffenen polizeilich ermittelt worden war, nachdem Drohbriefe im Postkasten anderer Bewohner:innen aufgefunden wurden. Der Beschwerdeführer hielt die Weitergabe seiner Daten an die Polizeibehörde ohne Rücksprache und Genehmigung durch ihn für rechtswidrig.

Nach näherer Prüfung des Falles stellte sich heraus, dass die Hausverwaltung die Daten des Betroffenen zulässig an die Polizeibehörde weitergegeben hatte, da sie sich auf eine datenschutzrechtliche Grundlage stützen konnte. Ein datenschutzrechtlicher Verstoß wegen unbefugter Weitergabe der Daten konnte somit nicht festgestellt werden.

Auskunftsersuchen im Rahmen von Ermittlungen können auf § 161 StPO gestützt werden. Diese Vorschrift ist allerdings die Rechtsgrundlage für die Staatsanwaltschaft und Polizeibedienstete als Ermittlungsbeamte der Staatsanwaltschaft für die Anforderung und Erhebung von Daten und gilt nicht für die Datenübermittlung von privaten Stellen an Polizeibehörden.

Nach § 24 Abs. 1 Nr. 1 BDSG dürfen Unternehmen personenbezogene Daten verarbeiten und damit auch gegenüber Behörden offenlegen, wenn dies zur Verfolgung von Straftaten erforderlich ist. Dabei sind die berechtigten Interessen der betroffenen Person an dem Ausschluss der Verarbeitung zu berücksichtigen. Wenn der Verdacht besteht, dass der Betroffene eine Straftat begangen haben könnte, wird ein entgegenstehendes Interesse des Betroffenen an der Verarbeitung regelmäßig einer Offenlegung der Daten nicht entgegenstehen.

Im Rahmen der Abwägung war die Hausverwaltung zu dem Ergebnis gekommen, dass das Interesse des Mieters das erhebliche Interesse an der Aufklärung und Verfolgung einer Straftat nicht überwog. Das ist datenschutzrechtlich nicht zu beanstanden. Die Aufforderung der Polizei, Daten zum Betroffenen zur Verfügung zu stellen, hatte die Hausverwaltung nach eingehender Prüfung erfüllt. Das Unternehmen hatte die Polizei zunächst um nähere Angaben gebeten, um die Anfrage und die Berechtigung zur Weitergabe der Daten seinerseits prüfen zu können. Erst nachdem die Polizeibehörde weitere Angaben zur Rechtsgrundlage und zum Sachverhalt zur Verfügung gestellt und angegeben hatte, dass im Rahmen der Ermittlungen Schriftstücke zu Vergleichszwecken benötigt werden, hatte das Unternehmen Daten zum Mieter weitergegeben.

Ist eine Übermittlung von Daten datenschutzrechtlich zulässig, sieht Art. 13 Abs. 3 DSGVO zudem eine Informationspflicht vor. Danach hat der Verantwortliche, wenn er beabsichtigt, personenbezogene Daten für einen anderen Zweck zu verarbeiten als für den Zweck, für den die Daten ursprünglich erhoben wurden, der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck zur Verfügung zu stellen. Von dieser Information kann nur abgesehen werden, wenn die Polizei eine dadurch entstehende Gefährdung der Ermittlungsmaßnahmen mitteilt. Auch dies sollte im Rahmen einer Anfrage einer Polizeibehörde vorab vom verantwortlichen Unternehmen geklärt und dokumentiert werden.

15. Beschwerdeunabhängige Prüfungen bei Inkassodienstleistern

Der HmbBfDI hat im Jahr 2023 eine beschwerdeunabhängige Kontroll- und Prüfaktion bei Inkassodienstleistern eingeleitet. Hierfür sind sowohl umfangreiche Dokumentationen angefordert als auch Vor-Ort-Kontrollen durchgeführt worden. Die Aktion wird sich noch bis weit in das Jahr 2024 hinein erstrecken.

Im Fachgebiet Inkasso und Auskunfteien des HmbBfDI ist seit Jahren ein konstant hohes Aufkommen an Beschwerden, Anfragen und sonstigen Meldungen zu verzeichnen. Gleichzeitig bringen die Betroffenen in diesem Gebiet stets ein hohes Interesse an einer Klärung datenschutzrechtlicher Fragen vor. Dies ist in besonderem Maße der Tatsache geschuldet, dass Inkassodienstleister einerseits solche Daten verarbeiten, die von den Betroffenen als sehr sensibel wahrgenommen werden, namentlich neben Adress- und Kontaktdaten auch Daten zur Bonität und zum Zahlungsverhalten. Andererseits werden diese Daten potentiell auch mit Dritten geteilt, insbesondere mit Auskunfteien bzw. Adressdienstleistern zum Zwecke der Adressermittlung nach dem Erhalt von Postrückläufern oder zur Einmeldung oder Einholung von Bonitätsinformationen. Hierzu erreichen den HmbBfDI viele Anfragen und Beschwerden hinsichtlich der Rechtmäßigkeit dieser inkassotypischen Datenverarbeitungsvorgänge. Weitere Beschwerden treten gehäuft bei Themen wie Personenverwechslungen auf, wenn sich also die im Rahmen einer solchen Adressermittlung die an den Inkassodienstleister übermittelte Anschrift als fehlerhaft herausstellt, und bei der Thematik ausbleibender Rückmeldungen auf geltend gemachte Betroffenenrechte der DSGVO, insbesondere Anträge auf Auskunft (Art. 15 DSGVO) und Löschung (Art. 17 DSGVO). Diese Beschwerden beziehen sich im Regelfall auf konkrete Inkassovorgänge, mit denen die Betroffenen konfrontiert werden.

Im Rahmen der ihm zustehenden Befugnisse kann der HmbBfDI allerdings auch unabhängig von dem Vorliegen eines konkreten Hinweises oder vorgetragenen Beschwerdesachverhaltes datenschutzrechtliche Kontrollen bei Verantwortlichen durchführen. Diese Befugnis schließt einerseits die Anforderung und Prüfung von Unterlagen wie z.B. dem Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO ein, andererseits auch die Aufforderung zur Beantwortung von spezifischen Fragen im Zusammenhang mit der geschäftlichen Verarbeitung personenbezogener Daten.

Darüber hinaus steht dem HmbBfDI die Möglichkeit offen, Vor-Ort-Kontrollen bei den Verantwortlichen durchzuführen. Eine solche Vor-Ort-Kontrolle bietet zunächst die Möglichkeit, einen lebensnahen Einblick in die Tätigkeit der Verantwortlichen zu erhalten. Darüber hinaus kann hierdurch auch ein direkterer Kontakt zu den dortigen Ansprechpersonen entstehen, insbesondere zu den internen oder externen Datenschutzbeauftragten, durch welche die zukünftige Kommunikation mit der Verantwortlichen erleichtert werden kann. Das wesentliche Ziel einer Vor-Ort-Kontrolle besteht aber regelmäßig darin, die Datenverarbeitungsvorgänge der Verantwortlichen nachzuvollziehen, auf Konformität mit den entsprechenden Vorschriften zu prüfen und bei der Feststellung von Verstößen auf deren Behebung hinzuwirken. Ergänzend hierzu führt die Ankündigung und Durchführung einer Vor-Ort-Kontrolle durch die zuständige Aufsichtsbehörde erfahrungsgemäß dazu, dass die Verantwortliche bestenfalls bereits proaktiv ihre Verarbeitungsvorgänge prüft und ggf. deren Umstellung einleitet, mindestens aber hinsichtlich der tatsächlichen Überwachungsfunktion der Aufsichtsbehörde sensibilisiert wird.

Sowohl aus Kapazitäts- bzw. Ressourcengründen als auch aus Gründen der Verhältnismäßigkeit liegt nahe, diese aufwändigen und zeitintensiven Prüfungen in der Regel priorisiert bei denjenigen Verantwortlichen durchzuführen, bei denen ein gesteigertes öffentliches Interesse an einer entsprechenden Kontrolle besteht. Ein solches Interesse kann sich aus verschiedenen Faktoren ergeben, beispiels-

weise aus der Natur der Tätigkeit der Verantwortlichen bzw. der Art der verarbeiteten Daten, der Anzahl der hinsichtlich der Verantwortlichen beim HmbBfDI eingehenden Beschwerden gemäß Art. 77 DSGVO oder auch grundsätzlich aus der (wirtschaftlichen) Größe bzw. Bedeutung des Unternehmens, soweit dort von einem entsprechenden Maß der Verarbeitung personenbezogener Daten ausgegangen werden kann.

Vor diesem Hintergrund hat der HmbBfDI seit dem Frühjahr 2023 die fünf relevantesten in Hamburg ansässigen Inkassodienstleister kontaktiert und im Rahmen der beschwerdeunabhängigen Prüfung jeweils zunächst zur Übersendung von Dokumenten aufgefordert. Erbeten wurden jeweils das Verzeichnis von Verarbeitungstätigkeiten, eine Auflistung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der verarbeiteten Daten sowie ein Überblick über die datenschutzrechtlich relevanten Kennzahlen des jeweiligen Unternehmens. Ergänzend hierzu wurden, soweit diese noch nicht vorlagen, Muster von Forderungsschreiben sowie von Auskünften gemäß Art. 15 DSGVO angefordert.

Diese zum Teil sehr umfangreichen Dokumente sind zunächst auf Vollständigkeit und anschließend eingehend inhaltlich geprüft worden. Unter Beteiligung des Referats Technik des HmbBfDI sind zudem auch technische Aspekte der Datenverarbeitungen und Datensicherheit geprüft und ausgewertet worden. Auf Grundlage dieser Auswertungen und seiner Vorerfahrungen fertigte der HmbBfDI Kataloge mit Fragen an, mittels derer die Prüfungen sodann weiter vertieft wurden. Bei dreien der größten in Hamburg ansässigen Inkassodienstleister führte der HmbBfDI in der Folge Vor-Ort-Kontrollen durch, zwei weitere wurden ausschließlich im schriftlichen Verfahren geprüft.

Ziel der Vor-Ort-Kontrollen war, ergänzend zu den in den angeforderten Dokumenten enthaltenen Informationen, eine umfassende und lebensnahe Übersicht über die Verarbeitung von Schuldnerdaten in diesen Unternehmen zu erhalten. Hierzu wurden im Rahmen der

fünf- bis sechsstündigen Kontrolltermine zunächst Informationen über die grundsätzliche Infrastruktur und die Software eingeholt, mittels welcher das jeweilige Unternehmen Daten verarbeitet. Daran konnten sich dann die zuvor erarbeiteten Fragen sowie weitere konkrete Fragen über die Verarbeitung von Schuldnerdaten anschließen. Diese Fragen wurden in der Reihenfolge eines typischen Verarbeitungsvorgangs adressiert, sodass zunächst die Übertragung von Schuldnerdaten durch die Gläubiger an den Inkassodienstleister und damit die erstmalige Erfassung bzw. Speicherung dieser Daten dort, anschließend die Verarbeitung wie die Verwendung zur Kommunikation mit den Schuldnern selbst sowie die Offenlegung an Dritte und abschließend die Einschränkung der Verarbeitung bzw. Löschung dieser Daten überprüft wurden. Ergänzend hierzu wurden die Abläufe sowie der grundsätzliche Umgang der Inkassodienstleister mit datenschutzrechtlichen Betroffenenrechten geprüft.

In diesem Rahmen stellte sich bei einem der Vor-Ort-Termine heraus, dass nach Zeitablauf zu löschende Datensätze noch vorhanden waren. Daneben konnte der HmbBfDI in diesen Terminen verschiedene Verbesserungen bei datenschutzrechtlichen Fragestellungen erzielen. Hierbei handelte es sich beispielsweise um Vorschläge zu noch weitergehenden Beschränkungen des Zugriffs auf personenbezogene Daten, die lediglich zur Erfüllung gesetzlicher Aufbewahrungspflichten aufbewahrt werden, sowie um die Erhöhung der Transparenz in Fällen, in denen Schuldner:innen aufgrund einer vorangegangenen Adressermittlung angeschrieben werden. Diese Hinweise sind von den betroffenen Unternehmen auch aufgenommen und, soweit möglich, sehr zeitnah umgesetzt worden. Darüber hinaus konnte der HmbBfDI in diesen Terminen gezielt auf die thematischen Schwerpunkte hinweisen, die Gegenstand typischer datenschutzrechtlicher Beschwerden sind, und die Unternehmen in diesen Teilbereichen einerseits zu erhöhter Transparenz und der Verbesserung von Prozessen anhalten, andererseits auch auf die zur Verfügung stehenden Abhilfebefugnisse bei festgestellten Verstößen aus Art. 58 Abs. 2 DSGVO hinweisen.

Mit der Übersendung der Fragenkataloge in den Fällen, in denen eine Vor-Ort-Kontrolle nicht erforderlich war, wurde im Wesentlichen das gleiche Ziel verfolgt. Zwar blieb hierbei der Nebeneffekt der persönlicheren Kommunikation aus, allerdings konnten mit dieser Methode im Ergebnis die gleichen inhaltlichen Themenkomplexe wie bei den Vor-Ort-Kontrollen überprüft werden.

Als Gesamtergebnis der beschwerdeunabhängigen Kontroll- und Prüfaktion konnte der HmbBfDI abgesehen von einzelnen Befunden erfreulicherweise feststellen, dass bei den geprüften Inkassodienstleistern grundsätzlich ein hohes Maß sowohl an Professionalität als auch an Sensibilität hinsichtlich des Umgangs mit datenschutzrechtlichen Themen besteht. Die Unternehmen unterhalten jeweils eigene Abteilungen zur Bearbeitung datenschutzrechtlicher Anfragen und haben standardisierte Prozesse für die Verarbeitung der Schuldnerdaten im Rahmen von Inkassovorgängen eingerichtet. Die Verarbeitungsvorgänge einschließlich etwaiger Übermittlungen an Dritte werden nachvollziehbar dokumentiert. Auch die durch die Unternehmen erteilten Auskünfte gemäß Art. 15 DSGVO erfüllen die gesetzlichen Anforderungen und setzen dabei auch aktuelle europarechtliche Entscheidungen um, wie beispielsweise die Pflicht, die Empfänger personenbezogener Daten nicht nur als Kategorie, sondern konkret zu benennen (vgl. Urteil des Europäischen Gerichtshofs (EuGH) vom 12. Januar 2023, Az. C-154/21).

Der HmbBfDI beabsichtigt, diese beschwerdeunabhängigen Prüfungen einschließlich der Vor-Ort-Kontrollen auch in Zukunft in zunehmendem Maße und auch bei anderen Verantwortlichen und in anderen Fachgebieten durchzuführen. Dies schließt sowohl einen Prüfablauf wie in den geschilderten Fällen als auch unangekündigte Vor-Ort-Kontrollen ein.

16. 1-Cent-Überweisungen durch Inkassodienstleister

Der Betreff einer Überweisung eines Kleinbetrages ist nicht dazu vorgesehen, von Inkassodienstleistern als Kommunikationsmittel mit Schuldner:innen genutzt zu werden.

Auf der Grundlage einer Beschwerde hat sich der HmbBfDI mit der Praxis sogenannter 1-Cent-Überweisungen durch Inkassodienstleister beschäftigt. Dabei wird den Schuldner:innen ein Betrag in Höhe von einem Cent auf ihr Bankkonto überwiesen. Der Überweisungsbetreff enthält in der Regel eine Telefonnummer sowie ein Aktenzeichen des Inkassodienstleisters. Zusätzlich enthält er eine Bitte um einen Anruf und eine knappe Nennung des Grundes, regelmäßig die Forderung eines genannten Gläubigers. Die 1-Cent-Überweisung wird in dieser Form in gleicher Weise wie ein postalisches Schreiben oder eine E-Mail als Kommunikationsmittel eingesetzt, um Schuldner:innen auf eine bestehende Forderung gegen sie hinzuweisen bzw. sie hieran zu erinnern.

Der HmbBfDI hat in diesem Rahmen geprüft, ob diese Praxis in datenschutzrechtlicher Hinsicht zulässig ist. Der HmbBfDI kommt dabei zu dem Ergebnis, dass für die Verarbeitung der Kontodaten zu dem genannten Zweck (Kontaktaufnahme) keine Rechtsgrundlage besteht, da diese Verarbeitung im Regelfall weder erforderlich ist noch im überwiegenden Interesse der Inkassodienstleister liegt.

Zweck der Beauftragung von Inkassodienstleistern ist regelmäßig die vorgerichtliche Eintreibung offener Forderungen. Weder diesen legitimen Zweck noch die Zulässigkeit der hierfür erforderlichen Datenverarbeitungen – insbesondere die Datenübermittlung von Gläubigern an Inkassodienstleister als auch die Nutzung dieser Daten durch den Inkassodienstleister selbst – stellt der HmbBfDI dabei in Abrede. Auch ist anerkannt, dass häufig ein finanzielles

Interesse der Inkassodienstleister daran besteht, möglichst viele und kostengünstige Wege auszuschöpfen, um Schuldner:innen zur Kontaktaufnahme mit dem Ziel der Zahlung der offenen Forderungen zu bewegen. Umgekehrt haben auch Schuldner:innen ein Interesse daran, dass die durch ihre Zahlungssäumnis ausgelösten Zusatzkosten gering bleiben, um den offenen Forderungsbetrag nicht übermäßig zu erhöhen. In diesem Sinne würde bei einer Cent-Überweisung bei allen Beteiligten nur äußerst geringe Zusatzkosten anfallen.

Allerdings ist in datenschutzrechtlicher Hinsicht für die Kommunikation zwischen Inkassodienstleistern und Schuldner:innen der Einsatz von 1-Cent-Überweisungen regelmäßig schon deshalb nicht erforderlich, weil andere Kommunikationsmittel vorhanden sind, die zudem auch tatsächlich zur Kommunikation vorgesehen sind. Im Rahmen der Beauftragung eines Inkassodienstleisters übermittelt der Gläubiger üblicherweise diejenigen Kontaktdaten, die seitens der Schuldner:innen im Rahmen des zugrundeliegenden Rechtsverhältnisses angegeben worden sind. Häufig sind dies die Anschrift, die E-Mail-Adresse und in einigen Fällen auch die Telefon- bzw. Mobiltelefonnummer. Ein solches Kommunikationsmittel im Sinne eines von den Betroffenen zur Kommunikation bereitgehaltenen Kanals stellt die Bankverbindung nach Auffassung des HmbBfDI gerade nicht dar. Der Gläubiger hat die Bankverbindung der Schuldner:innen in der Regel zu einem bestimmten Zweck erhoben, beispielsweise dem Einzug von Beträgen im Lastschriftverfahren. Die Nutzung der Bankverbindung zu Kommunikationszwecken durch einen Inkassodienstleister stellt nach Auffassung des HmbBfDI dagegen einen wesentlich anderen Zweck dar, der auch nicht mit einer – unter bestimmten Voraussetzungen zulässigen – Zweckänderung gerechtfertigt werden kann. Somit müssen Betroffene im Regelfall weder damit rechnen noch dulden, dass ihre Bankverbindung zur Überweisung von Kleinbeträgen unter Beifügung eines entsprechenden Überweisungsbetreffs und damit zur Kommunikation mit ihnen verwendet wird. Auf die Frage der Geeignetheit dieses Kommunikationsmittels, also ob die Schuldner:innen den Inhalt des Überweisungsbetreffs überhaupt zeitnah zur Kenntnis nehmen

würden, kommt es daher nicht an, dennoch bezweifelt der HmbBfDI auch dies.

Zusätzlich hat der HmbBfDI berücksichtigt, dass sich aus einem solchen Überweisungsbetreff die Information ergibt, dass die Kontoinhaber:innen aufgrund einer offenen Forderung durch ein Inkassodienstleister kontaktiert werden. Diese üblicherweise negativ behaftete Information erreicht insoweit nicht lediglich die Schuldner:innen, sondern gerät auch in den potentiellen Wahrnehmungsbereich ihrer Bank. Für Schuldner:innen kann damit die Befürchtung erheblicher negativer Konsequenzen entstehen. Im Rahmen der PSD2-Richtlinie ist seit einigen Jahren zudem möglich, dass Kontoinhaber:innen den Zugriff auf ihr Konto auch Drittdienstleistern gewähren, beispielsweise zur individuellen Prüfung der Bonität. Unter diesen Umständen ist folglich nicht ausgeschlossen, dass auch Dritte den entsprechenden Überweisungsbetreff zur Kenntnis nehmen. Abschließend bewertete der HmbBfDI auch, dass sowohl bei ungerechtfertigten Forderungen als auch spätestens nach Zahlung einer bestehenden Forderung ein Interesse daran besteht, diese Information aus dem Bankkonto zu löschen. Soweit eine Löschung oder Korrektur überhaupt möglich ist, müssten die Kontoinhaber:innen im Regelfall selbst mit einem entsprechenden Wunsch an ihre Bank herantreten, was der HmbBfDI als erhebliche Zusatzbelastung einstuft.

Diese Auffassung hat der HmbbBfDI im Rahmen der Prüfung dem Inkassodienstleister mitgeteilt. Dieser versicherte, dass er von einem weiteren Einsatz der 1-Cent-Überweisungen zu rein kommunikativen Zwecken absehen wird. Nach Kenntnis des HmbBfDI verzichten die weiteren in Hamburg ansässigen Inkassodienstleister ohnehin schon auf dieses Mittel.

17. Smarte Liefer- und Ladezonen („SmaLa“)

Das Projekt Smarte Liefer- und Ladezonen („SmaLa“), das der HmbBfDI bereits im Jahre 2021 beratend begleitet und in seinem Tätigkeitsbericht vorgestellt hat, soll in seine zweite Phase überführt werden. Für die damit verbundenen datenschutzrechtlichen Fragen stand der HmbBfDI der zuständigen Behörde für Wirtschaft und Innovation (BWI) auch im Berichtszeitraum als Ansprechpartner zur Verfügung.

Das Reallabor „SmaLa“ ermöglicht es registrierten Paketdiensten und Lieferant:innen, mithilfe einer App verfügbare Modellladezonen aufzufinden und zu reservieren. Ziel des Projektes ist es, herauszufinden, ob das digitale Buchungsangebot dazu beitragen kann, den mit der Suche von Ladezonen verbundenen Verkehr und die damit einhergehenden Umweltbelastungen sowie verkehrsgefährdendes „Parken in zweiter Reihe“ zu reduzieren.

In der ersten Projektphase wurden im Bezirk Hamburg-Mitte vier smarte Liefer- und Ladezonen eingeführt. Diese sehen ein absolutes Halteverbot vor, von dem Zustellfahrzeuge, für die eine Buchung über die „SmaLa“-App vorliegt, vorübergehend ausgenommen sind. Für welche Nutzer:innen die Ausnahme gilt, wird auf digitalen Schildern, mit denen die Ladezonen ausgestattet sind, erkennbar. Diese zeigen in verkürzter Form eine für die jeweilige Buchung generierte Ticket-ID an, die den Nutzer:innen auch über die App buchungsbezogen bereitgestellt wird.

In seiner zweiten Phase soll das Projekt auf 25 smarte Liefer- und Ladezonen in drei Hamburger Bezirken ausgeweitet werden. Ein bis zwei dieser Zonen sollen mit automatisch absenkbaren Pollern ausgestattet werden, um einer Nutzung durch nicht autorisierte Fahrzeuge vorzubeugen.

Die BWI hatte erwogen, eine solche Automatik unter Einsatz von Kamerasystemen zu realisieren, die eine Erfassung des Kennzeichens anfahrender Fahrzeuge und einen anschließenden Abgleich mit den Kennzeichen, für die eine Buchung erfolgt ist, ermöglichen sollte. Diese Lösung barg jedoch die Gefahr, dass auch Kennzeichen unbeteiligter Fahrzeuge erfasst würden, so dass der HmbBfDI bereits im Jahre 2021 angeregt hatte, andere Umsetzungsmöglichkeiten in Betracht zu ziehen. Der durch die BWI zuletzt entwickelte Lösungsansatz sieht eine punktuelle Erhebung sog. Geofence-Daten der Nutzer:innen vor.

Um ein automatisches Ein- und Ausfahren der Poller zu gewährleisten, sollen danach zunächst Geofencing-Bereiche, die sich wie virtuelle Ringe um die Liefer- und Ladezonen legen, definiert werden. Beim Passieren der jeweiligen virtuellen Grenze durch das Zustellfahrzeug soll die Information, dass der Geofencing-Bereich befahren oder verlassen wurde, über die App an das Backend von „SmaLa“ übermittelt und der Poller aktiviert werden.

Da diese Informationen auch zu Analysezwecken erhoben werden und insbesondere Erkenntnisse darüber liefern sollen, ob und – falls ja – wie lange gebuchte Ladezonen tatsächlich genutzt werden, sieht die im Rahmen der zweiten Projektphase angestrebte Lösung eine entsprechende Eingrenzung aller smarten Liefer- und Ladezonen und nicht nur solcher mit Pollern vor.

Damit würden bei Nutzung der „SmaLa“-App neben – u.a. – einem durch die BWI individuell ausgestellten Registrierungscode zur Freischaltung der App und dem Kfz-Kennzeichen des jeweiligen Lieferfahrzeugs künftig ggf. auch Geofence-Daten im obigen Sinne verarbeitet. Bei diesen Informationen handelt es sich jedenfalls dann um personenbezogene Daten i.S.d. Datenschutzrechts, wenn der Registrierungscode zugunsten einer natürlichen Person und nicht etwa eines Unternehmens ausgestellt oder aber das Fahrzeug, dessen Kennzeichen bei der Buchung verarbeitet wird, auf eine natürliche Person zugelassen ist, so dass vermittels dieser Informationen eine Zuordnung zu einer natürlichen Person erfolgen kann.

Da das Vorhaben damit neue datenschutzrechtliche Fragen aufwirft, wird es auch in seiner zweiten Phase durch den HmbBfDI begleitet, der die BWI insbesondere zur Rechtsgrundlage der Datenverarbeitung, zu Transparenz- und Löschpflichten sowie etwaigen Möglichkeiten, den Umfang der zu verarbeitenden Daten i.S.d. Grundsatzes der Datenminimierung nach Art. 5 Abs. 1 lit. c) DSGVO zu reduzieren, berät.

Vor dem Hintergrund des Grundsatzes der Datenminimierung, wonach die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss, regt der HmbBfDI insbesondere an, die zur Analyse erhobenen Daten zu anonymisieren, sobald der Auswertungszweck die Aufrechterhaltung des Personenbezugs nicht länger erfordert.

Eine Anonymisierung ist dabei zu bejahen, wenn in einem Datensatz alle personenbezogenen Daten entfernt wurden, so dass dieser Datensatz auch unter Hinzuziehung weiterer Informationen keiner einzelnen natürlichen Person zugeordnet werden kann. Wie dies im konkreten Fall umgesetzt werden kann, ist zum Berichtszeitpunkt Gegenstand von Gesprächen mit der BWI, die auch im Jahre 2024 fortgesetzt werden sollen.

18. Prüfung des Tracking bei Webshops

Die Nachverfolgung des Nutzungsverhaltens auf Webseiten oder in Apps ist in den meisten Fällen nur mit einer Einwilligung der Nutzenden zulässig. Im Berichtszeitraum führte der HmbBfDI auf Webseiten eines Versandhandelskonzerns umfassende Prüfungen zum Einsatz von Cookies und vergleichbaren Technologien durch.

Von einer europaweiten Beschwerdeaktion der Organisation NOYB waren auch Verantwortliche im Zuständigkeitsbereich des HmbBfDI betroffen. Gegenstand der Beschwerden waren Webseiten und dort

eingesetzte Consent-Lösungen, bei denen nach Auffassung der Organisation NOYB irreführende Cookie-Banner eingesetzt worden seien. Mit den vorgefundenen Gestaltungen seien datenschutzrechtliche Anforderungen an „freiwillige, für den bestimmten Einzelfall und in informierter Weise abgegebene" Einwilligungen nicht wirksam eingeholt worden. Zudem sei ein „Widerrufsbutton" auf der ersten Ebene des Cookie-Banners nicht vorhanden gewesen.

Da die Beschwerden inhaltlich identische Beschwerdegegenstände aufweisen, wurde für diesen Themenkomplex durch den Europäischen Datenschutzausschuss (EDSA) die Task Force „Cookie Banner" errichtet, an welcher der HmbBfDI mitwirkt. Auf diese Weise soll ein bestmöglich harmonisierter Ansatz zur Bearbeitung der Beschwerden durch die jeweils zuständigen mitgliedstaatlichen Behörden gewährleistet werden. Der Abschlussbericht der Task Force wurde unter https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en veröffentlicht.

Das geprüfte Unternehmen des Versandhandelskonzerns, die ABOUT YOU SE & Co. KG, ist europaweit tätig und betreibt unter vielen europäischen Top-Level-Domänen einheitlich gestaltete Webshops. Bei den vier eingereichten Beschwerden zu Webseiten des Konzerns handelt es sich zum einen um eine Webseite mit der Top-Level-Domäne .de, zum anderen um drei weitere Webshops für Mitgliedsstaaten unter deren jeweiligen Top-Level-Domänen.

Für die Prüfung des deutschen Webshops kamen zusätzlich zu den Vorgaben der DSGVO auch diejenigen des TDDSG als nationale Umsetzung der ePrivacy-Richtlinie zur Anwendung.

Für die Speicherung von oder den Zugriff auf Informationen in einer Endeinrichtung (z. B. Mobiltelefon, Tablet oder PC) ist eine wirksame Einwilligung gemäß § 25 Abs. 1 Satz 1 TTDSG i. V. m. Art. 4 Nr. 11 DSGVO einzuholen, soweit dies nicht ausnahmsweise nach § 25 Abs. 2 Nr. 2 TTDSG entbehrlich ist. Für die nachgelagerte

Verarbeitung personenbezogener Daten ist es erforderlich, dass eine Rechtsgrundlage vorliegt. In der Regel kann auch diese nur auf eine Einwilligung gestützt werden.

Anlässlich der o.g. Beschwerden wurde die Webseite zu verschiedenen Zeitpunkten aufgerufen und dokumentiert, ob und unter welchen Umständen Daten von Besucher:innen mithilfe von Cookies und ähnlichen Technologien verarbeitet worden sind. Dabei wurden zahlreiche Vorgänge festgestellt, die nicht als unbedingt erforderlich i. S. d. Ausnahmeregelung des § 25 Abs. 2 Nr. 2 TTDSG zu bewerten sind und für die auch keine wirksamen Einwilligungen eingeholt wurden.

Im Verlauf des Anhörungsverfahrens hat das verantwortliche Unternehmen umfassende Anpassungen vorgenommen und damit die jeweiligen Datenschutzanforderungen nach dem TTDSG und der DSGVO umgesetzt. Einwilligungsbedürftige Zugriffe auf Endeinrichtungen der Nutzer:innen sowie die sich daran anschließende nachgelagerte Verarbeitung personenbezogener Daten werden seitdem nur noch nach vorheriger informierter Einwilligung vorgenommen. Das Unternehmen hält dazu nun auf der ersten Ebene der Consent-Lösung eine Funktion „Ablehnen“ vor, mit der das Ablehnen einwilligungsbedürftiger Einträge ebenso einfach mit einem Klick ermöglicht wird wie die Erteilung der Einwilligung.

Soweit die Beschwerde das Fehlen eines expliziten „Widerrufs-Buttons“ rügt, sieht der HmbBfDI darin keinen Datenschutzverstoß. Dies entspricht der in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) erarbeiteten Orientierungshilfe für Anbieter:innen von Telemedien (OH Telemedien, siehe auch 31. TB Datenschutz 2022, Kap. III 13):

> *„Sofern die Verlinkung die Nutzenden direkt an die Stelle zur Möglichkeit des Widerrufs leiten und gerade keine Suchvorgänge nötig sind, kann eine direkt auffindbare Widerrufsmöglichkeit auch in einer Datenschutzerklärung platziert werden.“*

Zu diesem Ergebnis kommt auch die Task Force Cookie Banner. Nach dieser kann Betreiber:innen von Webseiten nur vorgegeben werden, leicht zugängliche Lösungen zur Wahrnehmung des Widerrufsrechts vorzuhalten. Nicht vorgeschrieben werden kann dagegen, eine bestimmte Lösung zur Ermöglichung des Widerrufs wie z. B. ein „schwebendes Symbol" („Hovering Button") an einer bestimmten Stelle vorzuhalten.

Wegen der festgestellten Datenschutzverstöße nach § 25 TTDSG und Art. 5 Abs. lit. a und Art. 6 Abs. 1 lit. a DSGVO wurde in dem Verfahren zur Webseite unter der „.de" Top-Level-Domäne eine Verwarnung nach Art. 58 Abs. 2 lit. b DSGVO ausgesprochen.

Die Prüfung der Beschwerden, die Webseiten von About You unter Top-Level-Domänen europäischer Mitgliedsstaaten betreffen, haben im DSGVO-Bereich vergleichbare Datenschutzverstöße aufgezeigt. Im Ergebnis des beim HmbBfDI geführten Verfahrens und diesbezüglicher Erörterungen hat das Unternehmen alle weiteren seiner europäischen Webseiten und Webshops zwischenzeitlich umgestellt und datenschutzrechtlich umfassend angepasst.

Wegen des grenzüberschreitenden Charakters der Beschwerden betreibt der HmbBfDI als federführende Aufsichtsbehörde das Kooperationsverfahren nach Art. 60 DSGVO, um betroffene Aufsichtsbehörden der Mitgliedsstaaten über die Verfahren in Kenntnis zu setzen und eine diesbezügliche Entscheidung abzustimmen. Das Kooperationsverfahren dauert an.

Berichte

1. Intelligente Videoüberwachung Hansaplatz

Die eingesetzte intelligente Videoauswertungssoftware „IVBeo“ stellt nach Prüfung des HmbBfDI den Versuch dar, einen Beobachter zu schaffen, der nicht so abgelenkt werden kann wie ein menschlicher Betrachter. Die Software bewirkt aber noch keine qualitativ tiefere Erschließung der Informationen.

Seit August 2019 werden der Hansaplatz und angrenzende Straßen im Stadtteil St. Georg von der Polizei Hamburg an bestimmten Tagen und zu festgelegten Uhrzeiten videoüberwacht. Diese gefahrenabwehrrechtliche Maßnahme war bereits Gegenstand einer umfangreichen Prüfung des HmbBfDI (vgl. 29. TB Datenschutz 2020 S. 64 ff.).

Durch eine Presseanfrage am 12.5.2023 wurde der HmbBfDI auf eine geplante technische Aufrüstung der Videoüberwachungsanlage am Hansaplatz aufmerksam gemacht. Auf Nachfrage des HmbBfDI bei der Polizei wurde ein Projektstart zum 14.7.2023 in Aussicht gestellt. Am 12.6.2023 erhielt der HmbBfDI Unterlagen zur Prüfung. Am 28.6.2023 wurde die Anlage im Polizeikommissariat am Steindamm (PK11) dem HmbBfDI vorgestellt.

Das System IVBeo befindet sich bereits durch die Polizei Mannheim im Einsatz und sollte in Hamburg zunächst ein auf drei Monate begrenzter Pilotversuch einer intelligenten Auswertung von Videodateien sein. Ab dem 14.7.2023 wurden die Bilder von vier Kameras zusätzlich zu der einfachen Videoüberwachung durch eine Software verarbeitet. Durch die intelligente Videobeobachtung wurden die Datenströme aus den vier ausgewählten Kameras hinsichtlich auffälliger Bewegungsmuster (z.B. Schläge, Tritte, Stürze) ausgewertet. Wenn IVBeo ein solches Muster erkennt, spielt das System das Live-Bild ohne weitere Hervorhebungen auf einem separaten Monitor ab und zeitgleich werden die anwesenden Polizeibeamt:innen durch

Signal auf die Gefahrensituation aufmerksam gemacht. Die Entscheidungsfindung, ob tatsächlich eine Gefahr vorliegt und weitere Maßnahmen zu treffen sind – z.B. Entsendung von Einsatzkräften –, liegt dabei stets beim menschlichen Beobachter.

Das System lernte in Hamburg im Rahmen des Pilotversuchs nicht selbstständig neue Muster, sondern arbeitet auf Basis der Mustererkennungen des Systemeinsatzes in Mannheim. Nach Angaben der Polizei Hamburg ist IVBeo menschlichen Beobachtern in manchen Aspekten der Konzentration und Fehlererkennung über lange Zeiträume am Stück überlegen. Während der menschliche Beobachter potentiell immer das gesamte Bild und damit auch viele Unbeteiligte wahrnimmt, löscht die (idealisierte) intelligente Technik die irrelevanten Szenen innerhalb einer logischen Sekunde und gibt nur den Hinweis auf tatsächliche Störer an menschliche Beobachter weiter.

Mitte Oktober wurde dieser Versuch nach Mitteilung der Polizei Hamburg zunächst planmäßig beendet, um in eine Evaluationsphase überzugehen. Projektbericht und Evaluation wurden dem HmbBfDI im weiteren Verlauf zugeleitet und in einem Vor-Ort-Termin am 1.12.2023 ausführlich erläutert.

Nach Prüfung der Sach- und Rechtslage, sowohl zu Beginn der Pilotphase als auch nach deren Abschluss, bestanden zunächst keine durchgreifenden datenschutzrechtlichen Bedenken. Grundproblem bei der Bewertung des Systems ist allerdings, dass selbstlernende Systeme ihre Handlungsweise nicht wie ein Mensch begründet erklären können und sollen. Diese bestehenden Unwissenheitsrisiken konnten auch durch den Pilotversuch nicht ausgeräumt werden.

Das System IVBeo als Ergänzung der Videoüberwachung am Hansaplatz verarbeitet personenbezogene Daten und führt zu einem Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen. Für die Verwendung des ergänzenden Systems ist somit eine Rechtsgrundlage notwendig. Die Polizei Hamburg stützt sowohl die einfache Videoüberwachung am Hansaplatz als auch IVBeo auf

§ 18 Abs. 3 Gesetz über die Datenverarbeitung der Polizei (PolDVG). Diese Ermächtigungsgrundlage erlaubt der Polizei neben der Videobeobachtung grundsätzlich auch die einfache Verarbeitung von Bildaufzeichnungen zur vorbeugenden Bekämpfung von Straftaten. Eine (weitere) Verarbeitung von Aufzeichnungen kann jedoch nur dann auf § 18 Abs. 3 PolDVG gestützt werden, wenn die (anschließende) Verarbeitung nicht wesentlich tiefer in die Grundfreiheiten von Bürger:innen eingreift, als die vorher erfolgte einfache Videoüberwachung. Hinweise auf einen qualitativ intensiveren, zusätzlichen Eingriff durch die automatisierte Auswertung neben der reinen Videoüberwachung ergaben sich aus der Prüfung, Evaluation und dem Projektbericht bisher aber nicht. Anders als beim Einsatz anderer, komplexer Systeme, soll keine neue Auswertungstiefe erreicht werden, die Daten sollen weder neu verknüpft noch mehrstufigen Analysen unterzogen werden. Die Eingriffstiefe ist daher im Ergebnis nicht wesentlich höher und vor allem qualitativ nicht anders zu beurteilen als die bisherige Überwachung. Es ist insgesamt die Tendenz zu entnehmen, dass das System allenfalls einen brauchbaren Assistenten darstellt.

Eine Neubeurteilung der Eingriffstiefe mit dem Ende des Pilotversuchs ist zunächst ebenfalls nicht notwendig. Die eingesetzte Technologie verfügt in der Gesamtschau über die Fähigkeiten und Beschränkungen, wie diese auch aus den bisher dem HmbBfDI vorgelegten Dokumenten hervorgingen. Aus der Evaluierung ergab sich, dass bei einer Vielzahl von Detektionen für die Polizei Hamburg nicht nachvollziehbar war, warum das System anschlug. Durch den menschlichen Beobachter konnte in diesen Fällen letztlich keine Gefahrensituation erkannt werden. Ob es sich um Fehldetektionen handelte, war so nicht abschließend bewertbar. Dies schränkt die Belastbarkeit der vorgelegten Evaluation deutlich ein.

Die Vision, dass in Zukunft eine Verringerung der Eingriffsintensität der Beobachtung durch die Polizei erreicht werden kann, weil nur bei Erkennungen durch das intelligente System auch eine Beobachtung durch einen Menschen erfolgt (Hinweis auf Bildschirm), bleibt

daher erstmal eine Zielvorstellung des Projekts. Vom Ersatz menschlicher Polizeiarbeit durch eine Maschine ist das System – wie auch die Ergebnisse aus Mannheim vermuten ließen – noch weit entfernt. Realistisch betrachtet wird sich mittelfristig nur ein weiterer Parallelbetrieb der konventionellen und der intelligenten Überwachung im Hinblick auf die Gefahrenabwehr verantworten lassen. Auch das Kernprojekt in Mannheim wurde um drei weitere Jahre verlängert.

Diskriminierungsrisiken wurden in der Stellungnahme des HmbBfDI gemäß Art. 60a Abs. 4 Hamburgische Verfassung vom 4.7.2023 an die Bürgerschaft als schwer bewertbar dargestellt. Jedenfalls wurden in den Auswertungen keine Hinweise erkennbar, dass z.B. abweichende Bewegungsmuster durch (körperliche) Behinderungen einen relevanten Teil der Fehlerkennungen des Systems ausmachten. Dies mag mit der durch IVBeo genutzten positiven Mustererkennung zusammenhängen: Das System erkennt nicht negative Abweichungen von einem – wie auch immer zu definierenden – „normalen" Bewegungsablauf, sondern erkennt positiv bestimmte antrainierte negative Muster wie Treten, Schlagen, Stürzen. Die vom HmbBfDI bereits an der bisherigen Videoüberwachungsanlage gerügten technischen Absicherungen im Hinblick auf eine rechtskonforme Protokollierung von Datenzugriffen und Ausleitungen sowie die Anforderungen an eine ordnungsgemäße Nutzerauthentifizierung bleiben allerdings weiterhin offen. Auch nach dem Pilotversuch wurden dem HmbBfDI insoweit keinerlei Verbesserungen bekannt. Eine Authentifizierung mit Chipkarten soll nach letzter Mitteilung der Polizei Hamburg wohl umgesetzt worden sein. Details sind dem HmbBfDI bis Redaktionsschluss jedoch nicht zugegangen. Ob die gewählte Umsetzung wie bemängelt nun die personengenaue Zuordnung der Zugriffe ermöglicht, bedarf weiterer Sachaufklärung.

Das Gesamtergebnis weckt auf Seiten der Polizei Hamburg den Wunsch, auch in Hamburg das System weiter trainieren und lernen lassen zu können. Die Weiterentwicklung wirft jedoch seitens des HmbBfDI einige rechtliche Fragen auf. Eine Fortentwicklung der intelligenten Beobachtung durch Verwendung von Realdaten u.a. von

unbeteiligten Passanten auf einem öffentlich zugänglichen Platz erscheint verfassungsrechtlich nicht von vornherein unmöglich. Ob dafür aber bereits eine gesetzliche Grundlage existiert, ist wohl zu verneinen. Mangels Vorlage konkreter Entwicklungsschritte durch die Polizei Hamburg konnten diese bisher jedoch nicht abschließend bewertet werden. Allgemein entsteht der Eindruck, dass bei anstehenden Reformen des PolDVG dem Themenkomplex KI eine größere Aufmerksamkeit zukommen muss. Dies betrifft nicht nur den bereits vom Bundesverfassungsgericht teilweise für verfassungswidrig erklärten § 49 PolDVG (vgl. 31. TB Datenschutz 2022, S.76), sondern insbesondere den Bereich der Videoüberwachung. Die exekutive Gefahrenabwehrtätigkeit soll nicht behindert werden und braucht in einigen Bereichen ein Update. Sie muss aber durch den Gesetzgeber auf ein solides rechtliches Fundament gestellt werden. Die Möglichkeiten und Grenzen der Technik dürfen nicht auf Grundlage weit gefasster, beliebiger Normen letztendlich der Exekutive überlassen werden. Hier ist der Gesetzgeber gefragt, einen angemessenen Ausgleich von Sicherheit und Freiheit herbeizuführen.

2. Einsatz von Microsoft 365 in der FHH

Microsoft 365 soll nach Vorstellung der Senatskanzlei in der Freien und Hansestadt Hamburg (SK) perspektivisch flächendeckend zum Einsatz kommen. Entscheidende datenschutzrechtliche Fragen sind bislang nicht abschließend beantwortet worden. Es bleibt im Berichtszeitraum offen, ob und wann deutschlandweite Forderungen der Datenschutzkonferenz (DSK) durch die Senatskanzlei für Hamburg umgesetzt werden können.

Im Berichtszeitraum führte der HmbBfDI intensive Gespräche mit der Senatskanzlei (SK) zum Einsatz von Microsoft 365 in der FHH. Nachdem die SK zunächst seit 2019 die prinzipielle Nutzbarkeit für eine ausgewählte Zahl von Test-Nutzenden in Form eines Proof of Concepts bestätigt hat, wurde im 3. Quartal 2023 begonnen, die

Verarbeitung auf produktive Umgebungen zu migrieren (sog. Minimum Viable Produkt, MVP).

Mitte des Jahres gab es eine erste Ankündigung der SK zum vorgesehenen Nutzungskonzept im sog. Projekt BestCloudBasis (BCB). Dieses wurde dem HmbBfDI vorgestellt, um einen Einblick in die geplanten Funktionalitäten zu erhalten. Neben den grundsätzlichen Büroanwendungen Word, Excel, PowerPoint, Visio und OneNote waren auch der Einsatz von OneDrive for Business, Whiteboard, Planner, Search, SharePoint, Outlook, Teams und Viva Engage vorgesehen. Somit stellt das Projekt weit mehr als nur eine Ablösung der bislang bestehenden Office-Anwendungen auf Büroarbeitsplätzen dar. Es gestaltet vielmehr die grundsätzliche Arbeitsumgebung der ausgestatteten Nutzenden völlig neu. Der Übergang vom PoC zum MVP wurde ebenfalls angekündigt, sodass zu dem Zeitpunkt feststand, dass spätestens ab September 2023 eine produktive Nutzung möglich sein soll. Datenschutzrechtliche Unterlagen konnten zu dem Zeitpunkt noch nicht vorgelegt werden. Daraufhin wurde ein Folgetermin vereinbart, sobald die Datenschutzunterlagen erstellt sind. Bereits kurz darauf wurde dem HmbBfDI mitgeteilt, dass die SK fachliche „Anregungen" für den Regelbetrieb entgegennehmen wird, diese jedoch „zeitig vorliegen sollten", um noch berücksichtigt werden zu können. Ebenso wurde eine Telemetrie-Messung in Aussicht gestellt, deren Durchführung „zu einem späteren Zeitpunkt" nachgereicht würde.

An dieser Stelle ist festzuhalten, dass für eine fundierte und belastbare Prüfung aller datenschutzrechtlich relevanter Verfahren stets ausreichend Zeit einzuplanen ist, damit Projekte nicht Gefahr laufen, die Grundrechte der betroffenen Personen mangels ausreichender Zeitpuffer hintenanstellen zu müssen.

Der HmbBfDI wies die SK daher darauf hin, dass anzunehmen sei, dass es solche Anmerkungen und Nachfragen mit hoher Wahrscheinlichkeit geben werde und bezog sich dabei auch auf die Ausführungen der Konferenz der unabhängigen Datenschutzaufsichts-

behörden des Bundes und der Länder (DSK), die im November 2022 festgestellt hat, dass die für den Einsatz von „Microsoft 365“ vorgesehene Standard-Auftragsverarbeitungsvereinbarung von Microsoft (Products and Services Data Protection Addendum, kurz „DPA“) nicht den Anforderungen des Art. 28 Abs. 3 DSGVO entspricht. Die DSK machte konkrete Problemfelder aus, auf die es bei der Evaluierung zur möglichen Nutzung von Microsoft 365 zu achten gilt. In Anknüpfung an diese Problemfelder haben mehrere Datenschutzaufsichtsbehörden gemeinsam eine Handreichung für die Verantwortlichen und konkrete, dezidierte Vorschläge für eine Zusatzvereinbarung erarbeitet, um diese dabei zu unterstützen, auf entsprechende vertragliche Änderungen hinzuwirken. So sind laut der Handreichung etwa die im DPA aufgeführten Löschfristen vertraglich anzupassen, ferner werden in der Handreichung die Anforderungen an die Information über den Einsatz von Unterauftragsverarbeitern aufgeführt. Ein weiterer wichtiger Aspekt der Handreichung ist der Umgang mit der Verarbeitung durch Microsoft zu eigenen Geschäftszwecken, den entsprechenden Textpassagen dazu im DPA und den Fragen zur Sicherstellung einer hinreichenden Weisungsbindung.

Die SK stellte dem HmbBfDI Ende Juli Datenschutzunterlagen zur Verfügung, die von der behördlichen Datenschutzbeauftragten abgenommen waren. Dazu zählten insbesondere eine Datenschutzfolgeabschätzung und eine Beschreibung der Verarbeitungstätigkeit. Aufgrund der erheblichen Bedeutung des Vorhabens für die hamburgische Verwaltung erfolgte die Bearbeitung beim HmbBfDI daraufhin mit hoher Priorität und hohem Personaleinsatz. Es wurden diverse Fragen und offene Punkte ausgemacht und an die SK zurückgemeldet. Ende August, kurz vor Beginn der Produktivsetzung, erfolgte schließlich der Austausch hierzu. Es wurde dann für eine zielgerichtete Zusammenarbeit vereinbart, dass die Fragenliste abschnittsweise in einzelnen Workshops besprochen und beantwortet werden soll. Die Workshops begannen im September und setzten sich in den folgenden zwei Monaten in enger Taktung fort. Vertreten war die SK mit anwaltlicher Unterstützung und eine Delegation des HmbBfDI aus technischen und rechtlichen Experten. Inhaltlich wurde

über die Aspekte der Auftragsdatenverarbeitung, Datenschutzfolgenabschätzung, Beschreibung der Verarbeitungstätigkeiten, Feinkonzepte (SharePoint Online, OneDrive for Business, Teams) sowie die generelle Projektplanung 2024 gesprochen. Zum Thema sollte eigentlich auch die ausgewertete Telemetrie-Analyse werden, die aber bis zum Ende des Berichtszeitraums nicht abgeschlossen werden konnte.

Es ist nach Abschluss der Workshop-Reihe festzuhalten, dass trotz intensiver Bemühungen grundlegende Fragestellungen noch nicht beantwortet werden konnten und Bedenken bezüglich der Rechtskonformität bestehen bleiben. Konkret geht es um Fragestellungen, die bereits vor einem Jahr durch die Datenschutzkonferenz herausgearbeitet worden sind und weiterhin im Raum stehen:

- Die genannten Problemfelder wirken sich insbesondere bei Funktionen aus, die von Microsoft als Verbundene Erfahrungen (Connected Experiences) bezeichnet werden und laut Microsoft „Inhalte analysieren“ und Office-Inhalte nutzen, um dem Nutzer „Designempfehlungen, Bearbeitungsvorschläge, Datenerkenntnisse und ähnliche Funktionen bereitzustellen“. Hierzu werden nicht näher genannte Informationen zu Zwecken von Microsoft aus der Umgebung der Kunden an Microsoft übermittelt. Die Gründe, aus denen Microsoft bestimmte Daten, die im Rahmen von Connected Experiences übermittelt werden, für einen bestimmten Zeitraum behalten darf, sind nicht abschließend erläutert. Zudem fehlt die Möglichkeit, einzelne Connected Experiences zu deaktivieren. Es ist lediglich möglich, teilweise auch gewünscht, Funktionalitäten wie Übersetzungsfunktionen vollständig zu deaktivieren. Die Einflussmöglichkeiten des oder der Verantwortlichen sind schon aufgrund dieses Automatismus in Bezug auf die Menge des Datenflusses eingeschränkt. Damit kann nicht ohne weiteres vermieden werden, dass Inhaltsdaten des Hoheitsträgers in den Zugriffsbereich von Microsoft gelangen, was angesichts der festgestellten Probleme im Bereich der Weisungsbindung und Verarbeitung von Auftragsdaten zu eigenen Geschäftszwecken zu einem Risiko werden könnte.

- Die Weisungen bei Vertragsbeginn sind nicht ausreichend dokumentiert und es fehlt an einer gemessen an Art.5 Absatz 2 DSGVO ausreichenden Aufstellung aller Weisungen und Voreinstellungen.
- Der Vorbehalt im Data Protection Addendum (DPA), dass Microsoft Daten zu eigenen Zwecken verarbeiten können soll, ist nicht transparent erläutert. Die tatsächlichen Zwecke sind nicht hinreichend erklärt. Weitere Erläuterungen von Microsoft sind bislang für den HmbBfDI nicht verfügbar, weil sie durch Microsoft gegenüber der SK als vertraulich gekennzeichnet sind.
- Die vorstehenden Punkte führen zu Frage, ob alle im Zusammenhang mit der Nutzung von Microsoft 365 auftretenden Verarbeitungsvorgänge tatsächlich von der genannten Rechtsgrundlage gedeckt sind und ob Grundsätze der Datensparsamkeit gewahrt sind.

Aus technischer Sicht wurden für eine nachvollziehbare Konfiguration des Dienstes Microsoft 365 sog. Feinkonzepte entworfen, aus denen die jeweils gewählten Parameter des hamburgischen Tenants (Bezeichnung für die Kundenumgebung der FHH bei Microsoft Azure) hervorgehen. Aus diesen Feinkonzepten ergeben sich einige Klarstellungen bzgl. der gewählten Konfigurationen und der damit verbundenen Datenverarbeitungen. Dies ermöglicht sowohl den Verantwortlichen als auch dem HmbBfDI eine fundierte Prüfung der technischen Rahmenbedingungen. Teilweise belegen die Feinkonzepte jedoch auch, dass vorgegebene Standardwerte von Microsoft ohne weitere Überprüfung übernommen worden sind. Dies ist umso kritischer, da Microsoft zu einigen Parametern keine öffentlich verfügbare Dokumentation anbietet und daher durch den HmbBfDI nicht überprüft werden kann, welches Verhalten und ggf. welche Verarbeitungen personenbezogener Daten dadurch hervorgerufen werden.

Die SK hatte Dataport beauftragt, die Feinkonzepte zu erstellen und fortzuschreiben. Jedoch wird klar, dass bislang nicht zu allen weiteren genutzten Diensten von Microsoft 365 solche Feinkonzep-

te und damit dokumentierte Konfigurationen zum Ende des Workshop-Prozesses vorliegen. So existieren zu den Kernkomponenten der Office-Anwendungen (Word, Excel, Powerpoint etc.) solche Informationen nicht. Aus diesem Grund ist im Ergebnis bislang nicht abschließend prüfbar, inwieweit das Verfahren Microsoft 365 den Grundsätzen aus Art. 5 DSGVO entspricht.

Positiv ist festzuhalten, dass die SK mit Microsoft in die von der DSK und dem HmbBfDI geforderte Vertragsnachverhandlung eingestiegen ist. Hier bleibt jedoch ein konkretes Ergebnis offen und es ist nicht absehbar, ob und in welchem Umfang Microsoft hier die geforderten Anpassungen zusichern wird.

Ebenso bleibt offen, ob das Projekt mit seinem Ende einer echten – und ursprünglich zu Beginn des Projekts in Aussicht gestellten – Evaluierung und einem Abgleich der Funktionalitäten zum Best-CloudBasis-Projekt in Schleswig-Holstein unterzogen wird. Die bereits vollzogene Lizensierung von bislang 3000 Lizenzen, von denen bislang 1000 in Benutzung sind, und der Umstand, dass den hamburgischen Behörden ausschließlich der Weg hin zu Microsoft 365 angeboten wird, lässt erahnen, dass es aus Sicht der SK keine Alternative geben wird.

Für Behörden mit erhöhten Sicherheitsanforderungen, sog. hohem Schutzbedarf, gibt es darüber hinaus noch gar keinen absehbaren Pfad, der bis zum Ende des Supportzeitraums der bestehenden Office 2019-Umgebung Ende 2025 zu gehen ist. Sollte sich in 2024 herausstellen, dass Anforderungen von diesen Behörden nicht erfüllt werden können, gibt es zum heutigen Stand keinerlei kommunizierte Backup-Strategie.

Zum Redaktionsschluss hat der HmbBfDI bereits weitere Austausche mit der SK in 2024 vereinbart. Es gilt, dass die bislang ungelösten Fragestellungen schnellstmöglich gelöst werden müssen. Hierfür wird es darauf ankommen, produktbezogen und detailliert die bisherige Planung zum vorgesehenen Betriebsumfang zu über-

prüfen sowie feingranular über alle einzusetzenden Dienste und die jeweiligen Einstellungsparameter, inkl. der damit verbundenen rechtlichen und technischen Implikationen, zu diskutieren.

3. Microsoft Rights Management System (RMS) in der FHH

Eine anstehende, technisch notwendige Änderung an RMS gefährdet die Verfügbarkeit bisher verschlüsselter Inhalte und potentiell personenbezogener Daten. Der HmbBfDI berät und stellt die Notwendigkeit von technisch besonders geschützter Kommunikation heraus.

Der HmbBfDI erfuhr im Mai 2023, dass das in der FHH u.a. als Schutz von E-Mails eingesetzte RMS aufgrund technischer Probleme nicht wie bisher weiterbetrieben werden kann. Stattdessen soll in geänderter Konfiguration ein Neuaufbau der zentralen Schlüsselhierarchie erfolgen. Folge des Neuaufbaus wird eine Diskontinuität der Verfügbarkeit bisheriger geschützter Inhalte sein. Alle bis zum Zeitpunkt des Neuaufbaus mit RMS geschützten Inhalte können dann nicht mehr entschlüsselt werden und werden daher unlesbar. Für alle RMS-geschützten Inhalte droht dadurch ein vollständiger Datenverlust, sofern diese nicht bereits oder spätestens bis zum Umschalttermin in anderer Form gespeichert wurden. Konkret betrifft dies RMS-geschützte E-Mails und bestimmte Anhänge in Microsoft Exchange, aber auch msg-Dateien oder Office-Dateien, die aus solchen E-Mails in Dateiablagen oder Aktensystemen gespeichert wurden.

RMS bietet seit 2014 allen FHH-Beschäftigten die Möglichkeit, interne E-Mails und Office-Dokumente zusätzlich zur Transportverschlüsselung mit einem stärkeren Vertraulichkeitsschutz zu versehen. Zwar stellt RMS keine vollwertige Ende-zu-Ende-Verschlüsselung dar, bietet aber zusätzlichen Zugriffsschutz für persönliche Kommunikation oder Inhalte mit höherem Schutzbedarf.

Im Lichte einer Neubeurteilung der Schutzmaßnahme RMS oder möglicher Alternativen positionierte sich der HmbBfDI in einem umfassenden Vermerk klar zur Aufrechterhaltung vergleichbarer technischer Angebote an Beschäftigte und Behörden. Der HmbBfDI sieht es als erforderlich an, dass Beschäftigten weiterhin Mittel zur Verfügung stehen, um fachlichen E-Mailverkehr beim Umgang mit sensiblen personenbezogenen Daten sowie vertrauliche nicht-fachliche Kommunikation wirksam vor unbefugter Kenntnisnahme zu schützen. Aus der Rechtsprechung des VG Mainz (Az. 1 K 778/19.MZ), aus einschlägigen Orientierungshilfen der Datenschutzkonferenz, aber auch aus FHH-eigenen Vereinbarungen (94er-Vereinbarung zur Bürokommunikation, TK-RL) ergeben sich Pflichten, in solchen besonderen Fällen Maßnahmen zu ergreifen, die über die Schutzwirkung einer Transportverschlüsselung hinaus gehen.

Die bevorstehende Diskontinuität von RMS wirft die Frage auf, ob RMS als mittel- und langfristige Lösung für diese Bedarfe weiterhin belastbar zur Verfügung steht. Der HmbBfDI rät dringend dazu, die Risiken für den zuverlässigen Betrieb von RMS zu re-evaluieren sowie frühzeitig nach standardkonformen und nachhaltigen Alternativen zu suchen.

Für die Abwendung von massiven Datenverlusten in Folge der Umstellung ist der HmbBfDI im Austausch mit den betroffenen Behörden. Als Stichtag der Umstellung ist nach mehrfach wiederholter Verschiebung derzeit der 29.02.2024 terminiert. Der Stand der Inventarisierung und Sicherung betroffener Inhalte in den Behörden ist derzeit weitgehend unbekannt.

4. Unterarbeitsgruppe Verschlüsselte Kommunikation

Die Informationssicherheitsbeauftragten der FHH diskutieren bestehende Verschlüsselungsstandards zur Kommunikation per E-Mail, um eine einheitliche Lösung für die FHH zu etablieren. Auch der HmbBfDI ist in dieser Unterarbeitsgruppe vertreten.

Zu Beginn des Jahres 2023 stellte Dataport das Projekt „Verschlüsselungsgateway" oder „zentraler Mailgateway" (ZGW) in verschiedenen Gremien der FHH vor. Ziel ist der Aufbau eines Dienstes für die Kommunikation von Steuer- und Finanzeinrichtungen. Mit der Vorstellung signalisierte Dataport eine Möglichkeit der Nutzung für weitere Behörden und Ämter. Präsentiert wurde das Projekt auch in der Arbeitsgruppe Informationssicherheitsmanagement (InSiMa), die regelmäßig durch das Amt für IT und Digitalisierung (ITD) der Senatskanzlei organisiert wird. In der Diskussion im Anschluss zur Vorstellung des ZGW stellte man Interesse und Bedarf an verschlüsselter Kommunikation fest, die allerdings über den Rahmen des geplanten Projektes hinaus gehen. Parallel zur Abschaltung des Microsoft Active Directory Rights Management Services (RMS, vgl. Kap. III 3) sollte auch die Möglichkeit bestehen, mit Teilnehmern außerhalb der FHH verschlüsselt Nachrichten auszutauschen. Die geschützte Kommunikation per E-Mail sollte besonders im Vordergrund stehen.

Mit der Gründung einer Unterarbeitsgruppe wollte man die Bedarfe und die bestehenden Lösungsangebote genauer betrachten. Neben dem geplanten ZGW wurden auch die Standards zur E-Mail-Verschlüsselung S/MIME und OpenPGP, sowie der Einsatz der elektronischen Poststelle mit dem zugrunde liegenden Protokoll für das elektronische Gerichts- und Verwaltungspostfach für den Einsatz in der FHH evaluiert. Um tiefere Einblicke in Konzepte und Handhabung zu erlangen, lud man Fachpersonal und Projektleitungen der jeweiligen Lösungen von Dataport und CERT Nord ein. Es wurden mögliche

Einsatzszenarien mit verfügbarer Software und die Vor- und Nachteile diskutiert.

Der HmbBfDI beteiligte sich an der Evaluation und sprach sich für die Variante aus, die eine Verwaltung von Kommunikationsteilnehmern mit echter Ende-zu-Ende-Verschlüsselung gestattet. Hierfür ist es dem HmbBfDI wichtig, auf einen Standard zu setzen, der unabhängig von Herstellern oder spezieller Hardware funktioniert. Ein Datenverlust, wie er durch die Abschaltung des bisherigen RMS-Dienstes entsteht, sollte durch zukünftige Lösungen ausgeschlossen werden. Nach dem Aufbau einer Public-Key-Infrastruktur mit öffentlichen, zentral verwalteten Zertifikaten wäre der Einsatz von S/MIME für jeden Arbeitsplatz der FHH ohne technische Hürden oder Kompromisse verfügbar.

Bisher besteht eine Entscheidungsfreiheit bei jeder einzelnen Behörde, wodurch keine einheitliche, stadtübergreifende verschlüsselte Kommunikation stattfinden kann. Eine allgemeine Lösung für den verschlüsselten Nachrichtenaustausch mit Kommunikationspartnern außerhalb des FHH-Netzes ist bislang noch viel weniger vorstellbar. Nicht jede Behörde kann die finanziellen und fachspezifischen Mittel aufbringen, eine geeignete Lösung aufzubauen. In der Unterarbeitsgruppe kam es während ihres Bestehens aufgrund der unklaren Bedarfe in den einzelnen Behörden und Ämtern zu keiner Entschließung. Vielmehr sieht der CISO der Senatskanzlei Handlungsbedarf und nimmt das Thema für 2024 mit in die Entscheidungsgremien der IT-Leitungen.

5. Checkliste zum Einsatz künstlicher Intelligenz

2023 war das Jahr, in dem künstliche Intelligenz (KI) sprunghaft in das Bewusstsein der Öffentlichkeit gerückt ist. Die einfache Verfügbarkeit leistungsstarker Chatbots hat Wirtschaft und Verwaltung zu der Möglichkeit inspiriert, ihre Abläufe mithilfe von KI-Anwendungen effizienter zu gestalten. Der HmbBfDI hat als erste Datenschutzbehörde einen Leitfaden dazu veröffentlicht, auf welche Aspekte dabei zu achten ist.

Generative KI in Form von Chatbots bietet die Möglichkeit, schnell und unkompliziert Inhalte zu erstellen. Bekannte Large Language Models (LLM) sind ChatGPT, Luminous oder Bard. In vielen Einrichtungen sind die Tools mittlerweile Teil des Arbeitsalltags geworden, oft jedoch ohne verbindliche Vorgaben zur Nutzung. Dass die Sprachmodelle üblicherweise in einer Cloud betrieben werden, birgt verschiedene Datenschutzrisiken. Zum einen ist der Schutz vertraulicher Daten gefährdet, weil viele Unternehmen mit demselben LLM-Modell cloudbasiert arbeiten, Eingaben für das weitere Training der Modelle genutzt werden und ihnen dadurch möglicherweise Geschäftsgeheimnisse und persönliche Daten übermittelt werden. Zum anderen besteht die Gefahr, personenbezogene Daten aufgrund unrichtiger Ergebnisse unzulässig zu verarbeiten, gerade bei besonders schützenswerten Datenkategorien. Die folgende Checkliste dient Unternehmen und Behörden als Leitfaden zur datenschutzkonformen Nutzung von Chatbots. Für die nähere Zukunft ist ein abgestimmter Leitfaden der Datenschutzkonferenz beabsichtigt, der sich voraussichtlich auch an der Checkliste des HmbBfDI orientieren wird.

1. Compliance-Regelungen vorgeben

Formulieren Sie klare und dokumentierte interne Weisungen, ob beziehungsweise unter welchen Voraussetzungen welche Tools infrage kommen. Konkrete Beispiele der zugelassenen und der untersagten Einsatzszenarien helfen bei der Verdeutlichung.

Wer keine internen Regelungen vorgibt, ob und wie generative KI im Arbeitsalltag eingesetzt werden darf, kann davon ausgehen, dass sich Beschäftigte und andere Angehörige der Organisationen eigenmächtig und unkontrolliert der neuartigen Hilfsmittel bedienen. Unter Umständen haftet für diese Handlungen die arbeitgebende Einrichtung.

2. Datenschutzbeauftragte einbinden
Beziehen Sie immer Ihre oder Ihren internen Datenschutzbeauftragte:n ein, wenn Sie interne Weisungen erstellen oder einen Anwendungsfall erstmals umsetzen. Je nach Anwendungsfall sollten Sie in dem Zuge eine Datenschutz-Folgenabschätzung erstellen. Gegebenenfalls kann es auch sinnvoll sein, Betriebs- und Personalrät:innen mit ins Boot zu holen.

3. Bereitstellung eines Funktions-Accounts
Stellen Sie berufliche Chatbot-Accounts zur Verfügung. Beschäftigte sollten nicht eigenständig und unter Verwendung privater Daten ein Konto erstellen. Denn so würde ein Profil zu den jeweiligen Beschäftigten hinterlegt. Wenn die Verwendung im beruflichen Kontext erwünscht ist, sollten auch berufliche Accounts zur Verfügung gestellt werden. Nach Möglichkeit sollten diese Arbeits-Accounts nicht die Namen einzelner Beschäftigter enthalten. Soweit die E-Mail-Adresse abgefragt wird, bietet sich die Angabe einer dafür angelegten Mailadresse an. Teilweise werden auch Mobilfunknummern bei der Registrierung verlangt. Auch hier empfiehlt es sich, ein dienstliches Telefon dafür zu benutzen. Der HmbBfDI rät davon ab, die private Nutzung dieser dienstlichen Accounts zu erlauben.

4. Sichere Authentifizierung
Betrieblich genutzte Accounts für KI-Chatbots bieten ein erhebliches Missbrauchspotential. Gelangen Angreifer:innen unberechtigt zur Anwendungsoberfläche, können sie gegebenenfalls bisherige Aktivitäten einsehen, sollte der Chatverlauf nicht deaktiviert sein. Über eigene Abfragen können sie außerdem persönliche Informationen und Geschäftsgeheimnisse in Erfahrung bringen. Aus diesem Grund muss auf die Authentifizierung ein besonderer Fokus gelegt

werden. Nutzen Sie starke Passwörter und integrieren Sie weitere Authentifizierungsfaktoren.

5. Keine Eingabe personenbezogener Daten
Grundsätzlich gilt: Wenn sich der Anbieter eines Chatbots in den Geschäftsbedingungen eine Verwendung für eigene Zwecke einräumen lässt, dürfen keine personenbezogenen Daten an die KI übermittelt werden. Das betrifft jegliche Informationen, die Rückschlüsse auf Kund:innen, Geschäftspartner:innen oder sonstige Dritte enthalten, und ebenso Daten der eigenen Beschäftigten. Eine dafür erforderliche Rechtsgrundlage wird in der Regel nicht zu finden sein. Auch die eingebende Person selbst darf nicht identifizierbar sein, wenn sich für die Verarbeitung ihrer Daten durch den Anbieter keine tragfähige Rechtsgrundlage finden lässt.

6. Keine Ausgabe personenbezogener Daten
Achten Sie darauf, dass Ergebnisse der KI-Anwendung möglichst keine personenbezogenen Daten enthalten. Auch wenn der Eingabebefehl keine Person nennt, kann die KI unter Umständen vorherige Eingaben oder Informationen aus dem Internet einbeziehen. Daher sollten die Eingaben auf Fallgestaltungen beschränkt werden, die keinen Bezug zu Einzelpersonen herstellen.

7. Vorsicht bei personenbeziehbaren Daten
Vermeiden Sie auch solche Eingaben, die unter Umständen auf konkrete Personen bezogen werden können. Es reicht nicht, Namen und Anschriften aus der Eingabe zu entfernen. Auch aus dem Zusammenhang lassen sich gegebenenfalls Rückschlüsse auf Autor:innen und Betroffene ziehen. Bei KI-Anwendungen, deren Bestimmung es ist, Querbezüge auch aus unstrukturierten Daten herzustellen, ist diese Gefahr besonders hoch.

8. Opt-out des KI-Trainings
Nutzen Sie die Option, die Verwendung Ihrer Daten zu Trainingszwecken abzulehnen. Oft verwenden die Hersteller von KI-Modellen alle getätigten Eingaben zum weiteren Training ihrer KI. Privatleute

und Beschäftigte anderer Unternehmen können diese Inhalte dann „erfragen". Je nach genutztem Dienst ist es jedoch möglich, der Verwendung zu Trainingszwecken zu widersprechen. Teilweise muss dafür ein spezifisches Vertragsmodell gebucht werden, das sich von der kostenfreien Standardanwendung unterscheidet.

9. Opt-out der History
Chatbasierte Dienste bieten häufig an, bisherige Eingaben zu speichern, um den Dialog zu einem Thema an einem späteren Zeitpunkt wieder aufnehmen zu können. Damit ist zwangsläufig eine Verkettung der Eingaben einer Person verbunden. Insbesondere bei der gemeinsamen Nutzung durch mehrere Beschäftigte sollte die History abgewählt werden, da Inhalte ansonsten für alle Kolleg:innen einsehbar sind.

10. Ergebnisse auf Richtigkeit prüfen
Die Ergebnisse einer Chatbot-Anfrage sind mit Vorsicht zu genießen. Large Language Models erzeugen Texte, die mit mathematischer Wahrscheinlichkeit dem gewünschten Ergebnis nahekommen. Dies bedeutet keinesfalls, dass alle ausgegebenen Informationen korrekt sind. Im Gegenteil: Die bekannten LLM berücksichtigen meist vergleichsweise alte Informationsstände. Sie sind darüber hinaus bekannt für das Phänomen der „Halluzination", bei der die KI scheinbar richtig und logisch erscheinende, tatsächlich aber falsche Aussagen erfindet. Es liegt in Ihrer Verantwortung als Nutzer:innen, das Ergebnis auf seine Richtigkeit zu überprüfen.

11. Ergebnisse auf Diskriminierung überprüfen
Auch unabhängig von ihrer sachlichen Richtigkeit können Ergebnisse unangebracht sein, wenn sie beispielsweise diskriminierend wirken. Eine darauf aufbauende Datenverarbeitung kann deshalb unzulässig sein, weil sie beispielsweise gegen das Allgemeine Gleichbehandlungsgesetz verstößt oder der Güterabwägung des Art. 6 Abs. 1 lit. f DSGVO nicht standhält. Auch hier tragen Sie als Nutzer:innen die Verantwortung zu überprüfen, ob die Antworten für die weitere Verwendung im gesetzlichen Rahmen tragbar sind.

12. Keine automatisierte Letztentscheidung
Entscheidungen mit Rechtswirkung sollten grundsätzlich nur von Menschen getroffen werden. Andernfalls sind die Voraussetzungen des Art. 22 DSGVO zu beachten. Erarbeitet ein LLM-basierter Chatbot Vorschläge, die durch Beschäftigte angenommen werden, müssen diejenigen darauf achten, dass ihnen ein tatsächlicher Entscheidungsspielraum zukommt. Vermeiden Sie es, aufgrund der fehlenden Transparenz der KI-gestützten Vorarbeit faktisch an die Vorschläge gebunden zu sein, weil Sie den Entscheidungsweg nicht nachvollziehen können. Auch unzureichende Ressourcen und Zeitdruck können dazu führen, dass Ergebnisse ungeprüft übernommen werden.

13. Beschäftigte sensibilisieren
Sensibilisieren Sie Beschäftigte durch Schulungen, Leitfäden und Gespräche dahingehend, ob und wie sie KI-Tools nutzen dürfen.

14. Datenschutz ist nicht alles
Der Schutz personenbezogener Daten darf durch die Nutzung von KI-Diensten nicht unterlaufen werden. Es empfiehlt sich darüber hinaus, weitere Aspekte wie den Schutz von Urheberrechten oder Geschäftsgeheimnissen zu regeln. Bei behördlichen Anwendungsfällen sind Weitergabeverbote nach dem Sicherheitsüberprüfungsgesetz (SÜG) und anderen Regelungen zu berücksichtigen.

15. Weitere Entwicklung verfolgen
Auf EU-Ebene wird aktuell die Regulierung künstlicher Intelligenz vorbereitet. Die künftige KI-Verordnung betrifft voraussichtlich nicht nur die Anbieter solcher Dienste, sondern auch bestimmte Nutzer:innen. Aufgrund fortschreitender technischer Lösungen und laufender Updates auf neue Systeme und Sprachmodelle sollte regelmäßig überprüft werden, ob die internen Vorgaben angepasst werden müssen.

Zudem prüfen die Datenschutzbehörden gerade in Musterverfahren, ob die am Markt befindlichen Sprachmodelle grundsätzlich rechtmäßig sind.

6. Geplantes Beschäftigtendatenschutzgesetz

Die Datenschutzkonferenz (DSK) fordert bereits seit mehreren Jahren die Schaffung eines Beschäftigtendatenschutzgesetzes. Ein Eckpunktepapier zum Beschäftigtendatenschutz, das gemeinsam vom Bundesministerium für Arbeit und Soziales (BMAS) und dem Bundesministerium des Innern und für Heimat (BMI) erarbeitet wurde, hat die langjährige Forderung neu belebt.

Bereits seit mehreren Jahrzehnten besteht die Forderung nach klaren Regelungen im Bereich des Beschäftigtendatenschutzes, ein Ziel, das nahezu alle Regierungen in dieser Zeit verfolgt haben. Auch die jetzige Ampel-Koalition bekennt sich im Koalitionsvertrag explizit zur Schaffung von Regelungen zum Beschäftigtendatenschutz.

Im Herbst 2009 wurde erstmalig ein Entwurf für ein Gesetz zum Datenschutz im Beschäftigungsverhältnis (Beschäftigtendatenschutzgesetz – BDatG) erarbeitet. Das geplante Gesetz sollte die bestehenden Vorschriften und Gerichtsurteile zum Beschäftigtendatenschutz vereinheitlichen und bestehende Lücken schließen. Das Gesetz wurde als Reaktion auf unzulässige Überwachungsmethoden von großen Konzernen als zwingend notwendig betrachtet, schaffte es aber nicht in das Gesetzgebungsverfahren. Der Gesetzgeber hat im Jahr 2009 mit § 32 BDSG a.F. dennoch eine Vorschrift erlassen, welche als erster Schritt zu einer umfassenden bereichsspezifischen Regelung betrachtet werden konnte. Weitere Bemühungen, ein eigenständiges Gesetz zu schaffen, sind u.a. auch von Gewerkschaften und Arbeitgebern auf erhebliche Kritik gestoßen und wurden letztlich nicht verabschiedet.

2014 – mit Blick auf die Verhandlungen über die Datenschutz-Grundverordnung (DSGVO) – hat die DSK erstmals mit einer Entschließung die Schaffung von Regelungen zum Beschäftigtendatenschutz

gefordert. Aufgrund des seinerzeit bevorstehenden Abschlusses der Verhandlungen über die DSGVO wurden aber jegliche Bemühungen der Bundesregierung damals ausgesetzt. Die seit Mai 2018 geltende DSGVO konnte keine Klarheit bei der Verarbeitung von Beschäftigtendaten schaffen. Die DSGVO enthält keine Spezialregelungen zum Beschäftigungsdatenschutz. Auch gibt es keine anderen EU-Instrumente zu diesem Gebiet, wie etwa eine Richtlinie zum Beschäftigtendatenschutz. Um die Harmonisierung in der EU zu gewährleisten, treffen Mitgliedstaaten keine eigenen Regelungen im Geltungsbereich der DSGVO, so dass ihre generalklauselartig formulierten Regelungen auch für den Beschäftigtendatenschutz anzuwenden sind. Allerdings enthält die DSGVO in Art. 88 die an die Mitgliedstaaten gerichtete Befugnis, spezifischere Vorschriften für den Beschäftigtendatenschutz zu erlassen. Im „neuen BDSG", das im Jahr 2018 mit Geltungsbeginn der DSGVO in Kraft getreten ist, wurde die alte Regelung des § 32 BDSG a.F. unverändert in § 26 BDSG n.F. überführt. Für die Vielzahl spezifischer Verarbeitungssituationen sind mit dem weiten Interpretationsspielraum des § 26 BDSG Unklarheiten für alle Beteiligten über die Zulässigkeit verschiedener Datenverarbeitungen entstanden.

Die DSK bekräftigte daraufhin im Jahr 2022 mit ihrer Entschließung „Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!" nochmals ihre Forderung nach Regelungen zum Beschäftigtendatenschutz. Während die Entwicklungen zum Beschäftigtendatenschutz bislang schleppend verliefen, konnten besondere Entwicklungen im Jahre 2023 dazu beitragen, dass dieses schon so oft gescheiterte Vorhaben, nun endlich in die Tat umgesetzt wird.

Neuen Schwung bekommt die Forderung nach einem Beschäftigtendatenschutzgesetz durch eine Entscheidung des EuGH, wonach der § 26 Abs. 1 S. 1 BDSG ggf. keine Anwendung mehr findet. Der EuGH hat mit Urteil vom 30. März 2023 entschieden, dass eine nationale Regelung zur Datenverarbeitung im Beschäftigungskontext im hessischen Landesrecht nicht von der Öffnungsklausel in Artikel 88 Absatz 1 DGVO gedeckt sei, weil die Regelung nicht den strengen Anforderungen des Artikel 88 Absatz 2 DSGVO genügte.

§ 26 Abs. 1 S. 1 BDSG ist nahezu wortgleich mit der hessischen Vorschrift, so dass das Urteil direkte Auswirkungen auf § 26 BDSG, die zentrale Vorschrift für Verarbeitungen von Beschäftigtendaten, haben könnte. Aufgrund dieser Entwicklungen und den anhaltenden politischen Bestrebungen veröffentlichten das BMAS und das BMI im Frühjahr ein Eckpunktepapier, in dem zwölf regelungsbedürftige Aspekte des Beschäftigtendatenschutzes herausgearbeitet wurden. Viele dieser Aspekte waren auch in den bisherigen Forderungen der DSK enthalten, so u.a. die Begrenzung der Überwachung von Beschäftigten, die Forderung nach Transparenz bei dem Einsatz künstlicher Intelligenz und mehr Rechtssicherheit bei kollektivrechtlichen Regelungen. Daneben wurde von den Bundesministerien auch ein besonderer Schutz im Bewerbungsverfahren gefordert – ein Aspekt, der ebenfalls Teil der Forderungen der DSK und auch Gegenstand einer im Entwurf befindlichen Orientierungshilfe der DSK ist.

Auf Grundlage dieses Eckpunktepapiers fand Ende April 2023 ein Stakeholder-Dialog mit Vertretern aus Praxis und Theorie statt (Betriebsräte, Gewerkschaftsvertreter, der Arbeitgeberverband, Experten aus der Wissenschaft). Auch der HmbBfDI nahm an diesem Stakeholder-Treffen teil.

Im Mai 2023 nahm die DSK diese wichtige Entscheidung des EuGH zum Anlass, den Gesetzgeber mit einer Entschließung vom 11.05.2023 erneut aufzufordern, ein Beschäftigtendatenschutzgesetz zu schaffen.

Die Anstrengungen des BMAS und des BMI, das bedeutende EuGH-Urteil sowie die eindeutigen Forderungen der DSK lassen hoffen, dass noch in dieser Legislaturperiode Regelungen zum Beschäftigtendatenschutz verabschiedet werden. Spezifischere Vorschriften sind unerlässlich für die Praxis, um Rechtsunsicherheiten im Beschäftigungsverhältnis zu begegnen und die Rechte aller Betroffenen zu schützen. Es bleibt zu hoffen, dass dieses Vorhaben aufgrund anderer politischer Priorisierung nicht wieder in den Hintergrund rückt.

7. Orientierungshilfe Hinweisgeber-Meldestellen (Whistleblowing)

Im Auftrag der DSK hat der HmbBfDI die Überarbeitung der seit 2018 existierenden Orientierungshilfe „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“ übernommen. Aufgrund einer entsprechenden EU-Whistleblowing-Richtlinie und dem in national umgesetzten Gesetz war eine Überarbeitung der bisherigen Orientierungshilfe angezeigt. Die Orientierungshilfe soll sich primär an nicht-öffentliche Stellen richten.

Nach der damaligen Veröffentlichung der Orientierungshilfe ist am 23.10.2019 die sog. „EU-Whistleblower-Richtlinie“ (RL 2019/1937/EU) in der Europäischen Union in Kraft getreten und verpflichtete die Mitgliedstaaten zur Umsetzung der Richtline in nationales Recht. Mit etwas Verspätung ist das Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz ‚HinSchG) in Deutschland sodann am 02. Juli 2023 in Kraft getreten. Spätestens mit dem Inkrafttreten dieses Gesetzes war der Anlass für eine Überarbeitung der bestehenden Orientierungshilfe gegeben.

Der Begriff „Whistleblowing“ ist nicht legaldefiniert. Im allgemeinen Sprachgebrauch bezieht er sich auf das Handeln von sogenannten “Whistleblowern”, die als hinweisgebende Personen verstanden werden sollten. Zwischenzeitlich wurde „hinweisgebende Person“ nach § 1 Abs. 1 HinSchG legaldefiniert und ist hiernach eine natürliche Person, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt hat und diese an die nach diesem Gesetz vorgesehenen Meldestellen meldet oder offenlegt. Mit solchen Hinweisen und Meldungen geht in aller Regel die Verarbeitung von personenbezogen Daten einher.

Mit dem Hinweisgeberschutzgesetz soll der bislang lückenhafte und unzureichende Schutz von hinweisgebenden Personen ausgebaut

werden. Zentraler Bestandteil des Gesetzes sind Regelungen für einen besseren Schutz hinweisgebender Personen und datenschutzrechtlich relevante Regelungen bezüglich der Verarbeitungsgrundlagen sowie Regelungen über die Vertraulichkeit und Ausgestaltung der zu erwartenden Verarbeitungsvorgänge.

Verfahren zur Meldung und Offenlegung von Missständen werden in der Regel aus dem Bedürfnis eingerichtet, zuverlässige und standardisierte Grundsätze der Unternehmensführung im täglichen Betrieb der Unternehmen zu sichern. Verfahren zur Meldung von Missständen sind als zusätzlicher Mechanismus für die Beschäftigten gedacht, um Missstände intern oder extern über einen bestimmten Kanal zu melden.

Innerhalb der Orientierungshilfe wird der HmbBfDI praxisrelevante datenschutzrechtliche Problemstellungen aufgreifen und Hinweise und Empfehlungen zu einzelnen datenschutzrechtlichen Fragestellungen erteilen. Inhaltlich geht es z.B. um einschlägige Rechtsgrundlagen der Verarbeitungen, ob und unter welchen Voraussetzungen ein Datenschutzbeauftragter eine interne Meldestelle betreiben könnte und der Frage danach, ob die Einrichtung einer internen Meldestelle immer ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 Abs. 1 S. 1 DSGVO zur Folge hat. Sollte eine Datenschutzfolgenabschätzung stets durchzuführen sein, hätte dies Auswirkungen auf § 38 BDSG, wonach ein Datenschutzbeauftragter nach § 38 Abs. 1 S. 1 BDSG erst zu bestellen ist, soweit in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind und kein Fall des Art. 37 Abs. 1 DSGVO vorliegt. Gem. § 38 Abs. 1 S. 2 BDSG müssen Verantwortliche unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen einen Datenschutzbeauftragten benennen, wenn Sie Verarbeitungen vornehmen, welche einer Datenschutzfolgenabschätzung gem. Art. 35 DSGVO unterliegen. Gem. § 12 Abs. 2 HinSchG ist eine interne Meldestelle verpflichtend einzurichten für Beschäftigungsgeber mit jeweils in der Regel

mindestens 50 beschäftigten Personen. Praxisrelevant ist dies, da ggf. mit der Einrichtung einer internen Meldestelle automatisch ein Datenschutzbeauftragter benannt werden müsste, ohne dass dies vorher der Fall war.

Der HmbBfDI wird sich dafür einsetzen, dass die Orientierungshilfe in 2024 so schnell wie möglich von der DSK verabschiedet wird.

8. Orientierungshilfe Bewerberdatenschutz

Immer wieder erhalten Aufsichtsbehörden Beschwerden über Bewerbungsverfahren, daher ist eine anwendungsbezogene Orientierungshilfe mit gemeinsamen Positionen längst überfällig. Der HmbBfDI hat im Auftrag der Datenschutzkonferenz (DSK) die Federführung für eine solche Orientierungshilfe übernommen.

Die Datenschutzbeauftragten des Bundes und der Länder (DSK) veröffentlichen gemeinsame Positionen in anwendungsbezogenen Orientierungshilfen, die Hinweise und Empfehlungen zu einzelnen datenschutzrechtlichen Fragestellungen enthalten. Mit der Orientierungshilfe „Personalgewinnung / Bewerbungsverfahren / Pre-Employment-Checks“ wird der Fokus auf datenschutzkritische Themen im Zusammenhang mit Bewerbungs- und Personalgewinnungsverfahren (Recruiting) gelegt und richtet sich primär an nicht öffentliche Stellen.

Jede Bewerbung geht mit der Verarbeitung personenbezogener Daten der Bewerbenden einher. Da eine Bewerbung eine möglichst umfassende Darstellung der Person beinhalten soll, enthält sie naturgemäß eine Vielzahl persönlicher und möglicherweise sensibler Daten im Sinne des Art. 9 der DSGVO. Diese Daten sind besonders schützenswert, und für Bewerber:innen ist es oft schwierig nachzuvollziehen, was während und nach dem Bewerbungsprozess mit diesen Daten geschieht. Für Bewerbungsverfahren gelten die Bestimmungen des Beschäftigtendatenschutzes gemäß § 26 Abs. 8

Satz 2 BDSG in Verbindung mit Art. 6 Abs. 1 DSGVO, auch wenn die Anwendbarkeit des § 26 BDSG aufgrund eines EuGH-Urteils vom 30.03.2023 derzeit in Frage steht. Die Verarbeitung von Daten von Bewerbenden bewegt sich stets in einem Spannungsfeld zwischen den verfassungsrechtlich garantierten Rechten der Bewerbenden auf den Schutz ihrer Persönlichkeitsrechte, insbesondere dem Recht auf informationelle Selbstbestimmung, und den dagegen abzuwägenden Interessen der Arbeitgebenden.

Neben klassischen Fragen zu den Löschfristen im Bewerbungsverfahren oder Abfragen bei Dritten und Backgroundchecks, liegt ein Fokus auf Fragen, die sich aufgrund des veränderten Arbeitsmarktes und der fortschreitenden Digitalisierung ergeben. Auch der demografische Wandel und ein Fachkräftemangel tragen dazu bei, dass in Deutschland zunehmend von einem Arbeitnehmermarkt gesprochen wird. Dieser entsteht, wenn die Anzahl offener Stellen die Anzahl geeigneter Bewerber:innen übersteigt. Infolge dieser Entwicklungen hat sich insbesondere der Bereich der Personalvermittlung z.B. im Social-Media-Bereich stark weiterentwickelt. Es können hierbei datenschutzrechtliche Probleme bei der Personalgewinnung über soziale berufliche Netzwerke sowie beim Outsourcing der Bewerbersuche durch sogenannte Headhunter entstehen. Das Bewerbungsverfahren beginnt oftmals früh, ohne dass die datenschutzrechtliche Relevanz und Abgrenzungen den beteiligten Personen bekannt sind. Nutzer:innen von beruflichen Netzwerken können angesprochen werden, ohne dass sie aktiv auf Jobsuche sind oder datenschutzrechtliche Vereinbarungen zwischen den potenziell Beteiligten abgeschlossen wurden. In solchen Konstellationen ergeben sich Fragen bezüglich der Abgrenzungen der datenschutzrechtlichen Verantwortlichkeiten.

Die technischen Möglichkeiten eines Bewerbungsverfahrens erlauben Auswahlentscheidungen mittels automatisierter Verfahren, den Einsatz von Lebenslauf-Scannern, sogenannten “CV Parsern”, sowie die Möglichkeit, Bewerbungsdatenmanagementsystemen einzusetzen. Dadurch entstehen große Datenbanken und z.B. sogenannte

Talentpools, die aufgrund des bestehenden Bewerbermarktes und der damit verbundenen Nachfrage eine erhebliche wirtschaftliche Bedeutung haben. Datenschutzrechtlich müssen diese Datensammlungen in Einklang mit datenschutzrechtlichen Bestimmungen gebracht werden und ein diesbezügliches Bewusstsein bei Verantwortlichen entstehen, um potenzielle Datenschutzverstöße für die Zukunft auszuschließen. Nur auf diese Weise können die Rechte der Bewerber:innen gewahrt werden.

Ein Zeitplan für die Veröffentlichung der Orientierungshilfe liegt nicht vor. Die Orientierungshilfe könnte durch ein mögliches Beschäftigtendatenschutzgesetz, welches in dieser Legislaturperiode angekündigt ist, flankiert werden. Die DSK forderte diesbezüglich in ihren Entschließungen vom 29.04.2022 und 11.05.2023, dass gesetzliche Regelungen zur Datenverarbeitung auch in der Bewerbungsphase erforderlich sind. In diesen Regelungen sollen Themen wie das Fragerecht der Arbeitgeber:innen, Anforderungen polizeilicher Führungszeugnisse, ärztliche Untersuchungen und Eignungstests, Datenerhebung aus Drittquellen (z. B. vorherige Arbeitsstellen), Umgang mit sozialen Netzwerken oder das sogenannte Active Sourcing geregelt werden.

9. TI-Modellregion Hamburg

Hamburg und Umgebung wurden von der gematik als erste Modellregion für digitale Gesundheit ausgewählt. Hier sollen zugelassene digitale Anwendungen und Dienste im Praxisbetrieb erprobt werden, um die bundesweite Einführung vorzubereiten – unter Berücksichtigung des Datenschutzes.

Mit Pressemitteilung vom 30. März 2023 hat die gematik GmbH (gematik) mitgeteilt, dass Hamburg und Umgebung als erste Modellregion für digitale Gesundheit ausgewählt wurden. Darum beworben hatte sich mit dem ÄrzteNetz Hamburg e. V. ein Zusammenschluss

aus Arzt-/Zahnarztpraxen, Kliniken, Apotheken, Ämtern, weiteren Einrichtungen des Gesundheitswesens sowie aus Herstellern/Dienstleistern, Verbänden und Versicherungen.

In dieser und der weiteren Modellregion Franken sollen bestehende und neue digitale Anwendungen und Dienste der Gesundheitsinfrastruktur sowie zukünftige Ausbaustufen in den Versorgungsalltag eingeführt werden. Die aus der Praxis gewonnenen Erkenntnisse sollen aufzeigen, wie die Anwendungen und Dienste im Gesundheitswesen sinnvoll genutzt werden können. Außerdem sollen sie zur Verbesserung der digitalen Angebote genutzt werden.

Die Telematikinfrastruktur (TI) ist nach § 306 Sozialgesetzbuch (SGB) Fünftes Buch (V) „die interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur, die der Vernetzung von Leistungserbringern, Kostenträgern, Versicherten und weiteren Akteuren des Gesundheitswesens sowie der Rehabilitation und der Pflege dient“. Sie umfasst eine dezentrale Infrastruktur (Komponenten zur Authentifizierung, zur elektronischen Signatur, zur Verschlüsselung sowie Entschlüsselung und zur sicheren Verarbeitung von Daten in der zentralen Infrastruktur), eine zentrale Infrastruktur sowie eine Anwendungsinfrastruktur bestehend aus Diensten für die gesetzlich vorgesehenen Anwendungen.

Die Datenverarbeitung mittels der Komponenten der dezentralen Infrastruktur liegt regelmäßig in der Verantwortung derjenigen, die diese Komponenten für die (oben genannten) gesetzlich vorgesehenen Zwecke nutzen. Wenn also z.B. eine Praxis den TI-Messenger zur Kommunikation mit einem Labor über einen Laborbefund einsetzt, muss sie sich in diesem Zusammenhang Gedanken machen über technische oder organisatorische Maßnahmen, die in der konkreten Nutzungssituation zu ergreifen sind, um dem besonderen Schutzbedarf und dem hohen Schutzniveau bei der Verarbeitung von sensiblen Gesundheitsdaten gerecht zu werden. Das gilt unabhängig davon, dass eine Anwendung wie der TI-Messenger grundsätzlich bereits zugelassen und vom Bundesbeauftragten für den Daten-

schutz und die Informationsfreiheit (BfDI) sowie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft wurde.

Mit Blick darauf ist der HmbBfDI im Juli 2023 an die Projektleitung der TI-Modellregion herangetreten, wird seitdem in die Planungen der Pilotierungen sowie in den Austausch zwischen den Projektbeteiligten und der gematik einbezogen und steht insoweit beratend zur Seite – auch über das Berichtsjahr 2023 hinaus.

10. Einführung eines neuen Krankenhausinformationssystems im Universitätsklinikum Hamburg-Eppendorf

Das Universitätsklinikum-Hamburg Eppendorf hat im Jahr 2023 das Projekt zur Umstellung des bisherigen Arbeitsplatzsystems auf eine alternative Software weiter vorangetrieben. Hierbei kam es mehrfach zu Verschiebungen innerhalb des Projekts, sodass die Umstellung im Berichtsjahr noch nicht stattfinden konnte. Weiterhin sind entscheidende datenschutzrechtliche und -technische Fragestellungen offen, die es vor Inbetriebnahme dringend zu klären gilt.

Die bisher im Universitätsklinikum Eppendorf (UKE) genutzte Software zur Patient:innen-Verwaltung Sorian sowie weitere klinische Systeme können aufgrund ihres auslaufenden technischen Supports nur bis Ende 2024 sicher betrieben werden. Aus diesem Grund erarbeitet die Klinik unter mittlerweile hohem Zeitdruck eine Nachfolgelösung namens CGM Clinical. Aufgrund der besonderen Bedeutung des Informationssystems für den Gesundheitsstandort Hamburg begleitet der HmbBfDI die Einführung beratend (vgl. 31. TB Datenschutz 2022, Kap. VI 1). Die neu entwickelte Software soll zunächst neben dem UKE auch in den Tochtergesellschaften Martini-Klinik GmbH, Altonaer Kinderkrankenhaus gGmbH (AKK) und Ambulanzzentrum des UKE GmbH eingeführt werden und perspektivisch bundesweit vertrieben werden.

Seit Beginn seiner Einbindung im April 2022 hat der HmbBfDI die Anforderung aufgezeigt und eingefordert, dass das UKE eine Risikobetrachtung vornimmt, um darauf aufbauend die notwendigen technischen und organisatorischen Maßnahmen zum Schutz der Betroffenen auszuwählen und einzurichten. Dieses Vorgehen entspricht der üblichen Praxis bei der Einführung von IT-Projekten. Bis zum Ende des Berichtszeitraums 2023 hat das UKE keine entsprechende vollständige Risikobetrachtung vorgelegt.

Gleichwohl wurde die technische Architektur der Software schrittweise konkretisiert und aufgebaut, ohne dass die Ergebnisse einer solchen Risikobetrachtung eingeflossen sind. Das UKE hat sich dabei für eine Ein-Mandanten-Lösung entschieden, bei der die Datenbestände der jeweiligen Klinikhäuser und deren Abteilungen alle in demselben Softwaremandanten abgelegt werden. Üblich und geboten ist bei Projekten dieser Größenordnung und Sensibilität eine Verteilung auf jeweils eigenständige Mandanten. Dadurch kann dann das Risiko minimiert werden, dass z.B. ein Hackerangriff oder ein Schadsoftware-Befall unmittelbar das Komplettsystem beeinträchtigt. Dennoch hat der HmbBfDI sich in dieser Hinsicht kompromissbereit gezeigt, wenn das daraus erwachsende Risiko durch angemessene gleichwertige Sicherungsmaßnahmen eingegrenzt und im akzeptablen Rahmen gehalten wird. Die Betrachtung solcher risikominimierenden Maßnahmen setzt jedoch als ersten Schritt zwingend die zum Ende des Berichtszeitraums noch ausstehende ausführliche Risikobetrachtung voraus.

Neben der Risikobetrachtung und der darauf aufbauenden risikominimierenden Maßnahmen fehlte es zum Redaktionsschluss zudem noch an grundlegenden Festlegungen wie einem ausdifferenzierten Rollen- und Berechtigungskonzept. Bevor die Software eingeführt werden kann, muss durch organisatorische Festlegung und durch Implementierung dieser Regeln im System klar sein, welche Person in welcher Klink und Abteilung unter welchen Voraussetzungen auf welche Daten zugreifen darf. Diese Dokumente sind zwingend vom UKE so rechtzeitig zu erstellen, dass sie bis zum Rollout noch technisch umgesetzt und ggfs. angepasst werden können.

Diese Anforderungen rechtzeitig vor dem Auslaufen des Supports von Sorian zu implementieren, wird für das UKE voraussichtlich herausfordernd, da aufgrund technischer Verzögerungen die Einführung der neuen Software nach mehrmaligen Verschiebungen mittlerweile erst gegen Ende der zur Verfügung stehenden Zeit geplant ist. So beabsichtigt das UKE die vollständige Ablösung des aktuellen klinischen Arbeitsplatzsystems bis Ende 2024. Es bedarf daher nun der unmittelbaren Umsetzung der datenschutzrechtlichen Anforderungen.

11. Datenkopie aus Patientenakten

Der EuGH stärkt das Recht von Patient:innen auf eine kostenlose Erst-Kopie der Patientenakte und bestätigt damit die bisherige Beratungspraxis des HmbBfDI.

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 26.10.2023 (Rechtssache C-307/22) klargestellt, dass jeder Person in ärztlicher Behandlung eine kostenfreie Kopie der Patientenakte zusteht. Dieser Anspruch umfasse den vollständigen Inhalt der Akte im Sinne einer originalgetreuen und verständlichen Reproduktion. Der Antrag ist, so der EuGH, voraussetzungsfrei und muss nicht begründet werden. Unentgeltlich sei nur die erste Kopie, für weitere Ausfertigungen dürfen Gebühren erhoben werden.

Zum Hintergrund: Dem Auskunftsrecht nach Art. 15 DSGVO steht in Deutschland die ältere nationale Regelung des § 630g Bürgerliches Gesetzbuch (BGB) entgegen, das Recht auf Einsichtnahme in die Patientenakte. Der Bundesgerichtshof (BGH) hatte dem EuGH in einem Verfahren Fragen zur Vorabentscheidung vorgelegt, auch zum Verhältnis der beiden Vorschriften. Ein Patient einer Zahnarztpraxis hatte wegen des Verdachts einer fehlerhaften Behandlung eine unentgeltliche Kopie seiner Patientenakte beantragt. Diese wollte ihm

die Praxis nur zur Verfügung stellen, wenn er die Kosten dafür trägt, wie es das BGB vorsieht. Aus den Ausführungen des EuGH ergibt sich Folgendes:

- Arztpraxen und Kliniken sind verpflichtet, eine erste Kopie der personenbezogenen Daten kostenfrei zur Verfügung zu stellen, auch wenn die antragstellende Person einen anderen als den Zweck verfolgt, von der Verarbeitung Kenntnis zu nehmen und deren Rechtsmäßigkeit zu überprüfen.
- Eine nationale Regelung kann zwar grundsätzlich zu einer Beschränkung des Auskunftsrechts führen, auch wenn diese Regelung vor Inkrafttreten der DSGVO erlassen wurde. Durch eine solche Regelung dürfen der betroffenen Person jedoch keine Kosten für eine erste Kopie ihrer personenbezogenen Daten auferlegt werden.
- Im Rahmen eines Arzt-Patienten-Verhältnisses hat eine betroffenen Person Anspruch auf eine originalgetreue und verständliche Reproduktion der Daten aus der Patientenakte, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu an der betroffenen Person vorgenommenen Behandlungen oder Eingriffen umfasst.

Die bisherige Beratungspraxis des HmbBfDI (vgl. 31. TB Datenschutz 2022, Kap. II 10) findet durch dieses Urteil Bestätigung. Betroffene können sich auf die Entscheidung berufen und von ihrer ärztlichen Einrichtung formlos, beispielsweise per E-Mail oder Brief, Auskunft und eine Kopie nach Art. 15 DSGVO beantragen. Arztpraxen oder Krankenhäuser sind dann verpflichtet, spätestens innerhalb eines Monats zu reagieren, Art. 12 Abs. 3 DSGVO.

12. Neues Gesundheitsdatennutzungsgesetz

Der Deutsche Bundestag hat am 14. Dezember 2023 das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten" (Gesundheitsdatennutzungsgesetz – GDNG) beschlossen. Mit diesem kommen auch neue Aufgaben auf den HmbBfDI bei der Datennutzung zu Forschungszwecken zu.

Im März 2023 hatte das Bundesministerium für Gesundheit (BMG) eine Digitalisierungsstrategie für das Gesundheitswesen und die Pflege vorgelegt – verbunden mit der Ankündigung, zentrale Vorhaben der Strategie noch 2023 auf den Weg zu bringen. Als eines der zentralen Handlungsfelder für die digitale Transformation hat das BMG, auch unter dem Eindruck der Coronavirus-Pandemie, die Nutzung von Gesundheitsdaten identifiziert. Dementsprechend hat es einen Referentenentwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG) erarbeitet, mit dem Schwerpunkt auf Regelungen zur Nutzung dieser Daten zu Forschungszwecken. Der Referentenentwurf wurde im Juni 2023 erstmals über das Onlineportal Netzpolitik.org geleakt und Anfang August mit kleinen Änderungen und unter dem Datum 03. Juli 2023 offiziell veröffentlicht.

Das künftige GDNG bettet die Datenschutzbehörden als zentrale Akteure eng in die Gestaltung medizinischer Datennutzung ein. So enthält z.B. § 6 Abs. 3 GDNG ein explizites Zustimmungserfordernis für die zweckändernde Übermittlung von Versorgungsdaten zur gemeinsamen Forschung. Ohne das positive Votum der Datenschutzbehörde darf das Vorhaben nicht begonnen werden. Solche behördlichen Genehmigungen sind ein Novum in der bislang gesetzlich vorgesehenen, eher reaktiven Aufsichtsstruktur. Auch darüber hinaus ist die beratende Einbeziehung der Datenschutzbehörden vorgesehen, die teilweise binnen sehr kurzer Frist eine Stellungnahme

abzugeben haben. Z.B. sieht der neue § 303e Abs. 5a SGB V eine behördliche Rückmeldung binnen zehn Arbeitstagen vor. Während dieser Zeit muss das betreffende Forschungsvorhaben ruhen. Damit dieses Zusammenspiel ohne Nachteile für die Forschung und die Freiheitsrechte der Betroffenen gelingt, ist eine frühzeitige und intensive Einbindung unverzichtbar.

Zum Entwurf des GDNG hatte die Datenschutzkonferenz (DSK) bereits am 14. August 2023 Stellung genommen (s. https://datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf). Eine gesonderte Stellungnahme zum ursprünglichen Artikel 5 des Entwurfs und einer darin vorgesehenen Änderung der Zuständigkeitsregelung des § 9 Bundesdatenschutzgesetzes (BDSG) hatten die unabhängigen Datenschutzaufsichtsbehörden der Länder schon unter dem 10. August 2023 abgegeben (s. https://datenschutzkonferenz-online.de/media/st/23_08_10_Datenschutzaufsicht-Laender-zu-Art_5_GDNG-E.pdf).

Artikel 5 GDNG-E sah anfangs (Stand 03. Juli 2023) eine Übertragung weitreichender Aufsichtszuständigkeiten von den Landesdatenschutzaufsichtsbehörden auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vor, die auch die Aufsicht über Kranken- und Pflegekassen und die Kassenärztlichen Vereinigungen sowie über alle Stellen, die gesundheitsbezogene Sozialdaten im Sinne des § 67 SGB X verarbeiten, umfassen sollte. Das hatten die Datenschutzaufsichtsbehörden der Länder unter anderem wegen nachteiliger Auswirkungen auf die Datenschutzkontrolle und die damit zusammenhängende Beratungs- und Kooperationspraxis als problematisch angesehen. Von jener Änderung des BDSG ist der Gesetzgeber abgerückt.

Die inhaltliche Stellungnahme der DSK zum GDNG-E und die in dieser geäußerten datenschutzrechtlichen Kritikpunkte hat der Gesetzgeber bei der weiteren Ausgestaltung des GDNG hingegen nur in Teilen berücksichtigt. So ist z.B. eine Regelung aufgenommen worden, die das GDNG und die darin normierte Weiterverarbeitung von

Versorgungsdaten zu Forschungszwecken durch eine behandelnde Gesundheitseinrichtung, z.B. ein Krankenhaus, in ein Verhältnis setzt zu landesrechtlichen gesetzlichen Vorschriften wie den Landeskrankenhausgesetzen. Weiterhin ist eine Regelung ergänzt worden zur gemeinsamen Nutzung und Verarbeitung der entsprechenden Daten durch öffentlich geförderte Zusammenschlüsse von datenverarbeitenden Gesundheitseinrichtungen einschließlich Verbundforschungsvorhaben und Forschungspraxennetzwerken nach Zustimmung der Datenschutzbehörde.

Trotz Kritik der DSK hat der Gesetzgeber es aber unter anderem dabei belassen, dass auch Kranken- und Pflegekassen datengestützte Auswertungen ohne Einwilligung der Versicherten vornehmen und diese auf die Ergebnisse dieser Auswertung hinweisen können. Ob und inwieweit die dazu seitens des Gesundheitsausschusses des Deutschen Bundestages eingebrachten Änderungen (z.B. die Anzeige der Ziele und Datengrundlagen einer solchen Auswertung vor Beginn der Verarbeitung personenbezogener Daten bei der Aufsichtsbehörde) geeignete Maßnahmen zur Minimierung der Risiken für die Rechte und Freiheiten natürlicher Personen darstellen, bleibt abzuwarten und muss weiterhin in den Blick genommen werden.

Am 14. Dezember 2023 ist auch das „Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens“ (Digital-Gesetz – DigiG) vom Bundeskabinett beschlossen worden. Kernelement jenes Gesetzes ist die elektronische Patientenakte (ePA), die für alle gesetzlich Versicherten eingeführt werden soll, die nicht widersprechen (Opt-Out). Wie dieses Widerspruchsrecht in der Praxis in geeigneter Form gewährt und ausgeübt werden kann, wird ein wichtiger Punkt sein.

13. Löschung von Datensammlungen nach Ende der Corona-Pandemie

Mit dem Auslaufen der Hotspot-Regelung im April 2022 wurde in Hamburg ein bedeutendes Kapitel in der Bekämpfung des Corona-Virus abgeschlossen. Letzte Maßnahmen, die zu pandemiebedingten Datenerhebungen verpflichteten, reichten bis in das Frühjahr 2023. Die Verarbeitung von Gesundheitsdaten im Zusammenhang mit dem Corona-Virus richtete sich hiernach wieder nach den allgemeinen datenschutzrechtlichen Regelungen.

Mit dem Auslaufen der Hotspot-Regelung im April 2022 wurde in Hamburg ein bedeutendes Kapitel in der Bekämpfung des Corona-Virus abgeschlossen. Letzte Maßnahmen, die zu pandemiebedingten Datenerhebungen verpflichteten, reichten bis in das Frühjahr 2023. Die Verarbeitung von Gesundheitsdaten im Zusammenhang mit dem Corona-Virus richtete sich hiernach wieder nach den allgemeinen datenschutzrechtlichen Regelungen.

Der HmbBfDI hat bereits auf das Auslaufen der Hotspot-Regelung in Hamburg zum 30. April 2022 reagiert und alle Unternehmen und öffentlichen Stellen dazu aufgerufen, ihre „Corona-Datenbestände“ zu überprüfen und pandemiebedingte Datenerhebungen einzustellen. Mit dem Wegfall vieler gesetzlicher Maßnahmen zur Eindämmung des Coronavirus in Hamburg und der schrittweisen Aufhebung der Corona-Verordnungen sind auch zahlreiche Befugnisse und Pflichten zur Erfassung personenbezogener Daten entfallen. Vorhandene Datenbestände sollten daher überprüft und nicht mehr erforderliche Daten umgehend gelöscht werden. Eine Datenspeicherung für den Fall einer möglichen zukünftigen Verschärfung der Corona-Lage ist nach Wegfall der rechtlichen Grundlagen nicht mehr möglich. Die Löschpflichten betreffen insbesondere alle Arbeitgeber:innen, die bis dato den 3G-Status ihrer Beschäftigten abgefragt haben und für diese Erhebungen nachweispflichtig waren.

2023 sind weitere Regelungen im Zusammenhang mit dem Corona-Virus weggefallen. So ist zum Beispiel die HmbSARS-CoV-2-Eindämmungsverordnung zum 01.02.2023 außer Kraft getreten. Damit sind auch die in § 7 HmbSARS-CoV-2-EindämmungsVO vorgesehenen besonderen Regelungen zur Wiederaufnahme der beruflichen Tätigkeit infizierter Personen in besonderen Einrichtungen vulnerabler Gruppen entfallen. Dennoch durften Beschäftigte in diesen Einrichtungen nach § 28b Absatz 1 Satz 1 Nummern 3 bis 5 IfSG, die positiv auf das Coronavirus getestet worden sind, ihrer beruflichen Tätigkeit in der Einrichtung (d.h. vor Ort) auch zukünftig während der Infektion nicht nachgehen. Sie durften ihre berufliche Tätigkeit vor Ort erst wieder aufnehmen, wenn sie seit 48 Stunden symptomfrei waren und einen negativen PCR- oder PoC-Test vorlegen konnten oder sich unter Aufsicht des Arbeitgebers negativ mit einem Schnelltest getestet haben. Entsprechende Tätigkeitsverbote und Regelungen zur Wiederaufnahme der Tätigkeit regelte auch nach dem Außerkrafttreten des § 7 HmbSARS-CoV-2-EindämmungsVO eine neue eigenständige landesrechtliche Verordnung zur beruflichen Betätigung in bestimmten Einrichtungen nach dem Infektionsschutzgesetz für den Zeitraum vom 01.02. bis zum Ablauf des 07.04.2023.

Gemäß § 28b Absatz 1 Satz 1 IfSG bestanden bis zum 07.04.2023 bundesrechtlich verschiedene Testnachweispflichten in medizinischen oder pflegerischen Einrichtungen fort.

Mit Wegfall dieser Rechtsgrundlagen besteht ein Fragerecht des Arbeitgebers/Dienstherrn nach Corona-Infektionen grundsätzlich nicht mehr, ebenso wenig eine coronaspezifische Auskunfts- oder Meldepflicht der Beschäftigten. Es besteht jedoch weiterhin die Möglichkeit, im Rahmen der betrieblichen Hygiene allgemeine Maßnahmen gegen die Verbreitung ansteckender Krankheiten (z.B. Grippe, Corona, andere Atemwegserkrankungen) zu ergreifen. Hieraus können sich indirekt Mitwirkungs- bzw. Mitteilungspflichten der Beschäftigten ergeben, wobei aber grundsätzlich keine Verpflichtung besteht, die Art der Erkrankung (z.B. Covid-19) zu offenbaren.

14. Urban Data Challenge

Die Analyse vorhandener Bewegungsdaten bietet Potenzial für die Verbesserung des öffentlichen Verkehrs und der Stadtentwicklung. Zur Entwicklung innovativer Lösungen hat die Stadt Hamburg Unternehmen und Universitäten aufgerufen, sich einer Urban Data Challenge zu stellen. Der HmbBfDI hat das Vorhaben in der Jury und durch Beratung der Projektumsetzung begleitet.

Zur Förderung von Innovationen bei der Mobilitätssteuerung ist die Stadt Hamburg eine Kooperation mit dem Think Tank The New Institute eingegangen. Gemeinsam mit dem Amt für IT und Digitalisierung, der Behörde für Verkehr und Mobilitätswende und dem Landesbetrieb für Geoinformation und Vermessung hat das Institut eine Urban Data Challenge initialisiert. Forschungsakteure wurden darin aufgerufen, Konzeptpapiere einzureichen, wie sie bestimmte Daten aus öffentlichen und privaten Beständen nutzen würden, um Verkehr und Stadtentwicklung voranzubringen. Damit das Gewinnerprojekt auch aus Datenschutzsicht Modellcharakter hat, war der HmbBfDI Teil der Jury und hat sich auch über die Auswahl hinaus mit Vorgaben zur Datenübermittlung und -auswertung sowie Beratung hinsichtlich der vertraglichen Umsetzung eingebracht.

Ziel der Challenge war es, dem überzeugendsten Projektteam Zugriff auf die benötigten Daten zu verschaffen und es mit einer finanziellen Förderung bei der Nutzung der Daten im Gemeinwohlinteresse zu unterstützen. Neben öffentlich verfügbaren Geoinformationen aus der Urban Data Platform ging es dabei vor allem um Bewegungsdaten, die von den privaten Unternehmen Bolt und IoT Venture zur Verfügung gestellt wurden. Bolt ist ein Verleiher von E-Scootern und Fahrrädern, während IoT Venture technische Bauteile mit GPS-Tracking-Funktion vertreibt.

Von den über 30 eingereichten Konzeptpapieren überzeugte die Ausarbeitung der Universität Bremen sowohl den HmBfDI als auch die übrige Jury am meisten. Ihr Vorhaben „MoveAI“ zielt auf die graphische Darstellung statistischer Analysen mithilfe künstlicher Intelligenz ab. Die entstehende Softwarelösung wird als Open Source öffentlich zugänglich gemacht werden.

Herausfordernd für die datenschutzrechtliche Zulässigkeit ist dabei die Datenherkunft der Bewegungsdaten. Dass Verleiher bzw. Anbieter von Verkehrsmitteln und deren Hardwarekomponenten über Positionsdaten verfügen und diese an Forschende weitergeben, ist nicht ohne weiteres zulässig. Die beiden Daten bereitstellenden Unternehmen befinden sich außerhalb des örtlichen Zuständigkeitsbereichs des HmbBfDI, sodass keine eingehende Prüfung der rechtmäßigen Ursprungserhebung möglich war. Jedoch ist bekannt, dass die Datenerhebung durch Bolt Gegenstand eines Ermittlungsverfahrens durch die zuständige estnische Datenschutzbehörde ist. Vor dem Hintergrund der jedenfalls ungeklärten Erhebungsumstände der Positionsdaten hat der HmbBfDI großen Wert darauf gelegt, dass personenbezogene Daten von Verkehrsteilnehmer:innen an das Gewinnerprojekt weitergegeben werden. Es darf in diesem Fall keine Rückführbarkeit für die Forschenden möglich sein, wer wann welche Route durch Hamburg genommen hat. Dazu ist zu vermeiden, dass Einzelfahrten im Detail rekonstruiert werden. Möglich ist das durch „Vergröberung“ der Datensätze und Aggregierung mehrerer Fahrten. Auch wird es zur Projektdurchführung voraussichtlich nicht notwendig sein, spezifische Uhrzeiten anstelle grober Zeitfenster sowie präzise Start- und Endpunkte einer Fahrt zu kennen.

Das Projektteam der Universität Bremen hatte sich in ihrer Konzeptskizze unter allen Einsendenden am besten mit diesen datenschutzrechtlichen Implikationen auseinandergesetzt. Zudem hat es durch die Challenge-Veranstalter konkrete Vorgaben zur Datenerhebung und -verwendung erhalten, die der HmbBfDI mit ausgestaltet hat. Daher ist der HmbBfDI optimistisch, dass die Umsetzung Modell-

charakter für die Datennutzung im Gemeinwohlinteresse auch auf Basis sensibler Informationen und im Einklang mit den Rechten Betroffener aufzeigen wird.

15. Audiovisuelle Umgebungserfassung bei Entwicklungsfahrten

Am 27. September 2023 hat die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, ein Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten beschlossen. Der HmbBfDI hat als Mitglied einer aus sieben Aufsichtsbehörden bestehenden Arbeitsgruppe aktiv an der Entstehung des Papiers mitgewirkt.

Mit dem Positionspapier adressiert die DSK datenschutzrechtliche Fragen im Zusammenhang mit der Verarbeitung audiovisueller Umgebungsdaten, die Automobilhersteller und Zulieferer zum Zwecke der Entwicklung automatisierten und autonomen Fahrens im Rahmen sog. Entwicklungsfahrten sammeln. Die unter realen Fahr- und Verkehrsbedingungen stattfindenden Entwicklungsfahrten werden durch speziell ausgerüstete Testfahrzeuge absolviert, die Verkehrssituationen insbesondere durch Video- und Audioaufnahmen optisch und akustisch erfassen. Dieses Datenmaterial dient nach Angaben der Hersteller dazu, die zu entwickelnden Systeme anhand des realen Verkehrsgeschehens zu trainieren. Zu den so erhobenen Umgebungsdaten zählen auch Daten Verkehrsteilnehmender – wie bspw. Kfz-Kennzeichen –, die sich in räumlicher Umgebung der Testfahrzeuge aufhalten.

Das Positionspapier befasst sich insbesondere mit der rechtlichen Grundlage und den Anforderungen an die Transparenz der Verarbeitung dieser Daten sowie dem Umgang mit Betroffenenrechten nach Art. 15 ff. der Datenschutz-Grundverordnung (DSGVO).

Als Rechtsgrundlage der Datenverarbeitung wird Art. 6 Abs. 1 UAbs. 1 lit. f) der DSGVO herangezogen. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Die DSK erkennt ein berechtigtes Interesse der verantwortlichen Hersteller an der Entwicklung von Fahrassistenzsystemen und -funktionen sowie des automatisierten und autonomen Fahrens im Grundsatz an. Sie verdeutlicht aber auch, dass die Verarbeitung audiovisueller Daten zu Entwicklungszwecken strafrechtlich gesetzte Grenzen nicht überschreiten und sich insbesondere nicht über die Bestimmungen des § 201 und § 201a des Strafgesetzbuches hinwegsetzen darf, wonach Verletzungen der Vertraulichkeit des Wortes und des höchstpersönlichen Lebensbereichs durch Audio- und Bildaufnahmen unter Strafe gestellt werden. Das Positionspapier betont, dass an strafbaren Datenverarbeitungsvorgängen bereits kein berechtigtes Interesse im Sinne des Datenschutzrechts bestehen kann.

Inwieweit die Erfassung audiovisueller Umgebungsdaten zur Verwirklichung der Entwicklungszwecke der Verantwortlichen im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO erforderlich ist, misst die DSK daran, ob diese Zwecke in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden können, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen. Als milderes Mittel in diesem Sinne benennt das Positionspapier u.a. die Datenverarbeitung unter Einsatz technischer Maßnahmen wie des Schwärzens, Verpixelns oder einer automatisierten Löschung unerheblicher Informationen. Entsprechend werden die Verantwortlichen verpflichtet, in regelmäßigen Abständen unter Berücksichtigung des Stands der Technik zu überprüfen, inwieweit etwa automatisierte Anonymisierungs- oder Löschverfahren einge-

setzt werden können, um den Eingriff in Persönlichkeitsrechte abzumildern oder auszuschließen. Das Positionspapier stellt klar, dass das Ergebnis dieser Prüfung zu dokumentieren ist.

Schließlich arbeitet die DSK Kriterien heraus, die im Rahmen der Abwägung zwischen den berechtigten Interessen der Verantwortlichen und den Interessen oder Grundrechten und -freiheiten der betroffenen Personen nach Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO Berücksichtigung finden können.

Auf der Herstellerseite soll demnach, soweit im konkreten Einzelfall zutreffend, positiv gewertet werden können, dass die zu entwickelnden Fahrfunktionen der Verbesserung der Verkehrssicherheit dienen, die Datenerfassung nicht auf die Identifizierung individueller Personen oder Personengruppen abzielt und personenbezogene Daten damit lediglich kurzzeitig und gleichsam im Nebeneffekt erhoben werden.

Auf der Betroffenenseite soll insbesondere die Intensität des Eingriffs in Persönlichkeitsrechte zu berücksichtigen sein. Der Eingriff wiege umso schwerer, wenn Daten offensichtlich nicht am Straßenverkehr beteiligter Personen erhoben würden, die regelmäßig nicht damit rechnen müssten, zu Entwicklungszwecken der Automobilindustrie aufgenommen zu werden. Dies gelte bspw. für Personen, die sich in von der Fahrbahn aus einsehbaren Räumlichkeiten, auf der Terrasse eines Gastronomiebetriebs oder auf eingezäunten Schulhöfen oder Spielplätzen aufhalten. Auch infolge einer Mehrfacherfassung bereits abgebildeter Straßenabschnitte könne es zu einer Wiederholung oder Vertiefung des Eingriffs in die Rechte betroffener Personen kommen. Außerdem stellt nach Einschätzung der DSK die Verarbeitung besonders schützenswerter Daten auch in Fällen, in denen Art. 9 Abs. 1 DSGVO keine Anwendung findet, einen intensiven Eingriff dar, der umso schwerer wiegt, wenn die Verarbeitung solcher Daten durch den Verantwortlichen objektiv zu erwarten und technisch oder organisatorisch vermeidbar war. Die Erhebung solcher Daten sei insbesondere dann objektiv zu

erwarten, wenn Einrichtungen oder Veranstaltungen wie z.B. Spielplätze, Kindergärten, Schulen, Krankenhäuser und Orte der Glaubensausübung erfasst würden. Die DSK weist darauf hin, dass die Verantwortlichen vor Durchführung der Entwicklungsfahrt darlegen und entsprechend der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO dokumentieren müssen, aus welchem Grund sich eine audiovisuelle Erfassung entsprechender Einrichtungen als unvermeidbar darstelle. Ein möglicher Grund könne in besonderen Ausnahmefällen etwa die Gewährleistung der hinreichenden funktionalen Sicherheit auch in Gegenwart vulnerabler Personen im Straßenverkehr und damit deren Schutz sein.

Ihren datenschutzrechtlichen Transparenzpflichten können die verantwortlichen Hersteller und Entwickler ausweislich des Positionspapiers nachkommen, indem sie die Entwicklungsfahrzeuge mit gut sichtbaren Piktogrammen zur stattfindenden Audio- und Videoaufzeichnung sowie den wesentlichen Informationen zum Verantwortlichen, dem Hauptverarbeitungszweck und der URL einer Informationsseite versehen. Auf Letzterer müsse dann eine vollständige Datenschutzerklärung zur Verfügung gestellt werden.

Im Zusammenhang mit den Betroffenenrechten nach Art. 15 ff. DSGVO führt die DSK insbesondere aus, dass die Identifizierung einer im Fahrzeugumfeld erfassten Person für die Verarbeitung der Daten zu Entwicklungszwecken nicht erforderlich sei. Damit sei der Anwendungsbereich des Art. 11 DSGVO eröffnet. Gemäß Art. 11 Abs. 2 S. 1, S. 2 1. HS DSGVO entfallen die aus Artikel 15 bis 20 DSGVO resultierenden Pflichten des Verantwortlichen, wenn er nachweisen kann, dass er nicht in der Lage ist, die potenziell betroffene Person zu identifizieren. Etwas Anderes gilt gemäß Art. 11 Abs. 2 S. 2 2. HS DSGVO nur dann, wenn die betroffene Person im Einzelfall selbst zusätzliche Informationen bereitstellt, die ihre Identifizierung ermöglichen. Entsprechend hat nach der DSK eine Auskunftserteilung gemäß Art. 15 DSGVO zu erfolgen, wenn die betroffene Person Angaben macht, die dem Verantwortlichen die Feststellung, ob sie Gegenstand einer audiovisuellen Aufzeichnung gewesen sein

könnte, möglich machen. In Betracht komme etwa die Benennung des genauen Ortes und Zeitpunkts der Aufnahme. Die DSK verpflichtet die Hersteller, betroffene Personen darüber zu informieren, welche Angaben im Einzelnen für eine Identifizierung benötigt werden.

Ob Bedarf für eine darüberhinausgehende gesetzliche Regelung der audiovisuellen Umgebungserfassung in Fahrzeugen sowohl bei Entwicklungsfahrten als auch im Regelbetrieb besteht, wird eine im Auftrag der DSK eingesetzte Arbeitsgruppe, welcher auch der HmbBfDI angehört, im Frühjahr 2024 prüfen.

16. Abo Modelle Medienhäuser / Abo Modell Beschluss DSK

Eine lang erwartete Positionierung der Datenschutzaufsichtsbehörden zu den sogenannten Pur-Abo-Modellen konnte mit dem Beschluss der Datenschutzkonferenz (DSK) „Bewertung von Pur-Abo-Modellen auf Websites" endlich realisiert werden. Der Beschuss geht auf die Initiative des HmbBfDI zurück und wird im eigenen Zuständigkeitsbereich konsequent durchgesetzt.

Als derzeitiger Co-Vorsitz des Arbeitskreises Medien der Datenschutzkonferenz hat der HmbBfDI in der Sitzung des Arbeitskreises im Februar 2023 eine Beschlussvorlage zu den sogenannten Pur-Abo-Modellen mit dem Ziel eingebracht, Aussagen darüber zu treffen, wie derartige Consent-Modelle datenschutzkonform auf den jeweiligen Webseiten eingebunden werden können. Der Beschlussvorlage ging – im Rahmen einer eingerichteten Unterarbeitsgruppe – eine umfassende Analyse verschiedener Beschwerden zu Medienhäusern durch die Organisation NOYB – European Center for Digital Rights voraus, die in mehreren Bundesländern eingereicht wurden.

Zwei dieser Beschwerden bezogen sich auf große Medienhäuser, die in die Zuständigkeit des HmbBfDI fallen und einer eingehen-

den Prüfung unterzogen wurden. Mit den jeweiligen Medienhäusern wurden die verwendeten Consent-Lösungen auf deren Webseiten umfassend erörtert, was im Ergebnis zu einer Anpassung der Banner geführt hat. Insbesondere wurde der Forderung des HmbBfDI nachgekommen, neben der bisher vorzufindenden Zustimmungsvariante und der Wahl eines „Pur-Abos" eine weitere Option im Banner zu implementieren, die es Nutzenden nunmehr ermöglicht, ihre Einwilligung feingranular zu erteilen. Mit dieser Forderung setzt der HmbBfDI außerdem Vorgaben des EuGH in der Rechtssache C-673/17 (Planet49, Entscheidung des EuGH vom 1. Oktober 2019, C-673/17, https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=1513772) um.

Ziel ist es, den Beschluss der DSK einheitlich im Zuständigkeitsbereich des HmbBfDI umzusetzen. Daher ist der HmbBfDI mit weiteren Medienunternehmen im engen Austausch, die zwar nicht von einer NOYB-Beschwerde betroffen waren, aber den Forderungen des DSK-Beschlusses ebenfalls nachkommen müssen. Hierzu zählt auch ein Medienunternehmen, dass erst jüngst in den Zuständigkeitsbereich des HmbBfDI wechselte und zuvor vom LfD Niedersachsen beaufsichtigt wurde. Die Gespräche sind bisher soweit vorangeschritten, dass die Umsetzung des Beschlusses zeitnah von dem Unternehmen zugesichert wurde.

Der veröffentlichte Beschluss (https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf) wurde schließlich nicht nur von verantwortlichen Stellen wegen seines klaren Bekenntnisses zur Legitimation derartiger Banner-Gestaltungen begrüßt, sondern kommt im Grundsatz als denkbare Lösung mittlerweile auch in der Rechtsprechung des EuGH (EuGH vom 4. Juli 2023, C-252/21, Rz. 150, siehe auch: HmbBfDI, Einordnung des EuGH-Urteils Meta gegen das Bundeskartellamt, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231122_Einordnung_EuGH_Meta_BKartA.pdf) zum Ausdruck:

„Daher [Anm. aufgrund der markbeherrschenden Stellung] müssen diese Nutzer die Freiheit haben, im Zuge des Vertragsabschlusses die Einwilligung in bestimmte Datenverarbeitungsvorgänge, die für die Erfüllung des Vertrags nicht erforderlich sind, einzeln zu verweigern, ohne dazu gezwungen zu sein, auf die Nutzung des vom Betreiber des sozialen Online-Netzwerks angebotenen Dienstes vollständig zu verzichten, was bedingt, dass ihnen, gegebenenfalls gegen ein angemessenes Entgelt, eine gleichwertige Alternative angeboten wird, die nicht mit solchen Datenverarbeitungsvorgängen einhergeht."

17. Fachprüfung eines Konformitätsbewertungsprogramms

Die fachlichen Prüfungen eines Programms zur Zertifizierung nach DSGVO sind aufgrund des Rückzugs des Antragstellers eingestellt worden.

In den drei zurückliegenden Berichtsjahren hat der HmbBfDI über das Verfahren berichtet, bei dem er in seiner Rolle als Akkreditierungsstelle nach Art. 42, 43 DSGVO gegenüber einem Hamburger Unternehmen tätig wurde (zuletzt im 31. TB Datenschutz 2022, Kap. III 12). Dieses hat als sog. Programmeigner ein Konformitätsbewertungsprogramm entwickelt, das als Grundlage für Zertifizierungen nach dem Datenschutzrecht dienen soll, nachdem es die einschlägigen nationalen und europäischen Anforderungen erfüllt.

Wir hatten insbesondere die Aufwände geschildert, die in dem komplexen Zusammenspiel der Akteure besteht. Neben dem HmbBfDI als fachlich prüfender Stelle ist dies die DAkkS (Deutsche Akkreditierungsstelle) und im weiteren Verfahren auch der Europäische Datenschutzausschuss (EDSA), der die verschiedenen Programme auf nationaler Ebene mit Blick auf einheitliche europäische Maßstäbe qualitätssichernd zusätzlich überprüft. Der HmbBfDI hat im Berichtszeitraum in diesem Rahmen in Kooperation mit anderen

europäischen Aufsichtsbehörden ein niederländisches Konformitätsbewertungsprogramm kommentiert und begleitet.

Im laufenden Berichtsjahr hat das hamburgische Unternehmen seinen Antrag auf Konformitätsprüfung zu unserem Bedauern zurückgezogen. Die bereits eingeleiteten europäischen Abstimmungen nach Abschluss unserer eigenen fachlichen Begutachtung wurden daher eingestellt.

Auch ohne ein laufendes Verfahren auf Grundlage des Antrags eines Programmeigners wird der HmbBfDI das Thema Akkreditierung und Zertifizierung im Rahmen des Arbeitskreises Zertifizierung der DSK begleiten und auch die Entwicklungen auf europäischer Ebene verfolgen. Auch wenn mittlerweile einige Konformitätsbewertungsprogramme in verschiedenen EU-Mitgliedstaaten final genehmigt wurden und der Bedarf insbesondere für generische Programme, die sämtliche DSGVO-relevanten Verarbeitungsvorgänge abdecken, insgesamt begrenzt sein dürfte, können jederzeit neue Anträge bei der DAkkS eingehen. Soweit sich die Antragsteller in der Zuständigkeit des HmbBfDI befinden, wird ihm die fachliche Prüfung obliegen.

18. Renten-Bingo

Der HmbBfDI hat die Rechtmäßigkeit der Datenverarbeitung zur Zusendung von Briefwerbung für das sog. Renten-Bingo untersucht. Nach Feststellung entsprechender Mängel stellte der Verantwortliche die Verarbeitung ein und wurde förmlich verwarnt.

Die Otto GmbH & Co. KG (im Folgenden: OTTO) hat auf Grundlage einer Kooperation mit der Faber Lotto-Service GmbH (im Folgenden: FABER) Kund:innen, die mindestens 50 Jahre alt sind, Briefwerbung zu deren anstehendem Geburtstag zugesandt. Diese bestand aus einem personalisierten Anschreiben von OTTO, dem eine sog. Bingo-Rubbelkarte für das von FABER organisierte Renten-Bingo

beigefügt war. In dem Anschreiben pries OTTO die Bingo-Rubbelkarte als besonderes Geburtstagsgeschenk an und empfahl die Teilnahme am FABER-Renten-Bingo. In der Fußzeile fand sich zudem der Hinweis, dass ,,bei Annahme eines weiteren Geschenks'' ein Goldbarren aus Feingold 999 gewonnen sei. Die Teilnahme am Renten-Bingo erforderte einen Anruf bei FABER, bei dem neben dem Mitspielcode auch personenbezogene Daten der Anrufer:innen abgefragt wurden. Empfänger:innen der Briefwerbung vermuteten eine unerlaubte Weitergabe ihrer personenbezogenen Daten an FABER und reichten Beschwerde beim HmbBfDI ein.

OTTO teilte auf entsprechende Nachfrage des HmbBfDI mit, dass keine Weitergabe der Daten von Kund:innen an FABER erfolgt, sondern erst der Anruf dazu führt, dass FABER Kenntnis von den personenbezogenen Daten erlangt. Diese Angaben bestätigten sich im Rahmen der Überprüfung des Kooperationsvertrags. Der HmbBfDI ließ sich jedoch auch die Rechtsgrundlage der Verarbeitung von Kund:innendaten zu Zwecken der Briefwerbung im Sinne der Kooperation darlegen. OTTO berief sich auf die Rechtsgrundlage des berechtigten Interesses aus Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DSGVO). Diese Rechtsgrundlage erfordert neben dem Vorliegen eines berechtigten Interesses des Verantwortlichen oder eines Dritten an der Datenverarbeitung auch eine Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person, die im Ergebnis nicht überwiegen dürfen. Erwägungsgrund 47 zur DSGVO gibt für die Interessenabwägung vor, dass sich die Zulässigkeit der Datenverarbeitung an den vernünftigen Erwartungen der betroffenen Person unter Berücksichtigung der konkreten Beziehung zum Verantwortlichen messen lassen muss. Entscheidend ist, ob eine Datenverarbeitung zu dem konkreten Zweck und in der konkreten Art und Weise überraschend ist oder die betroffene Person vernünftigerweise mit einer derartigen Datenverarbeitung rechnen muss. Bei der Bewertung der vernünftigerweise erwartbaren Datenverarbeitungsmethoden sind auch die Grundsätze einer fairen und transparenten Datenverarbeitung gemäß Art. 5 Abs. 1 lit. a DSGVO zu berücksichtigen.

Der HmbBfDI hat die von OTTO vorgenommene Interessenabwägung unter Berücksichtigung dieser Aspekte überprüft. Hierbei ist er zu dem Ergebnis gelangt, dass die Datenverarbeitung auf Basis der konkreten Kooperation in der Gesamtschau als unfair und intransparent zu bewerten ist und damit nicht den vernünftigen Erwartungen der OTTO-Kund:innen entspricht. Das Anschreiben diente nämlich dazu, die Geschäftsbeziehung der betroffenen Personen zu OTTO und ein ggf. daraus resultierendes Vertrauen zu nutzen, damit diese die Fremdwerbung zur Kenntnis nehmen, der Empfehlung vertrauen und durch einen Anruf bei FABER eigenständig ihre Daten preisgeben. Die Anpreisungen im Anschreiben suggerierten den OTTO-Kund:innen fälschlicherweise, dass es sich bei der Bingo-Rubbelkarte und dem Goldbarren um personalisierte Vorteile handelt, die unter Angabe ihrer Daten bei FABER für sie hinterlegt worden sind. Sie wurden nicht darüber aufgeklärt, dass keine Weitergabe von personenbezogenen Daten an FABER stattgefunden hatte. Die Interessenabwägung fällt somit zugunsten der betroffenen Personen aus, so dass Art. 6 Abs. 1 lit. f DSGVO nicht als Rechtsgrundlage der Datenverarbeitung herangezogen werden kann. Es hätte vielmehr einer Einwilligung der OTTO-Kund:innen gemäß Art. 6 Abs. 1 lit. a DSGVO bedurft.

Nach erster Mitteilung dieser rechtlichen Einschätzung hat OTTO die Kooperation mit FABER umgehend beendet und sich insofern einsichtig gezeigt. Zudem hat OTTO bei der Aufklärung des Vorgangs vollumfänglich und zeitnah kooperiert. Der HmbBfDI hat OTTO aufgrund des festgestellten datenschutzrechtlichen Verstoßes gemäß Art. 58 Abs. 2 lit. b DSGVO förmlich verwarnt.

19. Speicherung von Personalausweisnummern im Hotel

In einem Hamburger Hotel wurden in über 1.000 Fällen die Personalausweisnummern deutscher Gäste ohne Rechtsgrundlage gespeichert.

Im Rahmen seiner Aufsichts- und Kontrolltätigkeiten wurde der HmbBfDI im Dezember 2022 durch eine Beschwerde auf einen Datenschutzverstoß eines Hotelbetriebs aufmerksam gemacht.

Als ein ehemaliger Gast fünf Jahre nach dem Besuch eines Hotels eine Werbe-E-Mail zu seinem Geburtstag erhielt, ersuchte er um Auskunft, ob weitere personenbezogene Daten durch das Hotel verarbeitet wurden. Die Auskunft gemäß Art. 15 DSGVO offenbarte, dass neben seinen Kontaktdaten auch die Personalausweisnummer des Beschwerdeführers seit seinem Aufenthalt im Jahr 2018 von dem Hotel gespeichert wurde. Dies führte dazu, dass der Beschwerdeführer eine Beschwerde beim HmbBfDI einreichte.

Im Rahmen der Ermittlungen stellte sich heraus, dass die Speicherung der Personalausweisnummer des Gastes keinen Einzelfall darstellte. Das Hotel räumte nicht nur den Verstoß ein, sondern gab an, dass die Personalausweisnummern von weiteren über 1.000 deutschen Hotelgästen gespeichert wurden. In jedem dieser Fälle fehlte es an einer Rechtsgrundlage für die Verarbeitung, da keiner der in Art. 6 Abs. 1 S. 1 DSGVO aufgeführten Zulässigkeitstatbestände auf die Speicherung der Personalausweisnummern anwendbar war. Weder lag eine Einwilligung (Art. 6 Abs. 1 S.1 lit. a DSGVO) noch eine rechtliche Verpflichtung (Art. 6 Abs. 1 S. 1 lit. c DSGVO) zur Speicherung vor. Lediglich bei ausländischen Hotelgästen ist die Beherbergungsstätte gem. § 30 Abs. 2 S. 2 Nr. 8 BMG verpflichtet, die Seriennummer des Passes oder des Passersatzpapieres zu verarbeiten. In den ermittelten Fällen lag diese Konstellation allerdings nicht vor.

Durch das Einschreiten des HmbBfDI wurden sämtliche gespeicherten Personalausweisnummern der deutschen Hotelgäste gelöscht, die rechtswidrige Verarbeitung beendet und ein Bußgeldverfahren eingeleitet.

Dieser Vorfall verdeutlicht die Notwendigkeit der Sensibilisierung für die Einhaltung der Datenschutzbestimmungen in der Hotellerie. Die Speicherung von personenbezogenen Daten ohne rechtliche Grundlage kann nicht nur zu empfindlichen Bußgeldern führen, sondern gefährdet auch das Vertrauen der Gäste in den Schutz ihrer persönlichen Informationen. Es bleibt zu hoffen, dass dieses Verfahren eine nachhaltige Wirkung für die Branche entfaltet.

20. Google Street View

Google LLC hat im Jahr 2023 seinen Dienst Street View aktualisiert und erweitert. Am 25. Juli 2023 wurden sämtliche alten Panoramabilder von Straßenzügen in Deutschland aus den Jahren 2008 bis 2010 entfernt. Neue Aufnahmen aus den Jahren 2022 und 2023 wurden hochgeladen. Der HmbBfDI hat die Aktualisierung aufsichtsrechtlich begleitet.

Die Einführung des Google-Dienstes Street View im Jahr 2010 hatte zu einer breiten gesellschaftlichen Debatte geführt. Bei Bürger:innen bestanden erhebliche Bedenken, dass die Aufnahmen ihre Privatsphäre beeinträchtigen könnten. Der HmbBfDI hatte dem Unternehmen damals datenschutzrechtliche Vorgaben für die Veröffentlichung der Bilder von Straßenzügen gemacht. Denn die Bilder zeigen auch private Kraftfahrzeuge, Personen und private Grundstücke. Für Kfz-Kennzeichen und Gesichter hatte der HmbBfDI verlangt, dass diese unkenntlich gemacht werden. Private Grundstücke waren von Google unkenntlich zu machen, wenn die betroffenen Personen Widerspruch gegen die Abbildung eingelegt hatten. Der erhebliche Widerspruch gegen den Dienst führte dazu, dass das Unternehmen über 13 Jahre die Aufnahmen in Deutschland nicht aktualisierte.

An die damaligen Vorgaben hat sich Google nun auch bei der Neuauflage des Dienstes zu halten. Auch jetzt steht Eigentümer:innen und Mieter:innen privater Grundstücke ein Widerspruchsrecht zu, das auch vorab, d.h. vor der Veröffentlichung von Aufnahmen, ausgeübt werden kann (s. hierzu auch die vom HmbBfDI bereitgestellten Informationen unter https://datenschutz-hamburg.de/news/neue-bilder-bei-google-street-view-1). Der HmbBfDI hatte Google dazu aufgefordert, in der Pressekommunikation auf dieses (Vorab-) Widerspruchsrecht und die Möglichkeiten der Ausübung rechtzeitig vor der Veröffentlichung der neuen Bilder ausdrücklich hinzuweisen. Er hat die Einhaltung der datenschutzrechtlichen Vorgaben durch Google mit Bezug auf die Veröffentlichung der Bilder überwacht, Mängel in der Umsetzung bei dem Unternehmen beanstandet und zur Einhaltung der DSGVO-Vorgaben aufgefordert.

So fiel anhand von beim HmbBfDI eingelegten Beschwerden auf, dass Google als Antwort auf per E-Mail oder Post eingelegte Widersprüche gegen die Abbildung von Häuserfronten häufig mitteilte, dass der Widerspruch nicht bearbeitet werden könne, da eine Zuordnung der genannten Anschrift zu einem konkreten Grundstück nicht möglich sei. Das Unternehmen bat in den Fällen, den Widerspruch erneut über das Online-Formular Googles einzulegen. Hier wies der HmbBfDI Google darauf hin, dass das Unternehmen anhand einer mitgeteilten Anschrift unter Ausschöpfung sämtlicher frei zugänglicher Informationsquellen (wie etwa der Geodatenportale der Länder) eine Zuordnung zu dem betreffenden Grundstück vorzunehmen hat und er einen Verweis auf eine nochmalige Einlegung des Widerspruchs für nicht datenschutzkonform hält. Google hat die Bearbeitungsprozesse angepasst, sodass den HmbBfDI Beschwerden über die Aufforderung, den Widerspruch erneut über das Online-Formular einzulegen, seither kaum noch erreichen.

In vielen Fällen erfolgte, insbesondere bei per Post und per E-Mail eingelegten Widersprüchen, keine zeitnahe Information der betroffenen Personen über eine Berücksichtigung des Widerspruchs. Auch dies beanstandete der HmbBfDI gegenüber Google. Das Unter-

nehmen holt unterbliebene Mitteilungen an betroffene Personen inzwischen nach.

Auch ergab sich aus beim HmbBfDI eingelegten Beschwerden, dass Google an Personen, die Widerspruch gegen die Abbildung ihres Grundstücks eingelegt hatten, zunächst keine Hinweise nach Art. 13 DSGVO versandte, etwa dazu, welche Informationen aus dem Widerspruch wie lange bei Google gespeichert werden. Der HmbBfDI beanstandete gegenüber Google das Unterbleiben der Information. Das Unternehmen übersendet diese seither an die betroffenen Personen, die Widerspruch eingelegt haben, und teilt auch im Online-Widerspruchsformular entsprechende Informationen nunmehr mit.

Mit Bezug auf Googles Online-Formular für Widersprüche hat der HmbBfDI zudem beanstandet, dass Google hierin die Angabe forderte, ob die Berechtigung zum Widerspruch gegen die Abbildung der Häuserfront aus einer Stellung als Eigentümer:in oder aus einer Stellung als Mieter:in folgt. Dafür sah Google ein Feld mit den beiden Optionen vor, von denen die Betroffenen eine auszuwählen hatten. Da Google die Berechtigung in aller Regel nicht überprüft, hielt der HmbBfDI es vor dem Hintergrund des Grundsatzes der Datensparsamkeit nicht für erforderlich, diese Daten standardmäßig zu erheben. Google hat die Abfrage, ob die Berechtigung aus Eigentum oder aus Miete folgt, daraufhin aus dem Online-Formular entfernt.

Weitere Beschwerden erreichten den HmbBfDI in Fällen, in denen Unkenntlichmachungen trotz Widerspruchs nicht oder nur unzureichend vorgenommen wurden. In diesen Fällen forderte der HmbBfDI Google zur Berücksichtigung des Widerspruchs auf.

Aus Sicht des HmbBfDI hat sich gezeigt, dass die frühzeitige Einbindung der Aufsichtsbehörde durch das Unternehmen und die unternehmensseitige Kooperation zu Beginn und im Verlauf der Bereitstellung des Dienstes hilfreich waren, um die Datenschutzkonformität zu sichern und so die Grundrechte der betroffenen Personen zu wahren. Zugleich führte die offene Kommunikation zwar zu

öffentlichem Interesse, aber nicht zu einer mit 2010 vergleichbaren kritischen Debatte. Dies mag auch ein Hinweis auf eine veränderte Einstellung der Bürger:innen zur Digitalisierung sein, obgleich die Zahl der ausgeübten Widersprüche in Deutschland weit über denen in anderen Ländern liegen.

21. Akkreditierung zur Gruppenauslosung der Fußball-Europameisterschaft

Am 2.12.2023 hat die UEFA beim Final Draw in der Elbphilharmonie die Vorrundengruppen der Fußball-Europameisterschaft 2024 ausgelost. Die im Konzerthaus beschäftigten Personen wurden dazu einer Zuverlässigkeitsüberprüfung unterzogen. Bei dieser Akkreditierung hat der HmbBfDI zwischen den Interessen der Beschäftigten des Konzerthauses und des europäischen Fußballverbands vermittelt.

Das Hamburgische Polizeirecht sieht in § 51 PolDVG vor, Zuverlässigkeitsüberprüfungen der Beschäftigten vorzunehmen, die sich bei einer besonders gefährdeten Veranstaltung aufhalten. Eine solche Veranstaltung war die Gruppenauslosung zur Fußball-Europameisterschaft in der Elbphilharmonie. Daher war es Aufgabe des Veranstalters, die Kontaktdaten der Mitarbeiter:innen, die im Veranstaltungszeitraum im Konzerthaus präsent waren, mit deren Zustimmung aufzunehmen. Die Informationen waren der Polizei weiterzureichen, damit diese einen Abgleich mit ihren eigenen Datenbanken vornehmen kann. Ziel der Regelung ist es, keine bekannten Gefährder zu der Veranstaltung zuzulassen. Der Überprüfung unterlag nicht nur das Personal, das den Konzertsaal betritt, sondern auch beispielsweise Beschäftigte, die in der Elbphilharmonie ihren Büroarbeitsplatz haben. Das gesetzlich vorgesehene Verfahren ist nicht zu beanstanden und mit dem AK Sicherheit der Datenschutzkonferenz abgestimmt.

Fraglich war jedoch, ob alle erhobenen Daten für die Zuverlässigkeitsüberprüfung erforderlich sind. Zur direkten Kommunikation

mit den Einzelpersonen hat die UEFA als Veranstalter auch die E-Mail-Adressen und Telefonnummern der Beschäftigten in der Elbphilharmonie abgefragt. Unter der Maßgabe der Datenminimierung kam die Frage auf, ob die UEFA diese beiden persönlichen Angaben erheben darf, obwohl etwaige Rückfragen auch über den Arbeitgeber adressiert werden konnten. Da in dieser Hinsicht auch besonders qualifiziertes Schlüsselpersonal Zurückhaltung zeigte, der UEFA ihre Telefonnummer zu übermitteln, stand zwischenzeitlich die reibungslose Durchführung der Veranstaltung in Frage.

Der HmbBfDI hat zwischen den Interessen der UEFA auf unbürokratische Kontaktaufnahme und der Privatsphäre der Betroffenen vermittelt. Als sachgerechte Lösung wurde die Einigung erzielt, auf die Angaben individueller Telefonnummern verzichten zu können. Da als E-Mail-Adresse das berufliche Postfach verwendet werden konnte, mussten der UEFA so keine Angaben aus dem privaten Kontext offengelegt werden, die nicht zur Zuverlässigkeitsüberprüfung notwendig sind. Wegen des zeitlichen Drucks der kurz bevorstehenden Veranstaltung konnte das Pflichtfeld Telefonnummer nicht mehr technisch angepasst werden, jedoch wurde den Beschäftigten kommuniziert, dass auch ein Platzhalter wie z.B.“0000“ akzeptiert werde.

Für das Turnier im Sommer 2024 ist diese Kompromisslösung nur bedingt übertragbar, weil die Vielzahl der Spielorte und der Einsatz externer Arbeitskräfte ein höheres Bedürfnis an direkter Kommunikation nach sich ziehen. Zudem besteht bei in Stadien beschäftigten Personen ein engerer Sachzusammenhang zur UEFA als bei Mitarbeitenden in der Elbphilharmonie. Dazu tauscht sich der HmbBfDI mit dem Fußballverband unter Einbeziehung des AK Sicherheit der Datenschutzkonferenz aus.

BUSSGELDER IV.
ANORDNUNGEN, GERICHTSVERFAHREN

BUSSGELDER, ANORDNUNGEN, GERICHTSVERFAHREN

1. Beschäftigtendatenschutz: Information von Arbeitgeber:innen über krankheitsbedingte Abwesenheiten

Beschäftigten darf nicht die Pflicht auferlegt werden, ihre krankheitsbedingte Abwesenheit gegenüber einer Vielzahl von Kolleg:innen offenzulegen, wenn dies für die Zwecke der Aufgabenplanung und -umverteilung gar nicht erforderlich ist. Geschieht dies dennoch, drohen empfindliche Bußgelder.

Im Berichtszeitraum hat der HmbBfDI ein Bußgeldverfahren gegen ein in Hamburg ansässiges Unternehmen wegen Verstößen gegen Art. 32 DSGVO und Art. 9 DSGVO durchgeführt. Der HmbBfDI wurde aufgrund einer Beschwerde auf dieses Unternehmen aufmerksam. Der Beschwerdeführer bemängelte, dass er seine krankheitsbedingten Abwesenheiten per E-Mail einem großen Kreis von Kolleg:innen und Vorgesetzten mitteilen müsse, obwohl er mit einem Teil der Personen nicht direkt zusammenarbeite. Ferner habe sein Vorgesetzter den E-Mailverteiler zum Versand einer E-Mail genutzt, in der seine gesamten krankheitsbedingten Abwesenheitstage anprangernd aufgelistet worden seien.

Nach den Feststellungen des HmbBfDI gab es in dem Unternehmen interne Regelungen zu den Anzeige- und Nachweispflichten von Beschäftigten bei Erkrankungen. Diese sahen vor, dass die Krankmeldung grundsätzlich bei der Führungskraft der jeweiligen Abteilung zu erfolgen hat. Von diesem festgelegten Verfahren war eine Abteilung des Unternehmens mindestens für den Zeitraum von einem Jahr abgewichen. Die Beschäftigten dieser Abteilung waren vom Abteilungsleiter angehalten worden, ihre krankheitsbedingten Abwesenheiten durch eine E-Mail unter Verwendung eines eingerichteten E-Mailverteilers anzuzeigen. Dieser Verteiler enthielt 25 Empfänger. Bei den Empfängern handelte es sich nicht nur um die Vorgesetzten

der Beschäftigten und deren Vertreter. Der Verteiler enthielt vielmehr auch Personen, die in keinem direkten Arbeitszusammenhang mit dem jeweiligen Beschäftigten standen und deren Arbeitsabläufe und Aufgabenwahrnehmung durch die Abwesenheit des Beschäftigten nicht berührt waren.

Bei den über den Verteiler versandten Krankmeldungen handelte es sich um Gesundheitsdaten, die gemäß Art. 9 Abs. 1 DSGVO zu den „besonderen Kategorien personenbezogener Daten" zählen. Der Verordnungsgeber räumt diesen Daten eine besondere Stellung ein. Da sie ihrem Wesen nach besonders sensibel sind, werden an ihren wirksamen Schutz gesteigerte Anforderungen gestellt. Der gebotene wirksame Schutz wurde durch die Verwendung des großen E-Mailverteilers bei der Anzeige von Erkrankungen nicht gewährleistet. Durch die Vorgabe des Abteilungsleiters, für die Meldung von krankheitsbedingten Abwesenheiten den eingerichteten E-Mail-Verteiler zu verwenden, wurde ein Verfahren etabliert, durch das Gesundheitsdaten von Beschäftigten mit einer großen Gruppe von Kolleg:innen und Vorgesetzten geteilt werden mussten. Dieses Vorgehen erfolgte ausschließlich aus Praktikabilitätsgründen nach dem Motto „lieber zu viele Personen über die Abwesenheit von einzelnen Beschäftigten informieren als zu wenige", ohne dass eine tatsächliche Erforderlichkeit gegeben war. Die Übermittlung von Krankmeldungen an den direkten Vorgesetzten sowie die für Personalfragen verantwortliche Stelle bzw. an einen jedenfalls deutlich kleineren Adressatenkreis wäre zur Wahrung der Rechte und Pflichten des Arbeitgebers ausreichend gewesen.

Ebenfalls nicht erforderlich und damit rechtswidrig war nach den Feststellungen des HmbBfDI die von dem Abteilungsleiter per E-Mail vorgenommene Offenlegung der zusammengestellten Fehlzeiten des Beschwerdeführers gegenüber einer Vielzahl von Kolleg:innen. Die mit dem Versand der E-Mail einhergehende Verarbeitung der Gesundheitsdaten des Beschwerdeführers diente weder der Ausübung von Rechten noch der Erfüllung rechtlicher Pflichten aus dem Arbeitsverhältnis. Sie erfolgte offenkundig mit dem Zweck, den betroffenen

Beschäftigten vor seinen Kolleg:innen zu maßregeln und bloßzustellen. Dies fällt aber nicht in den Rechts- und Pflichtenkreis eines Arbeitgebers. Zur Vorbereitung eines bilateralen Gesprächs mit dem Beschwerdeführer – welches in der Tat die Ausübung eines arbeitsrechtlichen Rechts darstellen würde – war die Offenlegung der zusammengestellten Gesundheitsdaten des Beschwerdeführers gegenüber einer Vielzahl anderer Beschäftigter jedenfalls nicht erforderlich.

Der HmbBfDI hat wegen dieser Verstöße ein Bußgeld in Höhe von 75.000 Euro verhängt. Bei der Zumessung des Bußgelds wurde mildernd berücksichtigt, dass eine umfangreiche Zusammenarbeit mit der Aufsichtsbehörde stattgefunden hat, um den Verstößen abzuhelfen und dem Beschwerdeführer zum Zwecke der Wiedergutmachung ein Schmerzensgeld gezahlt wurde. Schärfend wurde der Umstand berücksichtigt, dass es sich bei den verarbeiteten Daten um Gesundheitsdaten handelte. Es wurden somit besondere Arten personenbezogener Daten verarbeitet, die ihrem Wesen nach sensibel sind und nach den Vorschriften der DSGVO einem besonderen Schutz unterliegen.

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

2. Mitarbeiterexzess live on Twitch.tv

Der HmbBfDI hat eine Geldbuße gegen einen Mitarbeiter eines Kreditinstituts verhängt, der live auf der Plattform twitch.tv personenbezogene Daten eines Gegenspielers in einem Videospiel abgefragt hatte, um diesen persönlich aufzusuchen.

Das Live-Streaming-Videoportal Twitch (twitch.tv) der Amazon.com, Inc., wird vorrangig zur Übertragung von Videospielen und zum Interagieren mit Zuschauern im Chat genutzt. Registrierte Nutzer:innen können einen eigenen Kanal erstellen und übertragen

dabei typischerweise Gameplay diverser Videospiele. Teilweise filmen sich die Spieler („Streamer“) dabei selbst, um die Interaktion mit ihren Zuschauern zu verbessern. Diese kommentieren das Spielgeschehen über die Chatfunktion und können mit anderen Zuschauern sowie dem Streamer interagieren.

Im Berichtszeitraum hat eine solche Übertragung eines Videospiels Anlass zur Einleitung eines Ordnungswidrigkeitenverfahrens durch den HmbBfDI gegeben: Ein Streamer hatte Gameplay des Videospiels Valorant, ein kostenfrei spielbarer Ego-Shooter der Firma Riot Games, übertragen und sich dabei selbst gefilmt. Bei dem Videospiel Valorant treten zwei Gruppen von jeweils fünf Spielern gegeneinander an und versuchen sich gegenseitig auszuschalten. Im Verlaufe des Spiels hatte sich der Streamer zunehmend über einen Spieler einer gegnerischen Gruppe geärgert und szenetypische Verbalinjurien geäußert. Nach einer weiteren Emotionalisierung hatte der Streamer sodann den von ihm gefassten Entschluss verkündet, den Wohnort des Gegenspielers zu ermitteln und ihn tags darauf aufzusuchen, unter Inaussichtstellung körperlicher Gewalt.

Zur Ermittlung des Wohnorts des anderen Spielers war der Streamer aus zwei Gründen in der Lage: Zum einen wurde ihm aus den Reihen seiner Zuschauer der Klarname des Gegenspielers zugespielt. Zum anderen hatte er eine herausgehobene Position in einem Kreditinstitut inne und deshalb Zugriff auf die Kundendatenbank des Kreditinstituts. Eine solche Abfrage der Kundendatenbank nahm der Streamer sodann vor. Im Besonderen konnten die Zuschauer des Streams mitverfolgen, wie der Streamer über geraume Zeit eine Recherche an seinem iPad durchführte und regelmäßig Zwischenstände über Rechercheerfolge berichtete. Dabei vermied es der Streamer unter Verweis darauf, dass er während der Übertragung nicht zu viel offenbaren dürfe, konkrete personenbezogene Daten des Gegenspielers aus der Datenbankabfrage offenzulegen. Gleichwohl machte er explizit deutlich, umfangreiche personenbezogene Daten abgerufen zu haben. Dass die Recherche tatsächlich erfolgreich war, zeigte sich auch am angekündigten Hausbesuch tags darauf. Zu einer körperli-

chen Auseinandersetzung kam es entgegen der Ankündigungen des Twitch Streamers nicht.

Gegen den Streamer hat der HmbBfDI eine Geldbuße im mittleren vierstelligen Bereich verhängt. Durch den Missbrauch der durch seinen Arbeitgeber eingeräumten Zugriffsrechte war er als Verantwortlicher anzusehen. Es handelt sich insoweit um einen Mitarbeiterexzess, bei dem Mitarbeiter geschäftliche oder dienstliche Mittel zu eigenen (privaten) Zwecken nutzen und sich damit zu Verantwortlichen aufschwingen.

Der Bußgeldzumessung waren die wirtschaftlichen Verhältnisse zu Grunde zu legen. Diese waren mangels konkreter Angaben zu schätzen. Objektive Anhaltspunkte zur Schätzung hatte der Streamer mehrfach innerhalb seines Streams geäußert und wiederholt betont, wie gut er wirtschaftlich dastehe, gerade und im Besonderen im Verhältnis zu seinem Gegenspieler.

Ferner war die Vorsätzlichkeit der Begehung zu berücksichtigen. Dem Streamer war bekannt, dass die Kundendaten des Arbeitgebers, dem Bankgeheimnis unterliegen und nur zu geschäftlichen Zwecken genutzt werden dürfen. Die Geldbuße wurde von ihm akzeptiert, der Bescheid ist rechtskräftig.

3. Geldbuße gegen Kindertagesstätte

Der HmbBfDI hat eine Geldbuße gegen eine Kindertagesstätte festgesetzt, die Aktenordner mit personenbezogenen Daten betreuter Kinder und deren Erziehungsberechtigten in einem öffentlich zugänglichen Altpapier-Depotcontainer entsorgt hat.

Im Frühjahr des zurückliegenden Berichtszeitraums machte ein Hamburger eine Entdeckung in einem Altpapier-Depotcontainer der Stadt Hamburg: Öffentlich zugänglich und unversehrt befanden sich

dort mehrere Aktenordner einer nahegelegenen Kindertagesstätte. Die Aktenordner enthielten eine Vielzahl von Dokumenten, wie z.B. Betreuungsverträge mit den Kontodaten Erziehungsberechtigter, von Bezirksämtern ausgestellte Kita-Gutscheine, Impfausweise von Kindern, Abholerlaubnisse, Kopien von Ausweisdokumenten Erwachsener, detaillierte Informationsbögen betreuter Kinder, Ergebnisse von Kindervorsorgeuntersuchungen und vieles mehr. Der Finder des Konvoluts informierte daraufhin die Kindertagesstätte, die aber nicht gewillt war, eine hinreichende Abhilfe für den offensichtlichen Missstand herbeizuführen. Dem Anrufer wurde lediglich angeboten, die Aktenordner selbst bei der Kindertagesstätte vorbeizubringen. Demgegenüber verweigerte die Kindertagesstätte eine Abholung oder das Angebot einer sachgerechten Vernichtung der Dokumente durch den Finder. Richtigerweise bezog dieser sodann den HmbBfDI ein.

Nach Prüfung der Sach- und Rechtslage sowie Anhörung der Kindertagesstätte setzte der HmbBfDI eine Geldbuße im niedrigen vierstelligen Bereich fest.

Die unsachgemäße Entsorgung von Dokumenten verstößt gegen Art. 32 Abs. 1 DSGVO. Hinzutritt, dass im vorliegenden Fall personenbezogene Daten von Kindern, d.h. von besonders schützenswerten Personen, für jedermann einsehbar waren. Auch enthielten die Aktenordner detaillierte Entwicklungsdokumentationen, Kontaktinformationen, in einigen Fällen Gesundheitsdaten und auch Informationen über Eltern und Abholberechtigte. In einem Dokument zur Vorsorgeuntersuchung wurde die Entwicklung der Hoden eines Jungen beschrieben, in einem anderen Dokument erklärt, dass ein Kind nun in der Lage sei, selbstständig die Toilette zu benutzen, aber noch lernen müsse, besser mit dem Reißverschluss umzugehen. Diese Beispiele verdeutlichen, dass die in einer Kindertagesstätte verarbeiteten personenbezogenen Daten der Kindesentwicklung naturgemäß intimste Einblicke ermöglichen. Darüber hinaus waren Kontaktdaten und Kontodaten im Zusammenhang mit Betreuungsverträgen verarbeitet worden. Viele Dokumente enthielten auch Unterschriften

der Eltern. In zwei Fällen wurden Kopien von Ausweisdokumenten entsorgt. Solchen Daten wohnt ein hohes Missbrauchspotenzial inne.

Aufgrund der Qualität der personenbezogenen Daten und der Tatsache, dass es sich bei vielen der Betroffenen um Kinder handelte, hat es der HmbBfDI für notwendig erachtet, eine Geldbuße zu verhängen. Bei der Bemessung der Geldbuße wurde zugunsten der Kindertagesstätte berücksichtigt, dass es sich um einen Erstverstoß handelte und lediglich eine fahrlässige Begehung nachgewiesen werden konnte. Die Geldbuße wurde akzeptiert, der Bescheid ist rechtskräftig.

4. Anweisung zur Erteilung einer Auskunft

Der HmbBfDI hat gegen einen Inkassodienstleister eine Anweisung zur Erteilung einer Auskunft und Bereitstellung einer Datenkopie erlassen. Diese muss nun mit Zwangsgeld durchgesetzt werden.

Den HmbBfDI hat eine Beschwerde erreicht, nach welcher ein Inkassodienstleister den Antrag eines Schuldners auf Auskunft und Datenkopie nach Art. 15 Abs. 1 und 3 DSGVO nicht beantwortet habe. Der HmbBfDI wandte sich daraufhin an den Inkassodienstleister. Im Rahmen der Prüfung teilte der Inkassodienstleister mit, dass er der Auffassung sei, als Rechtsdienstleister nach dem Rechtsdienstleistungsgesetz (RDG) weder zur Erteilung von Auskünften verpflichtet zu sein noch die Betroffenen über die Ablehnung ihrer Anträge informieren zu müssen. Nach seiner Ansicht sei seine Tätigkeit mit Rechtsanwält:innen vergleichbar. Er würde daher ebenso wie diese einer Schweigepflicht im Sinne eines Mandatsgeheimnisses unterliegen. Der HmbBfDI teilt die Auffassung nicht. Rechtsanwält:innen sind, wenn sie Inkassodienstleistungen übernehmen, grundsätzlich zur Erteilung der Auskünfte verpflichtet. Der Inkassodienstleister hielt trotz entsprechender Hinweise des HmbBfDI dennoch an seiner Position fest.

Der HmbBfDI hat daraufhin eine Anweisung nach Art. 58 Abs. 2lit. c) DSGVO erlassen und forderte den Inkassodienstleister dazu auf, dem Beschwerdeführer sowohl eine Auskunft gemäß Art. 15 Abs. 1 DSGVO zu erteilen als auch eine Datenkopie gemäß Art. 15 Abs. 3 DSGVO zur Verfügung zu stellen und dem HmbBfDI diese Umsetzung anzuzeigen. Für den Fall der Nichtumsetzung der Maßnahme binnen 2 Wochen wurde ein Zwangsgeld angedroht.

Diese Maßnahme hatte zunächst keinen Erfolg. Zwar kontaktierte der Inkassodienstleister den Beschwerdeführer nach Erlass der Anweisung und teilte allgemeine Informationen mit, es erfolgte aber weder eine konkrete Beauskunftung mit den in Art. 15 Abs. 1 DSGVO vorgesehenen Informationen noch die Übersendung einer Datenkopie gemäß Art. 15 Abs. 3 DSGVO. Eine Mitteilung an den HmbBfDI hierüber erfolgte ebenfalls nicht. Der HmbBfDI wird das angedrohte Zwangsgeld nunmehr durchsetzen. Sollten die Auskunft und die Datenkopie dann nicht erteilt werden, kann der HmbBfDI erneut ein Zwangsgeld androhen und durchsetzen.

5. Ende des ZOOM-Verfahrens

Nach zwei Jahren, in denen das Verfahren beim Verwaltungsgericht Hamburg anhängig war, endete der Rechtsstreit nun ohne inhaltliche Entscheidung des Gerichts. Durch den in der Zwischenzeit erfolgten Angemessenheitsbeschluss der EU hatte sich die Rechtslage so verändert, dass eine Durchführung des Gerichtsverfahrens nicht mehr sinnvoll gewesen wäre.

Im 30. TB Datenschutz 2021 (Kap. 4.6) hatte der HmbBfDI darüber informiert, dass er eine Warnung gegenüber der Senatskanzlei der Freien und Hansestadt Hamburg (FHH) ausgesprochen hat. Hintergrund war der damals geplante Einsatz der Videokonferenzsoftware Zoom, der nach Ansicht des HmbBfDI nicht mit der DSGVO vereinbar war. Die Senatskanzlei hatte sodann Klage vor dem VG Hamburg gegen die Warnung erhoben.

Am 10.7.2023 hat die Europäische Kommission einen Angemessenheitsbeschluss („Adequacy decision for the EU-US Data Privacy Framework“) i.S.d. Art. 45 Abs. 1 DSGVO bekannt gegeben. Damit sind sichere transatlantische Datenströme möglich und die vom EuGH in seinem Urteil vom 16.7.2020 (Rs. C-311/18 – Facebook Irland u. Schrems) aufgestellten Bedenken zumindest einstweilen ausgeräumt. Die tragenden Gründe der Warnung vom 11.8.2021 für den Einsatz der Videokommunikationssoftware „Zoom“, welche mit Blick auf die Übermittlung von personenbezogenen Daten in einen Drittstaat ohne geeignete Garantien zum Schutz dieser Daten zuvor bestanden, waren dadurch nach Ansicht des HmbBfDI im Wesentlichen entfallen.

Dies hat auch die Senatskanzlei so gesehen. In der Folge haben sich beide Seiten darauf verständigt, dass eine Fortführung des Gerichtsverfahrens wegen der geänderten Rechts- und Sachlage nicht mehr zielführend ist. Im Besonderen bestand kein Interesse daran, gerichtlich feststellen zu lassen, ob die streitgegenständliche Warnung unter der alten Rechts- und Sachlage zutreffend war.

Der HmbBfDI hat daraufhin die streitgegenständliche Warnung vom 11. August 2021 zum Einsatz der Videokonferenzsoftware „Zoom“ mit Wirkung für die Zukunft zurückgenommen. Der Vergleich entfaltete keine Rückwirkung, weshalb gerichtlich ungeklärt bleibt, ob der Einsatz von ZOOM auch vor der Adäquanzentscheidung rechtmäßig gewesen wäre.

6. Einstellung Gerichtsverfahren in Sachen Videmo 360

Das Hamburgische Oberverwaltungsgericht (OVG Hamburg) hat das Gerichtsverfahren in Sachen Videmo 360 eingestellt. Eine Entscheidung erfolgte lediglich über die Kosten. Eine von beiden Seiten angestrebte gerichtliche Überprüfung der ursprünglichen Anordnung des HmbBfDI aus 2018 durch das OVG Hamburg ist somit leider nicht erfolgt.

Mit Beschluss vom 17. Mai 2023 hat das OVG Hamburg das Verfahren über den Einsatz einer Software zur automatisierten Gesichtserkennung durch die Polizei Hamburg eingestellt, nachdem die Beteiligten den Rechtsstreit übereinstimmend für erledigt erklärt haben. Das mit der Berufung vor dem OVG durch den HmbBfDI angefochtene Urteil des Verwaltungsgerichts Hamburg (VG Hamburg, Urteil v. 23.10.2019 – 17 K 203/19) – wonach die vom HmbBfDI erlassene Löschungsanordnung gegen die Behörde für Inneres und Sport aufgehoben wurde – ist damit wirkungslos. Das Gericht hatte lediglich über die Kosten zu entscheiden. Unter Berücksichtigung des bisherigen Sach- und Streitstandes nach billigem Ermessen hat das OVG Hamburg die Kosten der Behörde für Inneres und Sport auferlegt, da diese nach Ansicht des Gerichts bei der Durchführung des noch anhängigen Verfahrens voraussichtlich unterlegen wäre.

Hintergrund des Verfahrens war der Einsatz einer Software zur automatisierten Gesichtserkennung im Zusammenhang mit dem G20-Gipfel im Jahr 2017 in Hamburg. Für ihren Einsatz durch die Polizei Hamburg wurde eine sog. Template-Datenbank mit einem wachsenden Umfang von anfänglich 17 Terabyte angelegt, in die von Bürger:innen bei der Polizei hochgeladene private Aufnahmen, polizeieigenes Videoüberwachungsmaterial sowie Material aus öffentlichen Verkehrsmitteln und aus den Medien – insgesamt ca. 32.000 Video- und Bilddateien – eingeflossen sind. Der HmbBfDI war der Ansicht, dass für den Einsatz der Software keine hinreichende Rechtsgrundlage

bestand und hat daher gegenüber der Polizei die Löschung dieser Template-Datenbank, d.h. einer Datenbank, die sämtliche Gesichter des Videoüberwachungsmaterials in mathematische Modelle umgerechnet enthält, angeordnet. Die Behörde für Inneres und Sport als Aufsichtsbehörde der Polizei Hamburg und Adressat des Bescheides hatte hiergegen Klage erhoben und war damit vor dem VG Hamburg auch erfolgreich. Nach Beantragung der Zulassung der Berufung durch den HmbBfDI löschte die Polizei die Template-Datenbank. Dies geschah nach Angaben der Polizei aus Gründen der Erforderlichkeit, da die Ermittlungen im Zusammenhang mit den Ausschreitungen abgeschlossen waren. Im Folgenden ließ das OVG Hamburg jedoch die Berufung des HmbBfDI zu. Aufgrund der zwischenzeitlichen Löschung war der Rechtsstreit allerdings als erledigt zu erklären.

Die vom Kläger nunmehr begehrte Feststellungsklage – also ob die nunmehr erledigte Anordnung jedenfalls ursprünglich rechtswidrig gewesen war – war nach Ansicht des Gerichts aber unzulässig, da es sich bei der streitgegenständlichen Anordnung des HmbBfDI um eine Einzelfallentscheidung handelte und die für eine derartige Klage benötigte Wiederholungsgefahr für das Gericht nicht erkennbar war.

Aufgrund der Unzulässigkeit der Feststellungsklage legte das Gericht die Kosten der Behörde für Inneres und Sport auf. Eine Entscheidung in der Sache ist somit nicht getroffen worden. Die grundsätzlichen Fragestellungen, die dieser Fall für die Praxis der Ermittlungsbehörden, der datenschutzrechtlichen Aufsichtsbehörden und nicht zuletzt für den Schutz sehr vieler unbeteiligter Personen aufwirft, bleibt letztlich für die Zukunft offen. Viele Fragestellungen wären bei einem nächsten Einsatz erneut aufzuwerfen. Insbesondere aber bleiben Tausende Bürger:innen letztlich im Unklaren, ob die Verarbeitung ihrer biometrischen Daten zu Recht erfolgte oder nicht.

GRENZÜBERSCHREITENDE THEMEN V.

GRENZÜBERSCHREITENDE THEMEN

1. EU-US Data Privacy Framework

Der neue Angemessenheitsbeschluss der Europäischen Kommission für die USA beendet in vielen Fällen die durch die Schrems-II-Entscheidung ausgelöste Hängepartie – aber nur für dieses Empfängerland und nur für solche Stellen, die er betrifft. Drittstaatentransfers in die USA sind damit deutlich vereinfacht, jedoch sind weiterhin Anforderungen zu beachten.

Der Angemessenheitsbeschluss ist als europäischer Rechtsakt verbindlich. Der Unionsgesetzgeber hat damit festgelegt, dass die von seinem Anwendungsbereich erfassten Empfänger:innen in den USA ein angemessenes Datenschutzniveau aufweisen. Datenübermittlungen an diese Stellen sind dann in demselben Rahmen zulässig, wie dies innerhalb der EU der Fall wäre. Wichtig ist jedoch, dass nicht alle US-Unternehmen von dieser Vereinfachung profitieren, sondern nur solche, die sich selbst dem Data Privacy Framework unterworfen haben. Es handelt sich dabei um spezifische Datenschutzgarantien, die die betreffenden Stellen in den USA umzusetzen haben. Die Teilnahme am Framework ist beim US-Handelsministerium zu melden, die dies in ihrer Liste unter www.dataprivacyframework.gov öffentlich macht. Vor einer Datenübermittlung in die USA sollte daher überprüft werden, ob die Empfänger auf der Liste stehen.

Ist dies nicht der Fall, sind weiterhin die übrigen Übermittlungsinstrumente der Art. 46 ff. DSGVO, also insbesondere die Standardvertragsklauseln zu nutzen. In dem Fall ist weiterhin das in der Schrems-II-Entscheidung des Europäischen Gerichtshofs geforderte Transfer Impact Assessment durchzuführen. Es kann für Empfänger:innen in den USA jedoch vergleichsweise kurz gehalten werden. Bei der Erstellung sollte auf die Executive Order 14086 des US-Präsidenten verwiesen werden. Dieser Rechtsakt der Vereinigten Staaten enthält zahlreiche Begrenzungen der Geheimdienstaktivitä-

ten sowie Datenschutz- und Verfahrensrechte für EU-Bürger:innen. Der Inhalt der Executive Order hat die EU-Kommission maßgeblich dazu veranlasst, den Status des angemessenen Datenschutzniveaus zuzuerkennen. Da die darin enthaltenen Limitierungen und Garantien auch für solche Konstellationen gelten, in denen Datenempfänger:innen nicht am Privacy Framework teilnehmen, kann die rechtsverbindliche Einschätzung der Europäischen Kommission auch auf diese Fallgestaltungen ausgedehnt werden. Verfasser:innen eines Transfer Impact Assessments können sich daher den Einschätzungen der Kommission in ihrer Analyse der Überwachungsgesetze und -praxis anschließen. Zu den Detailfragen, in welchen Konstellationen der Angemessenheitsbeschluss gilt und was andernfalls zu tun ist, hat die Datenschutzkonferenz unter Mitwirkung des HmbBfDI ausführliche Anwendungshinweise vom 4.9.2023 ausgearbeitet.

Der Angemessenheitsbeschluss schafft dringend benötigte Rechtssicherheit für den Moment. Ob er auch als dauerhafte Übermittlungsgrundlage langfristig genutzt werden kann, ist nicht sicher. Letztlich wird der Europäische Gerichtshof entscheiden, ob die Verbesserungen im Vergleich zu den zuvor für ungültig erklärten Angemessenheitsbeschlüssen nun ausreichen. Entsprechende Klageverfahren sind zu erwarten. Der Europäische Datenschutzausschuss hat in seiner Bewertung 5/2023 ein differenziertes Bild aufgezeigt. Er hat zahlreiche kritische Punkte identifiziert, sich aber nicht gegen eine Annahme des Beschlusses durch die EU-Kommission ausgesprochen. Die zentralen Defizite sind einerseits das Festhalten am Instrument der Massenüberwachung (sogenannte bulk collection) und andererseits die fehlende Transparenz im Rechtschutzverfahren.

Trotz dieser verbesserungswürdigen Punkte ist das Data Privacy Framework ein Erfolg für den Datenschutz. Im Zuge der Verhandlungen haben die USA bisher nicht dagewesene Zugeständnisse gemacht und ihr nationales Sicherheitsrecht an europäische Grundrechtsmaßstäbe angepasst. Der Beschluss kann jedoch kein Freibrief sein. Ob und inwiefern tatsächlich Geheimdienstaktivitäten auf ein verhältnismäßiges Maß reduziert werden und wirksamer Rechtsschutz

gewährleistet ist, kann nur die Umsetzung in der Praxis zeigen. Es ist nun Aufgabe der Datenschutzbehörden und der Kommission, dabei sehr genau hinzuschauen, und Aufgabe der US-Administration, tiefgreifende Prüfungen auch zu ermöglichen. Diesen Aufgaben wird insbesondere im Rahmen des in der Angemessenheitsentscheidung vorgesehenen Reviews nachgekommen werden. Die Evaluation findet erstmals im Jahr 2024 statt. Sie ist richtigerweise früher angesetzt worden als bei vergleichbaren Beschlüssen zu anderen Ländern.

Solange der Angemessenheitsbeschluss nicht für ungültig erklärt oder zurückgezogen wird, gilt er. Die Aufsichtsbehörden sind an ihn gebunden. § 21 BDSG sieht dabei vor, dass Behörden, die einen solchen Beschluss für ungültig halten, alle Verfahren, in denen es auf diese Frage ankommt, aussetzen und einen Antrag auf gerichtliche Entscheidung stellen. Das Gerichtsverfahren würde erst- und letztinstanzlich vor dem Bundesverwaltungsgericht geführt und letztlich dazu dienen, eine möglichst schnelle Vorlage zum Europäischen Gerichtshof zu ermöglichen. Vor dem Hintergrund der oben skizzierten Analyse des Angemessenheitsbeschlusses hält der HmbBfDI ihn derzeit nicht für ungültig und beabsichtigt kein Verfahren nach § 21 BDSG. In aufsichtsbehördlichen Prüfungen wird der Angemessenheitsbeschluss daher als tragfähige Übermittlungsgrundlage eingestuft. Sollte das Review zeigen, dass die Umsetzung in den USA gegenüber der relativ positiven Papierlage defizitär ist, wird der HmbBfDI seine Haltung überprüfen.

Der Kommissionsbeschluss beeinflusst auch die vom HmbBfDI koordinierte länderübergreifende Prüfaktion der Taskforce Schrems II. Die überprüften Fallgruppen zielten bewusst auf eingebundene Dienstleister ab, die typischerweise ihren Sitz in den USA haben. Der Angemessenheitsbeschluss sowie die geänderte Sicherheitsrechtslage in den USA führen dazu, dass die überprüften Datentransfers nun überwiegend nicht mehr zu beanstanden sind. Soweit noch Verfahren, die die USA betreffen, offen sind, hat die Taskforce sich darauf verständigt, diese jetzt abzuschließen. Während Anordnungen auf Aussetzung der Datenübermittlung nicht mehr

möglich sind, können weiterhin Sanktionen verhängt werden. Diese betreffen dann den rechtswidrigen Zustand in der Phase zwischen Schrems-II-Entscheidung und Angemessenheitsbeschluss. Zur Bildung einer gemeinsamen Linie bei dieser Ermessensentscheidung hat die Taskforce Kriterien ausgearbeitet, in welchen Fallgruppen eine nachträgliche Sanktion besonders angezeigt ist und in welchen Konstellationen eher von einer Sanktion abgesehen werden sollte. Mit der Taskforce ist die Datenschutzkonferenz ihrer Aufgabe nachgekommen, die Vorgaben des EuGH über eine rein reaktive Beschwerdearbeit hinaus umzusetzen. Dabei konnten in zahlreichen Fällen Verbesserungen durchgesetzt werden, indem die angesprochenen Unternehmen Dienstleister oder Speicherorte gewechselt haben. Die Signalwirkung der Prüfaktion hat auch in anderen, nicht angeschriebenen Unternehmen Aktivitäten entfaltet. Auch wenn die betreffenden Datenübermittlungen mittlerweile infolge des Kommissionsbeschlusses wieder rechtmäßig wären, wurden die Unternehmen in die Lage versetzt, in ihrer IT-Architektur auf verlässliche, langfristig einsetzbare Dienste vertrauen zu können.

2. Zusammenarbeit mit Wettbewerbsbehörden

Im Bereich der sozialen Netzwerke und Plattform-Dienste sind sowohl die Datenschutzaufsichtsbehörden als auch die Wettbewerbsbehörden in ihrem jeweiligen Sachgebiet aufsichtsbehördlich tätig. Wo nötig, stehen sie in engem Austausch miteinander, um in ihrer Zuständigkeit rechtskonforme Entscheidungen zu treffen.

Datenschutzaufsichtsbehörden und Wettbewerbsbehörden haben entsprechend ihrer Rolle und Aufgabenzuweisung unterschiedliche Perspektiven und Zuständigkeiten (Wettbewerbs- und Kartellrecht einerseits, Datenschutzrecht andererseits). Dennoch kommt es regelmäßig vor, dass dieselben Verarbeitungszusammenhänge im Fokus beider Bereiche sind. Bei der Betrachtung, ob das Verhalten eines

Marktteilnehmers rechtlich zu beanstanden ist, hat das Bundeskartellamt (BKartA) in der jüngeren Vergangenheit auch datenschutzrechtliche Fragestellungen bewertet. So untersagte das BKartA mit seinem Beschluss vom Februar 2019 Meta Platforms Ireland, Daten ohne explizite Einwilligung der Nutzer:innen zwischen verschiedenen Diensten auszutauschen.

Bereits vor Erlass des Beschlusses hatte das BKartA Kontakt mit dem HmbBfDI aufgenommen und sich auf Fachebene bzgl. der datenschutzrechtlichen Fragen abgestimmt. Da Meta gegen die Entscheidung des BKartA Rechtsmittel eingelegt und das angerufene nationale Gericht einige Rechtsfragen zur Auslegung der DSGVO hatte, ist das Verfahren dem Europäischen Gerichtshof zur Vorabentscheidung vorgelegt worden.

Der EuGH entschied im Sinne des Kartellamts und untersagte dem Facebook-Betreiber Meta Platforms Ireland, personenbezogene Daten der Nutzer:innen bei Aktivitäten außerhalb des sozialen Netzwerks ohne Einwilligung zusammenzuführen (siehe hierzu https://datenschutz-hamburg.de/news/eugh-urteil-im-fall-meta-gegen-das- bundeskartellamt). Dies war bisher gängige Praxis des Meta-Konzerns, der nutzer- und gerätebezogene Daten innerhalb und außerhalb des sozialen Netzwerks den entsprechenden Facebook-Konten zuordnet.

Zum einen handelt es sich dabei um Daten über den Aufruf dritter Websites und Apps, die durch Programmierschnittstellen (beispielsweise die „Facebook Business Tools“) mit Facebook verbunden sind, zum anderen um Daten über die Nutzung anderer zum Meta-Konzern gehörender Online-Dienste wie Instagram, WhatsApp oder Oculus.

Meta stützte sich bei dieser Praxis – anstelle einer Einwilligung – auf die Allgemeinen Nutzungsbedingungen, denen Nutzer:innen pauschal zustimmen mussten, um den Registrierungsprozess bei Facebook abschließen zu können. Das Bundeskartellamt sah hierin eine missbräuchliche Ausnutzung der marktbeherrschenden Stellung von

Facebook und einen Verstoß gegen die Datenschutzgrundverordnung (DSGVO).

Der EuGH gibt in seinem Urteil weitreichende Antworten auf die vorgelegten Fragen. So klärt die Entscheidung u. a. das Verhältnis zwischen Datenschutzaufsichts- und Kartellbehörden.

Dazu wird ausgeführt, dass Datenschutzaufsichts- und Kartellbehörden an den Grundsatz der loyalen Zusammenarbeit gebunden sind, der sich unter anderem aus Art. 4 Abs. 3 EUV herleitet. Es soll damit sichergestellt werden, dass keine voneinander abweichenden Auslegungen der DSGVO durch unterschiedliche Behörden erfolgen.

Die Hauptaufgabe der Datenschutzaufsichtsbehörden besteht darin, die Anwendung der DSGVO zu überwachen und durchzusetzen und gleichzeitig zu ihrer einheitlichen Anwendung in der Union beizutragen. Beides mit dem Ziel, die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen und den freien Verkehr solcher Daten in der Union zu erleichtern.

Die nationalen Wettbewerbsbehörden dagegen sind unter anderem für den Erlass von Entscheidungen zuständig, mit denen der Missbrauch einer beherrschenden Stellung durch ein Unternehmen festgestellt wird, um den Wettbewerb innerhalb des Binnenmarkts vor Verfälschungen zu schützen. Eine nationale Wettbewerbsbehörde tritt durch die Feststellung eines Verstoßes gegen die DSGVO allerdings nicht an die Stelle der Datenschutzaufsichtsbehörden.

Die nationalen Wettbewerbsbehörden sind nach dem Urteil des EuGH vielmehr verpflichtet, sich abzustimmen und mit den betreffenden nationalen Aufsichtsbehörden beziehungsweise der federführenden Aufsichtsbehörde zusammenzuarbeiten. 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.

> *„Ist dies der Fall, darf die nationale Wettbewerbsbehörde davon nicht abweichen, wobei es ihr aber freisteht, daraus eigene Schlussfolgerungen unter dem Gesichtspunkt der Anwendung des Wettbewerbsrechts zu ziehen."* (EuGH, Rn. 56)

Im Zweifel muss die Wettbewerbsbehörde die zuständige Datenschutzaufsichtsbehörde konsultieren und „um deren Mitarbeit bitten, um ihre Zweifel auszuräumen oder zu klären, ob sie eine Entscheidung der betreffenden Aufsichtsbehörde abwarten muss, bevor sie mit ihrer eigenen Beurteilung beginnt." (EuGH, Rn. 57)

Der EuGH hat damit klargestellt, dass primär und vorrangig die Datenschutzaufsichtsbehörden für die Anwendung und Durchsetzung der DSGVO zuständig sind. Während immer mehr Berührungspunkte zwischen Marktregulierung und Datenschutz entstehen, gibt die vom EuGH benannte Pflicht der Wettbewerbsbehörden, sich vorab mit den zuständigen Datenschutzaufsichtsbehörden abzustimmen, Verantwortlichen und Marktteilnehmenden die nötige Rechtssicherheit.

Datenschutzaufsichtsbehörden und Wettbewerbsbehörden haben zugleich großes Interesse daran, koordiniert zu agieren und aufzutreten, um eine effektive Rechtsdurchsetzung im Binnenmarkt sicherzustellen. In Umsetzung des Urteils gilt es nun, die Zusammenarbeit weiter zu intensivieren und zu konkretisieren.

Auch der jüngst in Kraft getretene Digital Markets Act (DMA) regelt, dass sich die unterschiedlichen Regulierungsregime und -behörden enger verzahnen. Als ein Vertreter der europäischen Datenschutzbehörden ist der Hamburgische Datenschutzbeauftragte Mitglied der „Hochrangigen Gruppe" (High Level Group) nach Art. 40 des DMA, die die EU-Kommission bei der Umsetzung berät.

3. Beschwerdebearbeitung bei grenzüberschreitenden Fällen

„Warum muss sich Facebook nicht an deutsches Recht halten?“ – Diesen oder ähnliche Sätze hört der HmbBfDI in der täglichen Beratung und Beschwerdearbeit relativ häufig. Warum dieser Eindruck entstehen kann und warum dieser Eindruck letztlich falsch ist, soll hier kurz erläutert werden. Wenn zum Beispiel eine betroffene Person mit Wohnsitz in Hamburg der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten durch Facebook gegen die DSGVO verstößt – welche Aufsichtsbehörde wäre dann für diese Beschwerde zuständig?

Der Grund dafür, dass dieser Eindruck entstehen mag, ist der durch die DSGVO eingeführte sogenannte „One-Stop-Shop-Mechanismus“. Dieser sieht vor, dass bei grenzüberschreitenden Datenverarbeitungen für Unternehmen, die in der EU ansässig sind und in mehreren EU-Mitgliedstaaten Datenverarbeitung betreiben, ausschließlich die Aufsichtsbehörde an ihrem Hauptsitz zuständig ist. Dies ermöglicht es Unternehmen, einfacher als vor der Einführung der DSGVO ihre datenschutzrechtlichen Angelegenheiten zu klären, da diese nunmehr einen zentralen Hauptansprechpartner haben. Diejenige Aufsichtsbehörde, innerhalb deren Zuständigkeitsbereich ein Unternehmen die europäische Hauptniederlassung hat, bezeichnet die DSGVO als die „federführende Aufsichtsbehörde“.

Wann liegt überhaupt eine grenzüberschreitende Verarbeitung vor? Der Begriff „grenzüberschreitende Verarbeitung“ wird in Art. 4 Nr. 23 DSGVO legaldefiniert als entweder

- eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist,

oder
- eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Liegt also im eingangs skizzierten Fall eine grenzüberschreitende Verarbeitung im Sinne der DSGVO vor? Facebook nimmt die Verarbeitungen innerhalb der Niederlassung in Irland vor. Allerdings hat diese Tätigkeit erhebliche Auswirkungen auf betroffene Personen nicht nur in Irland, sondern auch zum Beispiel auf Betroffene in Deutschland, da auch hier der Dienst Facebook genutzt werden kann. Es handelt sich daher um eine grenzüberschreitende Verarbeitung und der One-Stop-Shop-Mechanismus kommt zur Anwendung,

Im Falle von Facebook wäre also die irische Danteschutzbehörde federführend, da sich die europäische Hauptniederlassung von Facebook in deren Zuständigkeitsbereich befindet. Diese fungiert jedoch nicht nur als Ansprechpartner für Facebook, sondern hat auch gegenüber Facebook die Einhaltung des Datenschutzrechts durchzusetzen.

Heißt das nun, dass sich Betroffene mit Wohnsitz zum Beispiel in Deutschland in Fällen grenzüberschreitender Verarbeitung ausschließlich bei der federführenden Aufsichtsbehörde beschweren dürfen, wenn sie der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt? Müsste dieses Verfahren dann auch in der Amtssprache der federführenden Aufsichtsbehörde geführt werden?

Nein, denn hier kommt die sogenannte „betroffene Aufsichtsbehörde“ ins Spiel. Als „betroffene Aufsichtsbehörden“ werden zum Beispiel Aufsichtsbehörden bezeichnet, bei denen Betroffene Beschwerde eingereicht haben oder in deren örtlicher Zuständigkeit Personen ihren Wohnsitz haben, auf die die Datenverarbeitung er-

hebliche Auswirkung haben kann (vgl. Art. 4 Nr. 22 DSGVO). Betroffene können sich daher stets bei ihrer örtlichen Datenschutzbehörde beschweren. Diese wendet sich dann im Namen der Betroffenen an die federführende Datenschutzbehörde und informiert die Betroffenen über Fortschritt und Ergebnis der Untersuchung durch die federführende Aufsichtsbehörde.

Die betroffene Aufsichtsbehörde hat darüber hinaus ein Mitspracherecht bei der Behandlung einer Angelegenheit durch die federführende Aufsichtsbehörde (sog. „Kooperationsverfahren", siehe Art. 60-61 DSGVO). Kann zwischen federführender und betroffener Aufsichtsbehörde im Verfahren der Zusammenarbeit kein Konsens erzielt werden, wird die Sache dem Europäischen Datenschutzausschuss (EDSA) zur Entscheidung vorgelegt. Der EDSA ist eine unabhängige Einrichtung auf europäischer Ebene, in welcher unter anderem die nationalen Datenschutzbehörden aller Mitgliedstaaten der EU vertreten sind. Der EDSA hat die Aufgabe, Streitigkeiten zwischen den Aufsichtsbehörden bei der Durchsetzung der DSGVO beizulegen und so eine einheitliche Anwendung und Durchsetzung des Datenschutzrechts im gesamten Europäischen Wirtschaftsraum sicherzustellen (sog. „Kohärenzverfahren", siehe Art. 63 – 67 DSGVO).

Der „One-Stop-Shop-Mechanismus" entlastet daher nicht nur die Unternehmen, auch Verbraucher werden so effektiver geschützt, da betroffene Personen sich stets mit ihren Beschwerden an ihre lokale Aufsichtsbehörde wenden können; unabhängig davon in welchem EU-Land ein verantwortliches Unternehmen seinen Sitz hat. So erleichtert die DSGVO betroffenen Personen die Ausübung ihrer Rechte in Bezug auf ihre personenbezogenen Daten.

4. Chatkontrolle

Im Juli 2022 haben sich EDSA und EDPS gemeinsam kritisch zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern geäußert. Auch wenn die Ziele des Gesetzgebers völlig unstreitig, richtig und wichtig sind, birgt die durch die Entwürfe vorgesehene Umsetzung erhebliche Risiken.

Die Entwürfe des Europäischen Parlaments und des Rates für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern lassen Gefahren für die Grundfreiheiten, insbesondere der Kommunikationsfreiheit sämtlicher Kommunikationsteilnehmer:innen, erkennen, denn die Eingriffe in den Kommunikationsvorgang erfolgen unabhängig davon, ob der Einzelne einen Anlass hierfür gegeben hat.

Dieses Vorhaben wird daher von den Datenschutzaufsichtsbehörden kritisch begleitet. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich in einer Pressemitteilung zum Gesetzesvorhaben positioniert (https://www.datenschutzkonferenz-online.de/media/pm/23_10_17_DSK_Pressemitteilung_Chatkontrolle.pdf) und damit die Stellungnahme von EDSA und EDPS (https://edpb.europa.eu/system/files/2023-02/edpb_edps_jointopinion_202204_csam_de.pdf) ergänzt.

Das Gesetzesvorhaben zielt darauf ab, eine umfassende Überwachung von Kommunikationsinhalten zu ermöglichen. Da sich bei elektronischer Kommunikation eine Ende-zu-Ende-Verschlüsselung etabliert hat, wäre eine derartige Überwachung nur unter Umgehung von Verschlüsselungstechnologien möglich. Gleichzeitig würde eine solche Regelung in den Kernbereich der Kommunikationsfreiheit eingreifen.

Die Initiative des Gesetzgebers geht auf das Inkrafttreten des European Electronic Communication Codex (EECC) zurück. Diese Richtlinie löste alte Rahmenrichtlinien ab und brachte vor allem eine Erweiterung des Fernmelde- bzw. Kommunikationsgeheimnisses auf solche Dienste mit sich, die zuvor nicht als Telekommunikationsdienste angesehen werden konnten. Mit dem EECC hielt eine funktionsäquivalente Betrachtung Einzug in die rechtliche Bewertung elektronischer Kommunikationsdienste. Was wie ein Telekommunikationsdienst genutzt wird, soll nun auch als solcher angesehen werden und benötigt daher denselben Schutz, der bisher nur klassischen Telekommunikationsdiensten zukam. Dieser besteht darin, dass die Inhalte und näheren Umstände der elektronischen Kommunikation grundrechtlichen Schutz genießen und nicht zu anderen Zwecken als zur Übermittlung der Nachricht verarbeitet werden dürfen.

Da Anbieter solcher Dienste schon vor Inkrafttreten des EECC auf freiwilliger Basis die Kommunikationsinhalte ihrer Dienste zum Zwecke der Missbrauchserkennung überwacht hatten, sah sich der europäische Gesetzgeber veranlasst, Ausnahmen von der Kommunikationsfreiheit für diese Fälle über eine gesetzliche Regelung zu treffen. Eine datenschutzrechtliche Rechtsgrundlage konnte der europäische Gesetzgeber jedoch nicht schaffen, sondern verwies auf die allgemeinen und abschließenden Regelungstatbestände der DSGVO. Nach Auffassung der deutschen Aufsichtsbehörden lässt sich der DSGVO für die Ausnahmen von der Kommunikationsfreiheit keine Rechtsgrundlage entnehmen, die eine solche „Chatkontrolle“ ermöglichen würde.

Im europäischen Kontext wird dies nicht ausnahmslos so gesehen. Ein Konsens unter den europäischen Aufsichtsbehörden konnte daher in dieser Frage bisher nicht erzielt werden.

5. Prüfung von ChatGPT

Im Frühjahr 2023 hat Open AI mit der Veröffentlichung des textbasierten Dialogsystems ChatGPT auf Grundlage eines sogenannten großen Sprachmodells (Large Language Model, LLM), weltweit große mediale Aufmerksamkeit auf sich gezogen. Es hat auch erneut die Datenschutzbehörden mit dem Thema Künstliche Intelligenz konfrontiert.

Weil Open AI, ein zu diesem Zeitpunkt ausschließlich in den USA ansässiges Unternehmen, keine Niederlassung in der EU hatte und auch bis zum Redaktionsschluss nicht etabliert hat, griff der sogenannte One-Stop-Shop-Mechanismus nicht, wonach die Behörde des Mitgliedstaates federführend zuständig ist, in dem das Unternehmen seine Niederlassung bzw. Hauptniederlassung in der EU hat. Vielmehr sind dann diejenigen Behörden zuständig, in deren Gebiet Betroffene leben – im Fall von ChatGPT damit alle Aufsichtsbehörden in Europa.

In Abstimmung mit mehreren deutschen Datenschutzaufsichtsbehörden der Länder hat der HmbBfDI ein Verfahren gegen Open AI eröffnet, in dem er die Vereinbarkeit mit der DSGVO prüft. Darüber hinaus koordinieren sich die deutschen und europäischen Datenschutzaufsichtsbehörden, die ebenfalls Verfahren gegen Open AI eingeleitet haben im Rahmen einer europäischen Taskforce. Dabei geht es zunächst darum, das Verarbeitungsmodell von ChatGPT bzw. der dahinterstehenden LLM zu verstehen. Welche personenbezogenen Daten sind in diese Modelle eingeflossen? Welche Antworten können bei einem Dialog mit ChatGPT einen Personenbezug haben? Welche Vorkehrungen hat OpenAI getroffen, um Betroffene zu schützen?

Bisher gibt es zum Aufbau eines Sprachmodells, wie es bspw. Open AI anbietet, noch keine verbindlichen KI-spezifischen europäischen Vorgaben. Sie werden jedoch mit Inkrafttreten der KI-Verordnung

wirksam. Zum Redaktionsschluss dieses Tätigkeitsberichtes befand sich die KI-Verordnung in der Schlussphase des Gesetzgebungsprozesses. Unabhängig von solchen KI-spezifischen Vorgaben finden die Regelungen der DSGVO Anwendung. Sofern personenbezogen Daten in KI-Modellen verarbeitet werden, bedarf es einer Rechtsgrundlage nach Art. 6 DSGVO. Als Legitimation für die Verarbeitung kommt – schon aus tatsächlichen Gründen – lediglich die Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 Buchst. f DSGVO) in Betracht. Dies setzt voraus, dass seitens Open AI ein berechtigtes Interesse gegeben ist und die Rechte und Freiheiten der betroffenen Personen dieses Interesse nicht überwiegen.

Als berechtigtes Interesse gilt zunächst jedes vom Gesetz nicht verbotene Interesse, so dass von einem berechtigten Interesse bei Open AI grundsätzlich ausgegangen werden kann. Sodann ist im Rahmen einer Güterabwägung zu untersuchen, ob nicht die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen überwiegen. Für diese Abwägung ist entscheidend, welche Maßnahmen seitens Open AI ergriffen wurden, um den Rechten und Freiheiten der betroffenen Personen hinreichend Rechnung tragen zu können.

Daher hat der HmbBfDI, abgestimmt mit den anderen beteiligten Datenschutzaufsichtsbehörden wiederholt Fragen an Open AI gerichtet, um letztlich eine Bewertung der Rechtsgrundlage vornehmen zu können. Die Fragen betreffen u. a. die Art und Weise der Trainingsdatenerhebung und die technischen und organisatorischen Maßnahmen, insbesondere im Rahmen der Verarbeitung personenbezogener Daten besonderer Kategorien (Art. 9 DSGVO). Weiterhin wird nach Prozessen des Nachtrainings, den eingesetzten Filtermechanismen, der Verarbeitung von Nutzungsdaten bei Nutzung des Chatbots und den ergriffenen Maßnahmen gefragt, um die Betroffenenrechte nach Art. 12 ff. DSGVO sicherzustellen. Daneben stellen sich im Zusammenhang mit KI-Modellen Grundsatzfragen hinsichtlich des Personenbezugs von Modellen oder den generierten Texten.

Es ist absehbar, dass Open AI eine Niederlassung in einem europäischen Mitgliedstaat errichten wird. Der HmbBfDI bleibt dann als betroffene Behörde in die Verfahren eingebunden und wird Aufsichtsverfahren weiterhin entsprechend begleiten.

6. Verfahren vor dem EDSA in Sachen Meta

Der HmbBfDI hat gemeinsam mit anderen europäischen Aufsichtsbehörden vor dem Europäischen Datenschutzausschuss (EDSA) eine Reihe von Verfahren gegen Meta Platforms Ireland Limited (Meta) geführt. Dabei ging es vorwiegend um die Frage der gültigen Rechtsgrundlage für verhaltensbasierte Werbung. Trotz Klärung dieser Frage durch den EDSA stellt die Einführung eines Abo-Modells bei Facebook und Instagram die Datenschützer vor neue Herausforderungen.

Meta hatte sich bei Datenverarbeitungen zu Zwecken der personalisierten Inhalte oder Werbung lange Zeit auf die allgemeinen Nutzungsbedingungen gestützt, denen Nutzer:innen pauschal zustimmen mussten, um den Registrierungsprozess bei Facebook abzuschließen. Diese Praxis hat der EDSA mit seinen verbindlichen Beschlüssen im Dezember 2022 bezogen auf Facebook und Instagram unterbunden und klargestellt, dass Verarbeitungsvorgänge zu Zwecken verhaltensbasierter Werbung nicht auf die Rechtsgrundlagen Vertrag oder berechtigte Interessen gestützt werden dürfen. Der HmbBfDI hatte dazu im Vorweg die Einsprüche gegen die Beschlussentwürfe der irischen Aufsichtsbehörde, der Irish Data Protection Commission (IDPC), koordiniert und eingelegt sowie das Verfahren beim EDSA begleitet. Die verbindlichen Beschlüsse des EDSA wurden anschließend von der IDPC in endgültige Beschlüsse übernommen und Meta eine dreimonatige Umsetzungsfrist zur Anpassung an die DSGVO gewährt.

Bei der Umsetzung der Beschlüsse hatte sich Meta jedoch nicht sofort auf die Einwilligung gem. Art. 6 Absatz 1 lit. a DSGVO als einzig verbliebene Rechtsgrundlage für verhaltensbasierte Werbung stützen wollen. Im Rahmen eines informellen Austausches zwischen der IDPC und den betroffenen Aufsichtsbehörden in Europa hatte auch der HmbBfDI mehrfach Bedenken angemeldet und schriftliche Stellungnahmen zu Metas Umsetzungsplänen abgegeben, die jedoch auch nach Ablauf der Umsetzungsfrist nicht zu einer Einwilligungslösung bei Facebook und Instagram geführt haben.

Das führte schließlich dazu, dass die norwegische Aufsichtsbehörde im Juli 2023 zunächst eine Anordnung im Wege eines Dringlichkeitsverfahrens gemäß Art. 66 Absatz 1 DSGVO für Norwegen erließ und nach Ablauf der Anordnungsfrist von drei Monaten schließlich den EDSA um einen verbindlichen Beschluss ersuchte. Dieser beschloss im Oktober 2023 erneut, es Meta wegen anhaltender Verstöße zu verbieten, persönliche Daten ohne Einwilligung der Betroffenen für Werbezwecke zu verarbeiten. Auch dieses Verfahren beim EDSA begleitete der HmbBfDI in enger Abstimmung mit den Ländervertretungen sowie dem BfDI und gab Voten zu Abstimmungen im Plenum ab.

Parallel dazu hatte der Europäische Gerichtshof (EuGH) am 04. Juli 2023 (Az. C 252/219) Meta untersagt, personenbezogene Daten der Nutzer:innen bei Aktivitäten außerhalb des sozialen Netzwerks Facebook ohne Einwilligung zusammenzuführen. Im Rahmen eines Vorlageverfahrens hatte das Gericht obiter dictum die Möglichkeit eröffnet, dass auch große Anbieter von Social-Media-Diensten eine Bezahlvariante bzw. ein Abo-Modell alternativ zur Einwilligung anbieten können. Dabei erklärte der EuGH, dass diese Alternative gleichwertig zum einwilligungsbasierten Dienst sein muss und nur zu einem angemessenen Preis angeboten werden darf. Er hat jedoch nicht weiter erläutert, unter welchen Voraussetzungen dies im Einzelnen als rechtmäßig zu betrachten wäre.

Meta führte schließlich im November 2023 das Abo-Modell für ihre beiden sozialen Netzwerke Facebook und Instagram ein. Der HmbBfDI prüft nun aufgrund zahlreicher Beschwerden als betroffene Behörde, ob aus seiner Sicht bei der Einführung des Abonnements für werbefreie Nutzung die Voraussetzungen für eine wirksame Einwilligung nach Artikeln 4 (11), 7 DSGVO in die Verarbeitung eingehalten wurden. Hierbei stellt sich u.a. die Frage, unter welchen Umständen das Unternehmen Meta, das Online-Dienste auf sehr großen Online-Plattformen im Sinne des Gesetzes über digitale Dienste (DSA) anbietet, für die Verarbeitung rechtmäßig eine gültige und freiwillig erteilte Einwilligung einholen kann. Bei seiner Prüfung steht der HmbBfDI im engen Austausch mit der federführend zuständigen IDPC, aber auch mit dem Bundeskartellamt, dessen Verfahren gegen Meta nach dem vorgenannten Urteil des EuGH noch andauert.

Darüber hinaus hat der HmbBfDI im Januar 2024 gemeinsam mit den Datenschutzbehörden Norwegens und der Niederlande den EDSA um eine Klärung der Vereinbarkeit von Abo-Modellen bei sehr großen sozialen Netzwerken mit der DSGVO ersucht. Die deutschen Aufsichtsbehörden hatten sich bereits im März 2023 zu Abo-Modellen geäußert und die Rahmenbedingungen für deren Zulässigkeit formuliert. Eine gemeinsame europäische Positionierung gerade mit Blick auf europa- bzw. weltweit agierende Plattformen gibt es bis dahin aber nicht. Das Stellungnahmeverfahren beim EDSA gemäß Art. 64 Absatz 2 DSGVO ist ein stark formalisiertes Verfahren, das spätestens innerhalb von 14 Wochen abgeschlossen sein muss. Ziel des Ersuchens ist es, entsprechenden Anbietern auf dem europäischen Markt mehr Orientierung zu geben, unter den Aufsichtsbehörden gemeinsame Standards zu etablieren und berechtigte und drängende Fragen der Nutzenden beantworten zu können.

BERATUNGEN ÖFFENTLICHER STELLEN VI.

BERATUNGEN ÖFFENTLICHER STELLEN

1. Hamburgisches Krebsregister

Im Dezember 2023 wurde das Hamburgische Krebsregistergesetz reformiert. Damit ist der Gesetzgeber Anforderungen des Verwaltungsgerichts Hamburg nachgekommen, spezifische technische und organisatorische Maßnahmen zur Wahrung der Rechte und Freiheiten betroffener Personen gesetzlich festzulegen.

Das Krebsregistergesetz sieht nun eine engere Einbindung des HmbBfDI bei der Datenfreigabe an Forschungseinrichtungen vor. Neben der bislang schon enthaltenen Beteiligung vor der Freigabe nichtpseudonymer Daten ist jetzt auch vor der Entscheidung über Forschung mit pseudonymen Einzeldaten der HmbBfDI anzuhören. Zudem ist der HmbBfDI nach der Gesetzesänderung auch bei der Erstellung und Weiterentwicklung des Datenschutzkonzeptes zwingend zu beteiligen.

Zur verbindlichen Schaffung solcher organisatorischen und technischen Schutzmaßnahmen hatte das Verwaltungsgericht Hamburg den Gesetzgeber zuvor angehalten (Urt. v. 28.7.2022, Az. 21 K 1802/21). Wie im letzten Tätigkeitsbericht des HmbBfDI dargestellt (vgl. 31. TB Datenschutz 2022, Kap. VI 3) hatte das Verwaltungsgericht in seiner Entscheidung nicht moniert, wie die entsprechenden Maßnahmen, z.B. die interne Abgrenzung des Vertrauensbereichs (für die Erfassung und Verarbeitung der personenidentifizierenden Klartextdaten) zum Registerbereich, praktisch vom Hamburgischen Krebsregister (HKR) umgesetzt werden, sondern dass diese nicht konkret im Gesetz aufgezählt sind. Dem ist nun abgeholfen.

Zu der Frage, wie diese Beteiligung zukünftig aussehen wird, hat im Dezember 2023 ein Treffen von HmbBfDI und HKR stattgefunden. Themen waren neben der Art und Weise der Beteiligung des HmbBfDI mit Blick auf das Datenschutzkonzept auch seine Einbindung bei der

Überarbeitung des Informationsmaterials des HKR, das Patient:innen bei einer Erstmeldung schriftlich zur Verfügung zu stellen ist und mit dem diese unter anderem über ihr Widerspruchsrecht zu unterrichten sind. Auch über Anträge zum Beispiel von Hochschulen oder wissenschaftlichen Instituten auf Übermittlung von Daten aus dem HKR wurde gesprochen, zu denen der HmbBfDI dann anzuhören ist, wenn diese personenbezogen oder personenbeziehbar sind.

Was solche Datenübermittlungen betrifft, so ist festzustellen, dass die Datenschutz-Grundverordnung (DSGVO) in Erwägungsgrund 157 die Krebsforschung auf der Basis von Registerdaten ausdrücklich erwähnt und davon ausgeht, dass durch die Verwendung von Registerdaten bessere Forschungsergebnisse erzielt werden können, da sie auf einen größeren Bevölkerungsanteil gestützt sind. Zur Erleichterung der wissenschaftlichen Forschung, so heißt es im 157. Erwägungsgrund, können daher auch personenbezogene Daten verarbeitet werden, wobei sie angemessenen Bedingungen und Garantien unterliegen, die im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt sind. Auch die Anhörung des HmbBfDI stellt eine solche Bedingung dar. Seiner Aufgabe als Datenschutzaufsichtsbehörde wird der HmbBfDI insoweit weiterhin nachkommen und entlang der (neu) im HmbKrebsRG geregelten Voraussetzungen für Datenübermittlungen prüfen, ob diesen aus datenschutzrechtlicher Sicht Bedenken entgegenstehen.

2. Sozialrabatt auf Zeitkarten des hvv

Die Sozialbehörde bietet in Zusammenarbeit mit dem Hamburger Verkehrsverbund (hvv) die Möglichkeit an, Zeitkarten für die Nutzung des hvv zu einem um einen Sozialrabatt reduzierten Preis zu erwerben. Diesen Sozialrabatt leistet die Sozialbehörde als zusätzliche freiwillige Leistung, sofern in Hamburg gemeldete Bürger:innen existenzsichernde Leistungen nach SGB II, SGB XII oder Asylbewerberleistungsgesetz von einem Hamburger Leistungsträger beziehen. Eine bereits vor längerer Zeit vorgenommene Umstellung des Antragsverfahrens bringt datenschutzrechtliche Besonderheiten mit sich, zu denen eine Abstimmung mit dem HmbBfDI läuft.

Während leistungsberechtigte Personen, die den Sozialrabatt in Anspruch nehmen wollten, früher bei den leistungsgewährenden Stellen eine Sozialkarte beantragen und diese bei Fahrscheinkontrollen vorzeigen mussten, hat die Sozialbehörde durch die Umstellung eine Vereinfachung angestrebt. Diese soll dadurch erreicht werden, dass Empfänger:innen von Sozialhilfe, Grundsicherungen oder Leistungen nach dem Asylbewerberleistungsgesetz die vergünstigten Zeitkarten mit einem Antragsformular und einem Identitätsnachweis direkt in den Servicestellen des hvv bestellen können.

Die Ausgestaltung des Antragsformulars erweist sich dabei – aus datenschutzrechtlicher Sicht – als komplex. Denn die Daten der antragstellenden Personen werden von im hvv organisierten Verkehrsunternehmen als Vertragspartner der antragstellenden Person erhoben und an die Sozialbehörde, als die den Rabatt leistende Fachbehörde, weitergeleitet. Diese soll dann die Möglichkeit haben, die Antragsberechtigung mittels Abgleichs mit den leistungsgewährenden Stellen zu prüfen.

Die meisten Datenverarbeitungsvorgänge in dieser Konstellation lassen sich auf Rechtsgrundlagen stützen, sei es, dass die Verarbei-

tung zu Vertragszwecken oder zur Erfüllung von in der Zuständigkeit einer öffentlichen Stelle liegenden Aufgaben erforderlich ist. Für den zuletzt genannten Datenabgleich zwischen Sozialbehörde und den leistungsgewährenden Stellen (Jobcenter sowie Fachämter für Grundsicherung und Soziales der Bezirksämter) bedarf es allerdings einer Einwilligung der Person, die den Sozialrabatt beantragt. Zur konkreten Ausgestaltung – unter Berücksichtigung der Vorgaben der Datenschutz-Grundverordnung (DSGVO) zur Einwilligung – stand der HmbBfDI im Jahr 2023 im Austausch mit der Sozialbehörde und den weiteren Beteiligten. Der Beratungs- und Abstimmungsprozess wird im Jahr 2024 fortgeführt werden.

3. Sickereffektstudie der Behörde für Stadtentwicklung und Wohnen

Zur bedarfsgerechten Wohnungsbauplanung hat der Senat eine Studie in Auftrag gegeben. Die neuartige Methode zur Auswertung des Melderegisters bedarf guter Rechtsgrundlagen und technischer Sicherungen zum Schutz der Betroffenen.

Ziel der großangelegten Studie ist es, herauszufinden, welche Art von Wohnungsneubau am effektivsten ist, um den angespannten Wohnungsmarkt in Hamburg in Zeiten zunehmender Flächenknappheit und einer stetig wachsenden Bevölkerung nachhaltig zu entlasten und bezahlbaren Wohnraum für alle Einkommensgruppen zur Verfügung stellen zu können. Für die Planung der statistischen Erhebung zu sogenannten Sickereffekten beim Wohnungsneubau hatte die Behörde für Stadtentwicklung und Wohnen (BSW) dem HmbBfDI im Rahmen der gesetzlich vorgeschriebenen Beteiligungspflicht nach § 5 Abs. 2 Hamburgisches Statistikgesetz (HmbStatG) einen ersten Konzeptentwurf für eine „Studie zu umzugsketteninduzierten Versorgungseffekten des Wohnungsneubaus in Hamburg“ (Sickereffektstudie) zur Stellungnahme übersandt. Die Studie wird durch die BSW unter Einschaltung eines

Auftragsverarbeiters durchgeführt werden. Den Zuschlag erhielt die empirica AG.

Der von der BSW und empirica vorgelegte Konzeptentwurf fußt auf einer neuen wissenschaftlichen Methodik zur Untersuchung von Sickereffekten auf dem Wohnungsmarkt. Die Datenerhebung für die Studie soll nicht aufsetzend auf einer einfachen Stichprobenziehung aus dem Melderegister und rein befragungsbasiert erfolgen. Vielmehr sollen umfangreiche Auswertungen des Melderegisters das Auffinden sogenannter Umzugs- bzw. Sickerketten ermöglichen.

Da hinsichtlich des vorgelegten Konzeptentwurfs eine Vielzahl offener Fragen und datenschutzrechtliche Bedenken bestanden, machte der HmbBfDI in seiner Stellungnahme und weiteren Gesprächen deutlich, dass das Konzept grundlegend überarbeitet werden müsste und weitere Datenschutzunterlagen zu erstellen sind. Zugleich wurden der BSW Lösungsansätze und Maßnahmen für eine datenschutzrechtlich zulässige Umsetzung des Projektes aufgezeigt.

Die BSW betonte gegenüber dem HmbBfDI, welche enorme Bedeutung die Studie vor dem Hintergrund der globalen und europäischen Krisen der letzten Jahre, insbesondere dem Russland-Ukraine-Krieg und der extremen Wohnungsknappheit in Hamburg habe. Sie teilte mit, dass sie die erteilten Hinweise aufnehmen werde, die Lösungsansätze bezüglich deren Umsetzbarkeit prüfen wolle und an einer weiteren Beratung durch den HmbBfDI großes Interesse habe.

Im weiteren Beratungsprozess wurden in Stellungnahmen und Gesprächen die rechtlichen Rahmenbedingungen, mögliche Lösungsansätze und zu treffende Datenschutzmaßnahmen ausgiebig erörtert und das Studienkonzept seitens der BSW mehrfach überarbeitet. Problemfelder aus datenschutzrechtlicher Sicht waren bzw. sind folgende Bereiche:

- die Beachtung der rechtlichen Vorgaben des Bundesmeldegesetzes (BMG)

- Schaffung und Ausgestaltung einer landesrechtlichen Rechtsgrundlage für die Datenverarbeitung der BSW in Form einer Rechtsverordnung nach § 2 Abs. 3 HmbStatG
- zu schaffende landesrechtliche Rechtsgrundlage für die Datenverarbeitung in Form der Auswertung des Melderegisters und Übermittlung anonymisierter Daten durch die Meldebehörde im Hamburgischen Ausführungsgesetz zum Bundesmeldegesetz (HmbAGBMG)
- die Notwendigkeit unterschiedlicher Datenbasen für die Datensätze zur Befragung und Kettenauswertung sowie die Trennung der Datensätze
- die Gestaltung zuverlässiger Anonymisierungs- und Pseudonymisierungsprozesse

Die BSW hat bereits einen ersten Verordnungsentwurf erstellt, zu welchem der HmbBfDI im Rahmen des Beratungsprozesses Stellung genommen hat. Hinsichtlich der zu schaffenden Rechtsgrundlage bezüglich der Datenverarbeitungen durch die Meldebehörde im HmbAGBMG hat ein Gespräch zwischen BSW, HmbBfDI und der für das Meldewesen zuständigen Behörde für Inneres und Sport (BIS) stattgefunden, in welchem die BIS angekündigt hat, im Rahmen der ohnehin anstehenden Neufassung des HmbAGBMG eine solche Rechtsgrundlage schaffen zu wollen.

Zudem wurden verschiedene technische Maßnahmen zum Schutz der personenbezogenen Daten erörtert, wie beispielsweise die Anonymisierung der aus dem Melderegister selektierten Datensätze, eine Pseudonymisierung der Kettenanfänge sowie die Nutzung relativer (Umzugs-)Daten zum Kettenanfang. Diese Maßnahmen hat die BSW aufgegriffen, konkretisierende Unterlagen zu einer vorgesehenen Umsetzung (wie z.B. die Algorithmenbeschreibung der Anonymisierungsprozesse im Pseudocode) wurden angefordert, liegen aber bislang noch nicht vor.

Der HmbBfDI wird die Umsetzung des Projektes weiter beratend begleiten.

4. Digitalisierung der behördlichen Posteingangsbearbeitung

Im Rahmen der Digitalisierung der Verwaltung soll auch die Posteingangsbearbeitung digitalisiert und zentralisiert werden. Schreiben, die auf unterschiedlichen Wegen eine Behörde erreichen (Post, E-Mail oder Onlineformulare), sollen einheitlich verarbeitet werden. Der HmbBfDI begleitet beratend die Entwicklung entsprechender Projekte in der öffentlichen Verwaltung. Das Zeitalter von rein analogen Postfächern neigt sich dem Ende zu.

Die Posteingangsbearbeitung ist eine Kernaufgabe nahezu jeder öffentlichen Stelle. Die Kommunikation mit Bürger:innen ist wesentlich für viele Behörden. Sekretariate sind dabei die Schnittstelle und müssen die unterschiedlichen Eingangskanäle, meistens Briefpost und E-Mail-Funktionspostfächer, überwachen und Kommunikation weiterleiten. Diese Weiterleitung soll möglichst reibungslos, zügig und präzise stattfinden. Zu beachten sind stets die innerbehördlichen Zuständigkeiten, Sensibilität der Kommunikationsinhalte und Dringlichkeit. Die Digitalisierung dieser Aufgaben hat nicht nur das Potential, die Arbeitslast zu vereinfachen und zu verschlanken, sondern ist notwendiger Bestandteil einer vollständigen Digitalisierung aller Verwaltungsverfahren – ein Projekt, welches durch das Onlinezugangsgesetz derzeit vorangetrieben wird.

Der HmbBfDI hatte bereits im Jahr 2022 ein städtisches Projekt begleitet, welches die Posteingangsbearbeitung in Behörden digitalisieren sollte. Aus datenschutzrechtlicher Sicht positiv bewertet wurde, dass hier ein System geschaffen wurde, welches eine eigenständige Postfachstruktur enthielt und damit unabhängig von E-Mailpostfächern funktionierte. Im Rahmen dessen war direkt mitbedacht, dass Posteingänge mit kategorischen Löschfristen versehen wurden und die Software die Löschung nach bestimmter Zeit eigenständig übernimmt. Gleichzeitig wurde sichergestellt, dass ein einzelner Postein-

gang stets nur in einem Postfach auftaucht, d.h. bei Weiterleitung an die zuständige Stelle aus dem Postfach des Sekretariats o.ä. entfernt wird. So müssen die Verteilstellen nicht eigenständig darauf achten, Überbleibsel einer Nachricht zu löschen – ob aus Datenschutzgesichtspunkten oder wegen Speicherkapazitäten. Automatisierte Löschfristen sind hierfür eine deutliche Arbeitserleichterung. Derart simple Designentscheidungen werten ein Postbearbeitungssystem damit im Gegensatz zur klassischen E-Mail deutlich auf und erfüllen aus Sicht des HmbBfDI auch den Maßstab „privacy by design". E-Mail als Konzept, wie auch gängige E-Mailclients, sind nicht mit diesen Hintergedanken entworfen. Dies ist nicht verwunderlich, da E-Mails eigentlich nicht hausinterne Verteilungssysteme ersetzen sollten, sondern Briefe, Telegramme oder Faxe. Bei dieser Art von Kommunikation zwischen fremden Stellen ist es eher von Vorteil, dass Nachrichten zur eigenen Archivierung in Postausgängen verbleiben. In der hausinternen Postverteilung ist dies eher störend, wenn bspw. große E-Mailanhänge in jedes Postfach kopiert werden und händisch gelöscht werden müssen.

Als Rechtsgrundlage für derartige Postbearbeitungssysteme kommt § 4 HmbDSG in Betracht, da die Postbearbeitung selbstverständlich zur ureigenen Aufgabe einer jeden Behörde gehört. Als zusätzliches Problem war aber in dem damaligen Projekt der Einsatz eines KI-Moduls zu bewerten. Dieses sollte durch Auswertung des Nachrichteninhalts in der Lage sein, Vorschläge zu unterbreiten, welche hausinterne Organisationseinheit eine Nachricht am besten erhalten sollte – ein weiteres Werkzeug der Arbeitserleichterung. Art. 22 DSGVO spielte dabei keine einschränkende Rolle, da das Modul selbst keine Weiterleitungen vornimmt, sondern lediglich einen Vorschlag abgibt. Da weiterhin die menschliche Entscheidung den eigentlichen Vorgang auslöst, kann bereits nicht von einer automatisierten Entscheidung gesprochen werden. Der HmbBfDI kam überdies zu dem Ergebnis, dass der Plan, aus dem denkbaren Themenbereich der künstlichen Intelligenz und dem Einsatzfeld in der Verwaltung, einen sehr niedrigschwelligen Einsatz einer KI darstellt. Eingriffe in Grundrechte sind nicht zu erwarten, Gefährdungen von Menschen oder Daten

kaum vorstellbar. Eine tiefgreifende Kritik musste der HmbBfDI damit nicht formulieren. Einzig problematisch war die Trainingsphase des KI-Moduls. Da die öffentliche Verwaltung nicht auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO als Rechtsgrundlage zurückgreifen kann (s. Art. 6 Abs. 1 S. 2 DSGVO), steht keine allgemeine Rechtsgrundlage für eine Datenverarbeitung zur Verfügung. Öffentliche verantwortliche Stellen sind grundsätzlich darauf angewiesen, gesetzliche Rechtsgrundlagen vom Gesetzgeber zur Verfügung gestellt zu bekommen. Diese Gesetzeslücke hat der HmbBfDI im Verfahren angemerkt und darauf verwiesen, dass vorerst mit synthetischen Daten zum Training gearbeitet werden sollte.

In einem aktuellen Projekt begleitet der HmbBfDI nun die Einführung einer zentralen Digitalisierungsstelle, welche Posteingänge entgegennimmt und einscannt, um diese im Anschluss in einem elektronischen Postfach abzulegen. Die Zentralisierung dieser Aufgabe ist zwar begrüßenswert, da diese nicht nur rein praktisch schlankere und schnellere Abläufe erschafft und dadurch Arbeitskraft befreit wird. Gerade bei Poststücken mit sensiblen Daten mit erhöhtem Schutzbedarf entstehen aber aus der behördenübergreifenden Bearbeitung neue datenschutzrechtliche Fragen, aus denen erhöhte Schutzbedarfsanforderungen resultieren können. Aus datenschutzrechtlicher Sicht ist die Etablierung eines einheitlichen Verfahrens mit gemeinsamen Standards für die gesamte Verwaltung, die auch besonderen Schutzbedarfen Rechnung tragen, begrüßenswert. Statt ggf. abweichender Einzellösungen wird so ein Grundstein gelegt, eine datenschutzgerechte Gesamtlösung in Hamburg zu gestalten. Es bleibt zunächst abzuwarten, ob tatsächlich erhöhte Schutzbedarfsanforderungen ausreichend berücksichtigt werden.

Der HmbBfDI wird das Projekt weiter unterstützen und ist zuversichtlich, dass hier eine angemessene Lösung entsteht.

5. KI-Anwendung „LLMoin“

Die FHH nimmt sich des Themas Large Language Models (LLM) an, um deren Nutzen für einen Einsatz in der öffentlichen Verwaltung zu erproben und setzt dabei nicht nur im Projektnamen auf Lokalkolorit, sondern auch bei der Technik auf ein in Deutschland entwickeltes und betriebenes Sprachmodell.

Der rasant schnellen Entwicklung auf dem Gebiet der LLMs, getrieben zunächst insbesondere durch Dienste wie ChatGPT, hat sich die FHH zügig angenommen und die mögliche Nutzung von LLMs in der öffentlichen Verwaltung ins Auge gefasst. Zunächst wurden bereits Mitte des Jahres 2023 Anwendungshinweise zu ChatGPT formuliert. Dazu wurde dem HmbBfDI im Vorfeld der Veröffentlichung die Möglichkeit der Stellungnahme eingeräumt. Es konnten aus datenschutzrechtlicher Sicht notwendige Ergänzungen erreicht werden, etwa zu der Frage der Vermeidung der Eingabe personenbezogener Daten durch den Anwender in den Prompt, um einer Verarbeitung dieser Daten durch den Dienstanbieter zu Trainingszwecken vorzugreifen.

Der HmbBfDI wird auch bei der Erprobung eines von der Senatskanzlei auf Grundlage des Sprachmodells Luminous von Aleph Alpha beteiligt. Das Projekt wird zur Erprobung des Nutzens eines eigenen LLMs in die Wege geleitet und es sollen mit der Pilotierung einer internen Assistenzfunktion Nutzungspotentiale für die Arbeit in der öffentlichen Verwaltung ausgelotet werden. Stichworte wie Arbeitserleichterung, Effizienzsteigerung der Verwaltungsarbeit zugunsten der Bürgerinnen und Bürger stehen dabei im Vordergrund. Im Ergebnis kommt das Sprachmodell in verschiedenen Fachbehörden zum Einsatz. In den einzelnen Fachbehörden werden verschiedene Einsatzszenarien vorgesehen und vier Funktionen erprobt. Den Nutzerinnen und Nutzern standen Funktionen zur Textzusammenfassung, Textgenerierung, für „freies Prompting“ und ein Recherche-Assistent zur Verfügung. Nach Abschluss der Pilotphase folgt im ersten

Quartal 2024 die Auswertung des Pilotbetriebs, verbunden mit einer Evaluierung und Gegenüberstellung mit verschiedenen LLMs. Anschließend soll über eine Fortführung entschieden werden.

Der HmbBfDI begrüßt insbesondere, dass bei LLMoin ausdrücklich auf die Verarbeitung personenbezogener Daten verzichtet wird, d.h. es sollen weder personenbezogene Nutzungsdaten der Anwenderinnen und Anwender erhoben noch personenbezogene Daten bei der Eingabe von Befehlen verwendet werden. Die bereits in den oben genannten Anwendungshinweisen entwickelten Grundsätze wurden dementsprechend übernommen. Da es sich um ein bereits abschließend trainiertes Sprachmodell handelt, konnte zudem die Verarbeitung von personenbezogenen Daten zum Training des Modells vermieden werden. Im Beteiligungsprozess zu diesem Projekt soll dem HmbBfDI im Januar 2024 die abschließende datenschutzrechtliche Dokumentation zur Verfügung gestellt werden. Ein Hauptaugenmerk kann beispielsweise darauf liegen, welche technisch-organisatorischen Maßnahmen zur Vermeidung der Eingabe personenbezogener Daten getroffen wurden oder zukünftig getroffen werden.

Der Verlauf des Beteiligungsprozesses bleibt aber zunächst abzuwarten. Bislang bestand ein sehr guter und konstruktiver Austausch zwischen der Verantwortlichen und dem HmbBfDI. Insbesondere bleibt aber auch abzuwarten, wie Regulierungen auf europäischer Ebene, Stichwort AI Act, zukünftig dieses und vergleichbare Projekte beeinflussen werden.

6. Robotic Process Automation (RPA) in der FHH

Automatisierungstechnologie zur Entlastung der Beschäftigten in der Verwaltung erfordert eine genaue datenschutzrechtliche Einzelbetrachtung. Der HmbBfDI beriet zur architektonischen und prozessualen Ausgestaltung.

Bei Robotic Process Automation (RPA) handelt es sich um eine Technologie, die die automatisierte Ausführung von typischen und hochfrequenten Fachverfahrensabläufen ermöglicht. Dabei wird durch einen programmgesteuerten Ablauf (Roboter) ein dezidiert eingerichteter Facharbeitsplatz ferngesteuert, sodass die Bedienungsabläufe denen der bisher ausführenden Personen entsprechen sollen.

Aussagen zu RPA beziehen sich, sofern nicht anders beschrieben, in diesem Bericht auf die von der FHH eingesetzte Lösung von UiPath.

Der HmbBfDI erfragte erstmals im März 2021 nach Bekanntwerden von entsprechenden Plänen bei der Senatskanzlei (SK) eine Auflistung angedachter Pilotprojekte mit RPA. Im April 2021 erfolgte eine Kurzvorstellung von RPA für den HmbBfDI. Anlässlich der konkreten Nutzung von RPA im Rahmen von Kita-Online im April 2023, fand eine neue und tiefergehende Befassung mit der Technik RPA statt.

Als neue Technologie und Verfahrenskategorie innerhalb der FHH gilt und galt es seitens des HmbBfDI zunächst ein technisches Verständnis der RPA-Lösung aufzubauen. Zu diesem Zweck fanden zwischen April und August 2023 diverse Gespräche zwischen dem HmbBfDI und dem Amt für IT und Digitalisierung (ITD) sowie Dataport statt. Der HmbBfDI informierte sich zudem über die RPA-Infrastruktur-Pläne bei der Polizei. Auf Bitten des ITD um eine aktuelle Einschätzung erfolgte Ende August 2023 eine vorläufige Stellungnahme des HmbBfDI.

RPA stellt ein komplexes IT-Verfahren dar, das an mehreren Stellen in die IT der FHH integriert ist. Sogenannte Roboter führen automatisiert vordefinierte Tätigkeiten aus, in dem sie – wie ein Mensch – an einem eigenen virtuellen Arbeitsplatz Fachverfahren über die graphische Benutzeroberfläche steuern. Außerdem gibt es zentrale Komponenten zur Koordinierung und Überwachung der Roboter sowie zum Verwalten ihrer benötigten Zugangsdaten.

Mit Blick auf den technischen Datenschutz hält der HmbBfDI besondere Maßnahmen beim Einsatz von RPA für erforderlich und regt unter anderem folgende architektonischen und prozessualen Zusatzmaßnahmen für den weiteren Ausbau von RPA in der FHH an:

- Besonderer Schutz des zentralen Speichers für Roboter-Zugangsdaten. Hier gewährleistet der bestehende Ausbau bereits eine Verschlüsselung der ruhenden Daten. Der HmbBfDI regt an, eine Roboter-spezifische Verschlüsselung zu prüfen.
- Maßnahmen der kryptographischen Signatur von Programm-Code zur Sicherung der Authentizität und Integrität von Roboter-Programmen, um eine zentrale Manipulation von Roboter-Code zu erschweren.
- Eine besondere Bedeutung kommt bei RPA einem ausführlichen Test- und Freigabeprozess zu. Da Roboter prinzipbedingt graphische Bedienelemente statt wohldefinierter Programmierschnittstellen steuern, erfordert die Programmierung eine hohe Änderungstoleranz und lückenlose Fehlerbehandlung. Der HmbBfDI bewertet diesen Prozessschritt bei RPA durchaus als kritisch und regt an, diesen durch Informationsmaterial, standardisierte Abläufe und Überprüfungen bestmöglich zu härten.

Insgesamt hält der HmbBfDI einen datenschutzkonformen Betrieb von RPA in der FHH für umsetzbar. In jedem Fall hängt die konkrete Zulässigkeit eines RPA-basierten Verfahrens von den individuellen Umständen und der konkreten Ausgestaltung des Roboters ab. Für den derzeitigen Ausbau von RPA konnte der HmbBfDI im Austausch mit den RPA-Verantwortlichen noch zusätzliche Sicherheitsmaßnahmen identifizieren, die RPA noch breiter und sicherer einsetzbar machen dürften, und riet zu deren Umsetzung.

7. Scan Cars zur automatisierten Parkraumkontrolle

Zum Projekt „Digitalisierung Parkraumkontrolle – DigiParK" des Landesbetriebs Verkehr (LBV), das der HmbBfDI seit März 2022 begleitet, haben auch im Berichtszeitraum Beratungsgespräche stattgefunden. Ein Ziel des Projekts ist die Einführung von „Scan Cars" zur Überwachung des ruhenden Verkehrs.

Die mit Kamerasystemen ausgestatteten „Scan Cars" sollen Kennzeichen parkender Fahrzeuge erfassen und automatisiert mit einer Datenbank abgleichen, in der gültige Parkberechtigungen hinterlegt sind. Der Einsatz von „Scan Cars" könne nach Angaben des LBV die Überprüfung von bis zu 1000 Kennzeichen pro Stunde – das Zwanzigfache gegenüber dem manuellen Vollzug – und damit eine effizientere Aufdeckung von Parkverstößen ermöglichen.

Das Kfz-Kennzeichen als personenbezogenes Datum soll dabei in zwei Phasen verarbeitet werden. Zunächst müssten alle einem Kfz-Kennzeichen zugeordneten kurz- oder langfristigen Parkberechtigungen und Ausnahmegenehmigungen zum Halten und Parken digital verzeichnet werden. Nachfolgend könnte die Erfassung im Rahmen von Kontrollfahrten sowie der automatisierte Abgleich mit der digitalen Datenbank erfolgen.

Diese der Ermittlung von Ordnungswidrigkeiten dienenden Datenverarbeitungsvorgänge begründen einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der nur bei Vorliegen eines gesetzlichen Erlaubnistatbestandes gerechtfertigt sein kann. Der LBV hat einen entsprechenden Gesetzesentwurf zur Änderung des Straßenverkehrsrechts auf Bundesebene vorgelegt.

Der Gesetzesentwurf des LBV erlaubt in seiner zentralen Vorschrift zunächst die Abfrage von Kennzeichen bei der Beantragung oder

zum Nachweis von Berechtigungen und Genehmigungen zum Halten und Parken. Im Falle des Kurzzeitparkens sollen die Kennzeichen nach der aktuell vorgesehenen Regelung „nach Ende der Parkzeit, spätestens zum darauffolgenden Tage“ gelöscht werden.

Außerdem ermöglicht die Bestimmung die Verarbeitung von „Bild[ern] des Kennzeichens des Fahrzeugs (vorne und hinten)“ sowie des Ortes und der Zeit der Kontrolle mittels „optisch-elektronischer Einrichtungen“. Ergibt der ebenfalls gestattete digitale Abgleich, dass eine gültige Parkberechtigung vorliegt, sind die Daten ausweislich des Gesetzesvorschlags unmittelbar nach dem Kontrollvorgang zu löschen.

Die Übermittlung, Verwendung oder Beschlagnahme der erhobenen Daten nach anderen Rechtsvorschriften oder zur Profilbildung wird für unzulässig erklärt.

Den Fall der fehlenden Parkberechtigung regelt der Gesetzesvorschlag nicht. Nach Angaben des LBV soll in Fällen, in denen eine Parkberechtigung in der Datenbank nicht aufgefunden wird, die nähere Aufklärung und eine sich ggf. anschließende Verfolgung des Parkverstoßes entsprechend der heutigen Vorgehensweise behördlichem Kontrollpersonal übertragen werden.

Der Gesetzesentwurf ist dem HmbBfDI im Herbst 2023 zugeleitet worden. Anschließend hat ein erstes Gespräch mit Vertreter:innen der Behörde für Verkehr und Mobilitätswende (BVM) und des LBV zu den Regelungsinhalten und ihrer datenschutzrechtlichen Tragweite stattgefunden. Diskutiert wurde insbesondere auch die Übertragbarkeit der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zur Kfz-Kennzeichenerfassung und insbesondere seines Beschlusses vom 18. Dezember 2018, 1 BvR 142/15, auf die geplanten Datenverarbeitungsvorgänge.

In dieser Entscheidung hat das BVerfG festgestellt, dass automatisierte Kraftfahrzeugkennzeichenkontrollen aufgrund ihres erheb-

lichen Eingriffsgewichts zu ihrer Rechtfertigung jeweils auf Gründe gestützt werden müssen, die dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht oder sonst einem vergleichbar gewichtigen öffentlichen Interesse dienen. Der Gesetzgeber könne die Schwelle für besonders eingriffsintensive Überwachungsmaßnahmen näher konkretisieren und die Kennzeichenkontrolle etwa auch zur Verhinderung hinreichend gewichtiger Delikte zulassen, für deren Bekämpfung eine Kennzeichenkontrolle von besonderer Bedeutung sei, was gewichtige Ordnungswidrigkeiten einschließen könne (vgl. Rn. 99 der Entscheidungsgründe).

Stuft man Parkverstöße als keine hinreichend gewichtigen Ordnungswidrigkeiten in diesem Sinne ein, wäre die Ermächtigung zur automatisierten Kennzeichenkontrolle durch „Scan Cars" damit ggf. als unverhältnismäßig und der Grundrechtseingriff als nicht gerechtfertigt zu qualifizieren. Inwieweit die Erwägungen des BVerfG auf die geplanten Kennzeichenkontrollen durch „Scan Cars" übertragen werden können, ist jedoch fraglich. Der LBV hat vorgetragen, dem Beschluss des BVerfG habe in tatsächlicher Hinsicht eine andere Konstellation als die hier fragliche zugrunde gelegen, was eine abweichende rechtliche Beurteilung rechtfertigen könnte. Das BVerfG hatte sich in der zitierten Entscheidung mit dem verdeckten Einsatz automatisierter Kennzeichenerkennungssysteme zum Zwecke des Abgleichs mit polizeilichen Fahndungsbeständen zu befassen. Das Eingriffsgewicht einer offen und erwartbar stattfindenden Kennzeichenkontrolle durch Scan-Fahrzeuge könnte nach Ansicht des LBV demgegenüber ungleich geringer ausfallen.

Der HmbBfDI hat zu bedenken gegeben, dass bei Umsetzung des Vorhabens ein „anonymes" (Kurzzeit-)Parken im bewirtschafteten Parkraum künftig flächendeckend durch Straßenverkehrsbehörden ausgeschlossen werden könnte, was einen weiteren – ggf. auch im obigen Zusammenhang – zu berücksichtigenden Aspekt von grundsätzlicher Bedeutung darstellt.

Neben grundsätzlichen Fragen wurde auch die konkrete rechtliche und technische Ausgestaltung des Vorhabens thematisiert. Insoweit hat der HmbBfDI eine Konkretisierung der derzeit vorgesehenen Löschfristen für die beim Kurzzeitparken zu erhebenden Kfz-Kennzeichen angeregt und die geplante technische Ausgestaltung, die insbesondere eine Abbildung anderweitiger personenbezogener Daten etwa von Passanten verhindern muss, adressiert.

Am 29. September 2023 und damit wenige Tage vor dem Beratungsgespräch mit der BVM und dem LBV hatte der Bundesrat die Bundesregierung gebeten, im weiteren Reformprozess des Straßenverkehrsrechts die erforderlichen Rechtsgrundlagen zu schaffen, um ein rechtssicheres digitales Parkraummanagement zu ermöglichen (vgl. Stellungnahme des Bundesrates, Drucksache 381/23 (Beschluss)). In ihrer Gegenäußerung vom 4. Oktober 2023 hat die Bundesregierung festgestellt, dass der Vorschlag vor dem Hintergrund der Rechtsprechung des BVerfG zur Kfz-Kennzeichenerfassung einer vertieften Prüfung bedarf, womit insbesondere auch der oben zitierte Beschluss angesprochen sein dürfte. Die weitere Entwicklung der Initiative zur Einführung von „Scan Cars“ bleibt damit abzuwarten.

8. Videoüberwachung in Spielbanken

Die Videoüberwachung des Spielbankunternehmens soll ab 2024 vermehrt zu behördlichen Aufsichtszwecken herangezogen werden. Durch Videoüberwachung wird u. a. in das Persönlichkeitsrecht der Gäste der Spielbank eingegriffen, die sich in ihrer Freizeit unbeobachtet bewegen möchten.

Ende Juni 2023 trat die Behörde für Inneres und Sport mit dem Vorhaben einer Neuregelung der Videoüberwachung in der hamburgischen Spielbank an den HmbBfDI heran, nachdem die Konzession für den Betrieb der Spielbank Hamburg ab 1.1.2024 neu vergeben worden war. Das „große Spiel“ (Tischspiel), d. h. das manuelle

Roulette, und Kartenspiel an Tischen, muss nach dem Willen des Konzessionsgebers künftig am Hauptstandort und allen Dependancen der Spielbank Hamburg angeboten werden. Allerdings sieht sich die für die Steueraufsicht zuständige Behörde personell nicht in der Lage, die zutreffende Ermittlung der Steuern und sonstigen Abgaben der Spielbank durch anwesende Bedienstete des Finanzamts zu überwachen. Deshalb sollte das Spielbankunternehmen durch Änderung des Gesetzes über die Zulassung einer öffentlichen Spielbank (im Folgenden: Spielbankgesetz) verpflichtet werden, auch das große Spiel in allen Dependancen mit Videokameras zu überwachen und den für die Glücksspiel- und die Steueraufsicht zuständigen Behörden zugänglich zu machen. Bereits im 22. TB Datenschutz 2008/2009 (Kap. III 15.3 Videoüberwachung der Spielbank Hamburg zu aufsichtlichen Zwecken) und im 24. TB Datenschutz 2012/2013 (Kap. III 10.4 Technische Überwachung der Spielbank Hamburg) hatte der HmbBfDI sich mit Vorhaben der Videoüberwachung in der Spielbank Hamburg befasst und datenschutzrechtliche Bedenken geäußert.

Die Glücksspielaufsicht, die der Behörde für Inneres und Sport übertragen ist, überwacht das ordnungsgemäße Spiel; die der Finanzbehörde übertragene Steueraufsicht soll sicherstellen, dass alle Erträge ordnungsgemäß festgestellt und erhoben sowie steuerrechtliche Verstöße geahndet werden. Die Auflage, das große Spiel anzubieten, einerseits, und fehlende Aufsicht andererseits sind nicht miteinander vereinbar. § 6 Abs. 2b Spielbankgesetz ist deshalb ausgeweitet worden. Die Vorschrift verpflichtet die Spielbank, eine Videoüberwachung durchzuführen, allein um Daten zu Aufsichtszwecken zu übermitteln bzw. der Steueraufsicht einen automatisierten Abruf zu ermöglichen. Durch die Neuregelung hingegen sollten sowohl Spielbank- als auch Steueraufsicht direkten Zugriff auf die Videoüberwachung der Spielbank erhalten.

Gegen diese Pläne zur Änderung des Spielbankgesetzes hat der HmbBfDI im Vorfeld der Behördenabstimmung Bedenken geäußert. Durch die Videoüberwachung der Spielbank werden personenbezo-

gene Daten sowohl der Beschäftigten als auch der Gäste verarbeitet. Die Videoüberwachung der Spielbank greift tief in die Persönlichkeitsrechte der Beschäftigten der Spielbank und besonders der Gäste ein, die unbeobachtet ihrer Freizeitbeschäftigung nachgehen möchten. Diese Eingriffe müssen, jeweils dem Zweck der Videoüberwachung entsprechend, erforderlich und verhältnismäßig sein. Spielbankaufsicht und Steueraufsicht haben unterschiedliche Aufgaben, und die Nutzungsmöglichkeiten der Aufsicht müssen sich jeweils auf das erforderliche Maß beschränken.

Der HmbBfDI konnte erreichen, dass die Glücksspielaufsicht entgegen der ursprünglichen Pläne keinen Zugriff auf die Videosysteme der Spielbank erhält. Sie wird informiert und erhält auf Anforderung die relevanten Bilddateien, sollten Spielbank oder Steueraufsicht in den Videodateien Anhaltspunkte für solche Ordnungswidrigkeiten oder Straftaten erkennen, die der Glücksspielaufsicht unterliegen. Nicht erreichen konnte der HmbBfDI, dass die Finanzbehörde bzw. das Finanzamt eigene Videoüberwachung betreibt und sich auf die Nutzung dieser Bilddateien beschränkt. Die Steueraufsicht soll nach dem Willen des Gesetzgebers einen unbeschränkten Online-Zugriff auf die von der Spielbank gespeicherten Videobilder erhalten, und zwar zu nachträglichen Stichprobenkontrollen. Deshalb war es dem HmbBfDI besonders wichtig, dass im Spielbankgesetz genau festgelegt wird, auf welche gespeicherten Aufnahmen der Spielbank zugegriffen werden darf, insbesondere in welchen Fällen nur Handlungen der Personen sichtbar und in welchen Fällen Personen leicht identifizierbar sein dürfen. Zudem ist die Videoüberwachung zu Aufsichtszwecken durch den Spielbankunternehmer nach § 6 Abs. 2b Spielbankgesetz nur erlaubt, soweit nicht Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Darüber hinaus sind Zugriffe nach dem Spielbankgesetz und der vorrangigen DSGVO stets nur in erforderlichem Umfang zulässig. Um den Bruttospielertrag beim manuellen Spiel festzustellen, ist es nicht notwendig, Gesichter der Gäste zu erfassen. Es reicht der Einblick in das Spielgeschehen, um Manipulationen zu erkennen. Jedoch kann es zum

Nachvollziehen des regelkonformen Spielverlaufs erforderlich sein, zu erkennen, ob verschiedene Handlungen von derselben Person getätigt wurden, z.B. anhand der Kleidung. Zur Verfolgung steuerlicher Ordnungswidrigkeiten kann zudem die Identifizierung des handelnden Personals (Croupiers) erforderlich sein. Und schließlich ist es zum Schutz Betroffener wichtig, die Speicherdauer für Aufsichtszwecke zu begrenzen.

Letztlich sind sowohl durch das Spielbankgesetz als auch durch die DSGVO der Übermittlung zu Aufsichtszwecken so enge Grenzen gesetzt, dass die Rechte der Betroffenen bei der konkreten Ausgestaltung der zugänglichen Bilddaten gewahrt werden können. Besonderes Augenmerk wird der HmbBfDI deshalb künftig darauf zu richten haben, ob die Steueraufsicht wirklich nur solche Videoaufnahmen erhält, auf denen Betroffene lediglich im jeweils erlaubten Umfang sichtbar sind. Zu beachten ist, dass das Spielbankunternehmen zahlreiche Videokameras zu eigenen, anderen Zwecken als für die Aufsicht betreibt. Diese reichen von der Wahrnehmung des Hausrechts und der Zugangskontrolle in allen Bereichen der Spielbank, einschließlich Parkplatz, über Pflichten nach dem Geldwäschegesetz sowie Spielerschutz, und gehen über das Maß, das der Steueraufsicht zur Verfügung gestellt werden darf, hinaus. Daher steht außer Frage, dass die Schnittstelle zum Zugriff der Steueraufsicht nicht alle Kameras im Haus umfassen darf, sondern nur Aufnahmen, die nach den rechtlichen Maßstäben erforderlich und zulässig sind.

Die Steuerverwaltung plant, Anfang 2024 durch einen Verwaltungsakt nach der Spielordnung zu definieren, auf welche Videobilder ihr Zugriff einzuräumen ist. Dem HmbBfDI wurde eine Beteiligung bei der Ausgestaltung der Verwaltungsakte zugesagt. Dabei werden auch die weiteren konkreten Schutzbestimmungen in § 9 Abs. 6 Spielordnung zu beachten sein, die der HmbBfDI im Rahmen seiner Beteiligung durchsetzen konnte, wie Einschränkungen auf die Vogelperspektive, Verpixelungstechniken und eine KI-Anwendung, die erkennt, ob gerade ein Spiel läuft, und nur dann aufzeichnet.

Problematisch ist aus Sicht des HmbBfDI, dass die Spielordnung für die Einrichtung der Verpixelungstechnologie einen Übergangszeitraum bis zum 1.1.2025 einräumt, der behördliche Zugriff auf die Videoüberwachung aber bereits vorher erfolgen soll. Dies wird von der Steuerverwaltung mit der Verbindlichkeit in der öffentlichen Ausschreibung einerseits und der aufwändigen technischen Umsetzung andererseits begründet. Dadurch dürfte es einen begrenzten Zeitraum geben, in dem auch Gäste für die behördliche Aufsicht erfasst werden, ohne dass ihre Gesichter verpixelt werden. Die Dauer von maximal einem Jahr verkürzt sich allerdings dadurch, dass aufgrund der hohen technischen und organisatorischen Anforderungen mit der Ausweitung des großen Spiels nicht wie geplant zum 1.1.2024 begonnen wurde.

VII. ÖFFENTLICHKEITSARBEIT UND MEDIENBILDUNG

ÖFFENTLICHKEITSARBEIT UND MEDIENBILDUNG

1. Pressearbeit

Im Berichtsjahr 2023 erreichten den HmbBfDI rund 140 Presseanfragen. Wichtigste Themenbereiche waren hierbei Datenschutzfragen rund um Google Street View, Metas Pur-Abo-Modelle, polizeiliche Überwachungstechnologien sowie europäische Gesetzgebungsverfahren.

In 2023 erreichten den HmbBfDI zahlreiche Presseanfragen zum Update Google Street View. Hintergrund war die Ankündigung von Google neuen Aufnahmen zu veröffentlichen, die per Street View-Fahrzeug oder zu Fuß mit einem Kamerarucksack aufgenommen wurden. Als zuständige Datenschutzaufsichtsbehörde für Google in Deutschland hat der HmbBfDI mit einem umfassenden Informationsangebot Bürger:innen im ganzen Bundesgebiet bereits vor der Veröffentlichung der Bilder informiert und aufgeklärt. Diese Information sind auf ein überregionales mediales Interesse gestoßen.

Des Weiteren zogen die Regelungen bezüglich der Einführung des geplanten Abo-Modells bei Facebook und Instagram mediale Aufmerksamkeit auf sich. Meta musste sein Geschäftsmodell auf Druck der Datenschutzbehörden ändern. Ein Beschluss des Europäischen Datenschutzausschusses (EDSA) vom 27.10.2023 untersagt Meta als Betreiber der Dienste Facebook und Instagram die personalisierte Werbung ohne Vorliegen einer entsprechenden Einwilligung. Aus diesem Grund hat Meta angekündigt, kurzfristig ein Bezahl-Modell einzuführen, um entsprechende Anforderungen umzusetzen. Auch hier kam der HmbBfDI seinen Informationspflichten durch die Wahrnehmung diverser Interviews und Presseanfragen nach.

Insgesamt machten Anfragen zu den Internet-Konzernen Meta/Facebook und Google mehr als ein Drittel (36%) aller Anfragen des Berichtsjahres 2023 aus. Betrachtet man die Konzerne, liegt Google (22%) vor Facebook (14%). Die Digitalisierung der Gesellschaft wird auch im Jahr 2024 rasant voranschreiten. Daher ist davon aus-

zugehen, dass die Relevanz der Kommunikationsmaßnahmen des HmbBfDI zunehmen wird und der HmbBfDI weiterhin eine strategisch wichtige Rolle in der deutschlandweiten Datenschutz-Kommunikation einnimmt.

Zusätzlich zogen im Jahr 2023 europäische Gesetzgebungsverfahren, wie zum Beispiel der Digital Services Act (DSA), großes mediales Interesse auf sich. Bei den spezifisch hamburgischen Themen, die für Presseanfragen sorgten, lassen sich die Entwicklungen und Planungen rund um polizeiliche Überwachungstechnologien anführen.

Wie in den Vorjahren kann man hinsichtlich der Herkunft der anfragenden Medien sagen, dass über die Hälfte der Anfragen von überregionalen deutschen Medien stammt (62%). Anfragen regional hamburgisch-norddeutscher Medien sind im Vergleich zum Jahr 2022 auf einem ähnlichen Niveau geblieben und machen gut ein Drittel aus, wie die nachstehende Tabelle zeigt. Anfragen von ausländischen Medien sind gesunken.

Presseanfragen	2021	2022	2023
regionaler Medien:	28%	26%	29%
überregionaler Medien:	48%	53%	62%
ausländischer Medien:	24%	21%	9%

Tabelle1: Presseanfragen beim HmbBfDI 2021, 2022 und 2023

Im Berichtszeitraum 2023 hat der HmbBfDI insgesamt elf Pressemitteilungen veröffentlicht. Zudem haben der HmbBfDI selbst sowie mehrere Mitarbeiter:innen der Behörde diverse Vorträge und Präsentationen zu verschiedenen Themen des Datenschutzes gehalten und sich an öffentlichen Gesprächsrunden sowie Podiumsdiskussionen beteiligt.

2. Öffentlichkeitsarbeit

Der Bereich Öffentlichkeitsarbeit des HmbBfDI wurde im Jahr 2023 neu aufgestellt. Es wurde ein neues Websitekonzept entwickelt, das zeitgemäß ist und dem gestiegenen Informationsinteresse von Bürger:innen, aber auch Journalist:innen gerecht wird. Der Relaunch der Behördenwebseite www.datenschutz-hamburg.de war auch eine Reaktion auf die weiterhin hohe Anzahl an Presseanfragen, die den HmbBfDI erreichten.

Ein großes Projekt im Jahr 2023 im Bereich der Öffentlichkeitsarbeit war der Relaunch der Website www.datenschutz-hamburg.de. Im Zuge dessen wurde die Internetseite des HmbBfDI komplett überarbeitet. Der alte Internet-Auftritt war sowohl technisch als auch stilistisch nicht mehr zeitgemäß. Im Laufe der Jahre war der Internetauftritt des HmbBfDI unübersichtlich geworden und erlaubte keine intuitive Nutzung. Weder die Menüstruktur noch die Zuordnung der Inhalte waren selbsterklärend. Auch der gesetzlich vorgegebenen Barrierefreiheit konnte nicht umfänglich entsprochen werden.

In einer Verhandlungsvergabe ohne Teilnahmewettbewerb konnte ein erfahrener Dienstleister für den Relaunch der Website gefunden wurden. Innerhalb kürzester Zeit entwickelte der HmbBfDI gemeinsam mit dem Auftragnehmer ein neues Websitekonzept und -design. Beides wurde dann vom Auftragnehmer im Sommer 2023 technisch realisiert, sodass die neue Website im Oktober 2023 online gehen konnte. Der neue Website-Auftritt des HmbBfDI überzeugt mit einer nachvollziehbaren und übersichtlichen Struktur. Die Internetseite ist jetzt sowohl nutzungsfreundlich als auch zielgruppengerecht und barrierearm gestaltet. Sie spricht mit ihrem neuen modernen Design alle Zielgruppen (Bürger:innen, Datenschutz-Interessierte und -Fachleute) an. Bürger:innen können sich schnell informieren und unkompliziert die Beschwerdemöglichkeit über das präsent platzierte Formular finden. Fachpublikum und Firmen/Behörden können die für sie relevanten Handreichungen oder Gesetzestexte durch eine umfassende Suchfunktion rasch finden und abrufen.

3. Medienbildung

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat in enger Kooperation mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) das EU-Projekt #DigitaleVorbilder ins Leben gerufen. Hierbei handelt es sich um eine einzigartige Initiative, die erstmalig in Deutschland ein niedrigschwelliges und facettenreiches Informationsangebot speziell für Familien zu den relevanten Themen Datenschutz und Privatsphäre geschaffen hat.

Das Internet ist im Leben heutiger Kinder und Jugendlicher allgegenwärtig. Soziale Netzwerke, intelligente Geräte und künstliche Intelligenz gewinnen immer mehr an sozialer Bedeutung. Deshalb haben sich die Datenschutzbehörden von Hamburg und Mecklenburg-Vorpommern im Rahmen des EU-Projekts D.E.A.P zusammengetan. Ziel des Projektes ist es, Familien zu unterstützen und Eltern zu verdeutlichen, dass sie selbst auch digitale Vorbilder für ihre Kinder sind. Das Projekt bietet nicht nur leicht verständliche Informationen in verschiedenen Sprachen, sondern auch praxisnahe Tipps und Ratschläge für einen alltagstauglichen Umgang mit Datenschutz und Privatsphäre im digitalen Zeitalter. Die Kooperation zwischen dem HmbBfDI und dem LfDI MV sorgt für eine professionelle und fundierte Umsetzung des Projektvorhabens.

Gemeinsam mit dem Medienpartner TIDE strebt das Projekt #DigitaleVorbilder danach, Datenschutz greifbar und verständlich zu gestalten. Dies geschieht durch die Schärfung des Datenschutzbewusstseins mittels Online-Seminaren und barrierefreien Offline-Veranstaltungen. Für das Projektteam ist es dabei von zentraler Bedeutung, Familien für potenzielle Gefahren der digitalen Welt zu sensibilisieren, aber gleichzeitig keine Ängste zu schüren. Stattdessen verfolgt das Team einen konstruktiven Ansatz, der Eltern ermutigt, sich aktiv mit der digitalen Lebenswelt ihrer Kinder

auseinanderzusetzen. Hierbei legt das Projekt besonderen Wert auf die Hervorhebung der Vorteile digitaler Medien und schlägt gleichzeitig datenschutzfreundliche Lösungen vor.

Schon früh stellte sich heraus, dass der ursprüngliche Projektname "D.E.A.P." für die Zielgruppe nicht geeignet war. „D.E.A.P." ist nicht selbsterklärend und erfordert Erläuterungen, um verstanden zu werden. Da das Projekt einen niedrigschwelligen Ansatz verfolgt, war schnell klar, dass ein neues Logo und ein neuer Slogan notwendig sind. Der neue Slogan und Projektname lautet nun: "#DigitaleVorbilder – Familien gehen online". Der Slogan unterstreicht den Kerngedanken des Projektes, nämlich dass Eltern und enge Familienmitglieder die einflussreichsten Vorbilder für Kinder in der digitalen Welt sind.
In den ersten sechs Monaten hat das Projektteam alle Werbematerialien (Flyer, Postkarten, Roll-Ups, Fahnen) erstellt und die Kommunikationsstrategie zur Bewerbung der anstehenden Veranstaltungen ausgearbeitet. Zusätzlich wurde die Website der Datenschutzbehörde Hamburg angepasst, um das Projekt optimal der Öffentlichkeit vorzustellen und Informationen für interessierte Familien anzubieten (Link zur Projektwebsite www.digitale-vorbilder.eu).

Zusätzlich hat das Projektteam einen Beirat mit Expert:innen aus verschiedenen Fachbereichen ins Leben gerufen. Innerhalb der ersten zwölf Monate fanden zwei Treffen mit dem Beirat statt. Bei diesen initialen Zusammenkünften wurden die ersten Projektideen und -entscheidungen gemeinsam mit Fachleuten aus den Bereichen Familienbildung und soziale Dienste erörtert. Dies diente dazu, die Ratschläge des Beirats aktiv in die Projektplanung einzubeziehen.

Die Evaluierung des EU-Projekts wurde ebenfalls geplant. Es wurden zwei Evaluatorinnen hinzugezogen, um mit ihrer Unterstützung einen Online-Fragebogen zu entwickeln. Zusätzlich zu den Online-Fragebögen führen die Evaluatorinnen Interviews mit den Teilnehmer:innen der Veranstaltungen durch, um vertiefte Informationen zu erhalten. Von Interesse ist dabei immer, ob es nützliche Erkenntnisse und

Tipps für die Teilnehmenden gab und ob es Themen gibt, die noch bedient werden sollten.

In den ersten Monaten des Projekts stand die Veranstaltungsplanung im Vordergrund. Am 30. September 2023 startete der Medienaktionstag gleichzeitig in Hamburg und Schwerin (Mecklenburg-Vorpommern), gefolgt von einer Veranstaltung in Torgelow (Mecklenburg-Vorpommern) am 4. November 2023. In Hamburg setzten sich die Besucher:innen mit der Frage auseinander, inwieweit sie ihren Kindern ein digitales Vorbild sind und was ein digitales Vorbild ausmacht. In einer Podiumsdiskussion erfuhren sie zudem, wie wichtig es ist, ihre Kinder aktiv im Netz zu begleiten. Während sich die Kinder und Jugendlichen mit medienpädagogischen und kreativen Angeboten auseinandersetzten, diskutierten die Eltern in weiterführenden Workshops mit Expert:innen darüber, wohin Daten fließen, warum persönliche Daten geschützt werden müssen und wie man einen wirksamen Schutz der Privatsphäre umsetzt.

Am 8. November 2023 fand das erste Online-Seminar zum Thema „Gaming: Spielend sicher!“ statt. Zwei Expert:innen sprachen über die Risiken von Online-Spielen und gaben Ratschläge für den Umgang mit problematischen Situationen in Familien. Vier Wochen später folgte das zweite Webinar zum Thema „Smarte Spielzeuge – Datendiebe im Kinderzimmer“. Die Online-Seminare werden bis zum Sommer 2024 in einem 3-4-wöchigen Rhythmus fortgesetzt. Dabei werden verschiedene Themen behandelt, darunter Kinderschutz in digitalen Räumen, Datenschutz und Cybermobbing, Rechte, Verantwortlichkeiten und Pflichten als Eltern in digitalen Räumen sowie eine Einführung in Social-Media-Apps.

Auf der Grundlage von Expert:innengesprächen und Beiträgen aus den Vor-Ort- und Online-Veranstaltungen wird dann gemeinsam mit dem Medienpartner TIDE Bildungsmaterial in Form von Videos und Podcasts produziert. Die Materialien werden kontinuierlich auf der Projektwebsite www.digitale-vorbilder.eu veröffentlicht, beginnend im ersten Quartal 2024.

Das Projekt zeigte schon im ersten Jahr einen erheblichen Bedarf an Beratung und Sensibilisierung auf. Sowohl die Medienaktionstage als auch die Webinare wurden gut von der Zielgruppe angenommen. Diese positive Resonanz lässt vermuten, dass auch in Zukunft mit einer ähnlichen Beteiligung zu rechnen ist. Der HmbBfDI ist stolz darauf, dieses wegweisende EU-Projekt bis Ende 2024 fortzuführen, um weiterhin einen positiven Einfluss auf das Bewusstsein und die Handlungsweise von Familien in Bezug auf Datenschutzfragen zu nehmen. Mit #DigitaleVorbilder wird eine nachhaltige Plattform geschaffen, die nicht nur informiert, sondern auch dazu ermutigt, verantwortungsbewusste Entscheidungen im digitalen Raum zu treffen.

Es ist gleichwohl offensichtlich, dass eine nachhaltige Sensibilisierung für Datenschutz nicht allein durch sporadische Veranstaltungen erreicht werden kann. Aus diesem Grund ist es von besonderer Bedeutung, die Förderung der Datenschutzkompetenz in Hamburg auch über das Ende des Projekts im Jahr 2024 hinaus konsequent voranzutreiben. Dies gewährleistet, dass den Bürger:innen Hamburgs auch weiterhin eine Anlaufstelle für ihre offenen Fragen zum Datenschutz zur Verfügung steht. Gewonnene Erkenntnisse aus dem Projekt können dabei sinnvoll eingesetzt werden, um eine effiziente und gezielt auf die Bedürfnisse der Zielgruppen abgestimmte Entwicklung weiterer Sensibilisierungsmaßnahmen zu ermöglichen.

4. Workshop-Reihe mit Beschäftigten der Kinder- und Jugendhilfe

Der HmbBfDI traf sich zum Austausch und zur Vermittlung datenschutzrechtlicher Inhalte mit Fachkräften der Offenen Kinder- und Jugendarbeit. Gerade Fragen rund um Foto- und Filmaufnahmen bewegten die Teilnehmenden.

Im Rahmen eines von der Sozialbehörde veranstalteten ESF-Projektes (Vermittlung digitaler Medienkompetenzen, Teilprojekt 2

„AAAOKJA“) hielt der für „Soziales“ zuständige Rechtsreferent des HmbBfDI einen Vortrag. Die Veranstaltung trug den Namen „Ihre Fragen zum Datenschutz“ und richtete sich an Fachkräfte der Offenen Kinder- und Jugendarbeit.

Ziele der Veranstaltung waren die Vermittlung datenschutzrechtlicher Grundlagen, das gegenseitige Kennenlernen und die Stärkung des datenschutzrechtlichen Bewusstseins im Bereich der sozialen Arbeit. Hierbei wurden zunächst die Grundsätze und Zusammenhänge der Datenschutz-Grundverordnung erläutert. Die Veranstaltung endete mit einer Fragerunde. Ein besonderes Interesse der Teilnehmenden bestand hinsichtlich des Umgangs mit Fotografie- und Filmaufnahmen in den Einrichtungen, weshalb hier unterschiedliche Szenarien durchgespielt und aus datenschutzrechtlicher Sicht beurteilt wurden. Insbesondere wurde hervorgehoben, dass man sich bei Filmprojekten von Einrichtungen eine schriftliche Einwilligung bei den Teilnehmenden einholen sollte. Diese sollten ebenfalls Schilderungen zum Projekt und den Umständen enthalten, damit bei möglichen Konflikten nachgewiesen werden kann, dass die Beteiligten hinsichtlich der Tragweite hinreichend informiert worden sind.

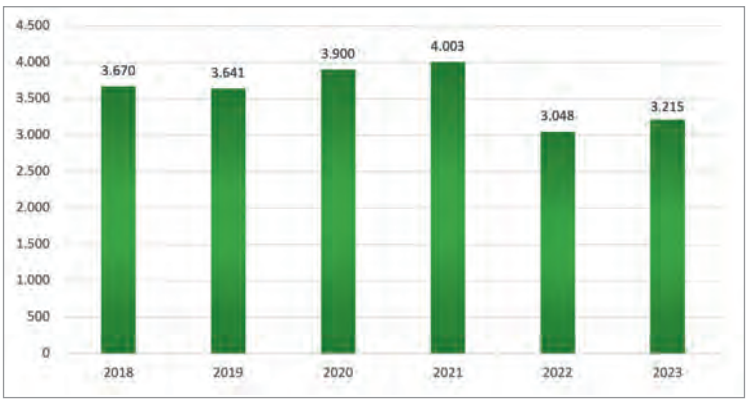
Für das Jahr 2024 sind bereits weitere Veranstaltungen in diesem Zusammenhang geplant.

VIII. INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT

INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT

1. Statistische Informationen (Zahlen und Fakten)

Im Berichtsjahr 2023 haben den HmbBfDI insgesamt 3.215 schriftliche Eingänge erreicht. Damit sind die Eingaben nach dem Rückgang im letzten Jahr wieder angestiegen. Die Beschwerden sind deutlich gestiegen und liegen wieder über dem Niveau von 2019. Die Beratungen von Betroffenen und datenschutzrechtlich verantwortlichen Stellen bleiben weiter auf einem hohen Niveau.

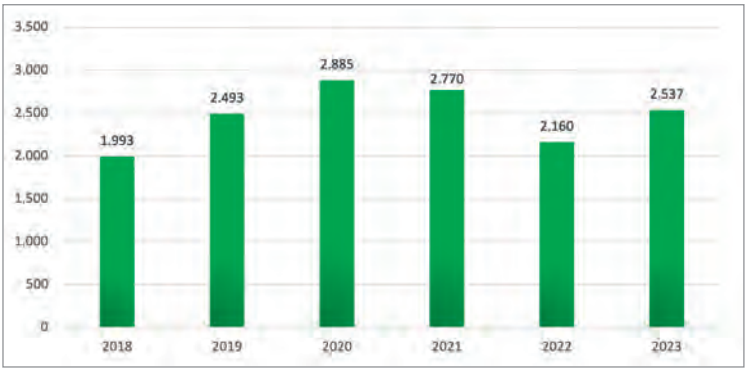


Schriftliche Eingänge beim HmbBfDI seit 2018

1.1 Beschwerden und Beratungen

Die datenschutzrechtlichen Beschwerden sind das Kernstück der Tätigkeit der Beschäftigten des HmbBfDI. Einerseits sind diese Beschwerden, die auf Grundlage des Art. 77 DSGVO eingelegt werden können, der direkte für Weg für Bürgerinnen und Bürger, ihre Rechte – mit Unterstützung des Hamburgischen Datenschutzbeauftragten – durchzusetzen. Andererseits bilden sie aber auch die Grundlage für Fälle mit europäischer Zusammenarbeit, für Ordnungswidrigkeitsverfahren, Bußgelderhebungen und unter Umständen auch für Gerichtsverfahren unter Beteiligung des HmbBfDI. Im Berichtszeitraum wurden 2.537 datenschutzrechtliche Beschwerden beim

HmbBfDI eingereicht. Dies ist der dritthöchste Wert seit Anwendung der DSGVO und damit auch der dritthöchste Wert an Beschwerden, die den HmbBfDI jemals erreicht haben.



Beschwerden nach Art. 77 DSGVO beim HmbBfDI seit 2018

Bei den Beratungen gab es eine kleine Verschiebung der Beratung von Betroffenen zu den sogenannten verantwortlichen Stellen, also Behörden und Unternehmen:

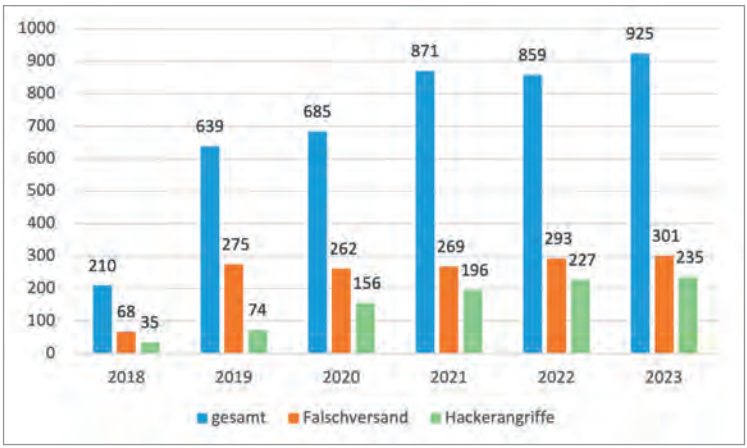
Schriftliche Beratungen von				
Jahr	**Betroffenen**	**Unternehmen**	**Behörden**	**Gesamt**
2022	254 (70%)	98 (27%)	9 (3%)	361
2023	211 (64%)	103 (31%)	15 (5%)	329

Bei der Erfassung der telefonischen Beratungen bleibt festzustellen, dass mit 1.130 Beratungen im Berichtsjahr 2023 der Spitzenwert von 2022 (1.432) zwar nicht erreicht wurde, aber auch dieser Wert auf einem hohen Niveau steht.

Jahr	Telefonische Beratungen
2023	1.130
2022	1.432
2021	642
2020	634
2019	821
2018	nicht gesondert erfasst

1.2 Meldungen nach Art. 33 DSGVO („Datenpannen“)

Die Meldungen nach Art. 33 DSGVO, also die Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, steigen zwar relativ nicht mehr in dem Maße an wie in den ersten Jahren der Anwendung der DSGVO, mit 925 Meldungen wurde im Jahr 2023 aber wieder ein neuer Höchstwert erreicht. Dabei sind die weiter ansteigenden Hackerangriffe hervorzuheben.



Meldungen nach Art. 33 DSGVO beim HmbBfDI seit 2018

Zwar sind die absoluten Zahlen im Vergleich zu den Vorjahren nur geringfügig gestiegen, bei Betrachtung der relativen Zahlen wird aber deutlich, dass die Hackerangriffe schon bald der häufigste Grund für eine Meldung nach Art. 33 DSGVO sein dürften. Machten die Hackerangriffe im Jahr 2019, also in dem Jahr, in dem die DSGVO zum ersten Mal über ein komplettes Kalenderjahr Anwendung fand, nur 12% der gemeldeten Datenpannen aus, waren es 2023 bereits 26%.

1.3 Abhilfemaßnahmen

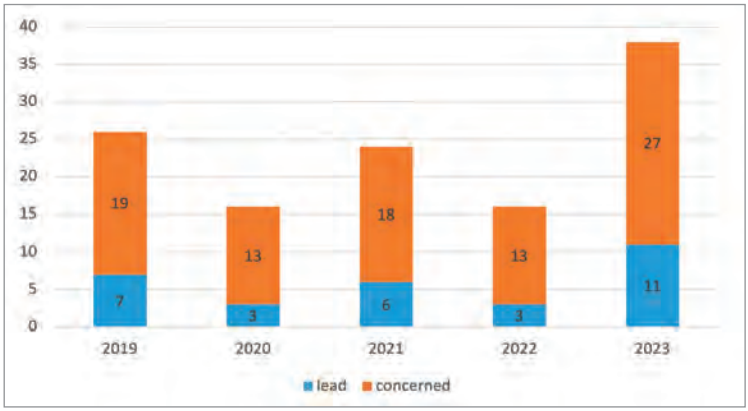
Auch in diesem Berichtszeitraum hat der HmbBfDI wieder von seinen verschiedenen Abhilfebefugnissen (Art. 58 Abs. 2 DSGVO) Gebrauch gemacht. Im Einzelnen wurden im Jahr 2023 folgende Maßnahmen ergriffen:

Maßnahme	Rechtsgrundlage	Anzahl 2023
Warnungen	Art. 58 Abs. 2 lit. a	0
Verwarnungen	Art. 58 Abs. 2 lit. b	26
Anweisungen und Anordnungen	Art 58. Abs. 2 lit. c-g und j	2
Geldbußen	Art. 58 Abs. 2 lit. i	8
Widerruf von Zertifizierungen	Art. 58 Abs. 2 lit. h	0

1.4 Europäische Verfahren

Seit Anwendung der DSGVO und damit der Einführung einheitlicher Datenschutzstandards bei den Mitgliedstaaten der Europäischen Union hat sich die Zusammenarbeit der Datenschutzaufsichtsbehörden deutlich verändert. Das formale Verfahren bei sogenannten grenzüberschreitenden Fällen, also wenn ein Sachverhalt oder ein Beschwerdegegenstand die Bürgerinnen und Bürger mehrerer europäischer Mitgliedstaaten betrifft, wurde formalisiert und ist mittlerweile Routine. Solche Fälle werden in das Binnenmarkt-Informationssystem der Europäischen Kommission (IMI – Internal Market Information System) eingegeben, die Aufsichtsbehörde, in der die datenschutzrechtlich verantwortliche Stelle ihren Sitz hat, übernimmt die Federführung (lead authority) und ebenfalls betroffene Behörden können sich als solche zu erkennen geben (concerned authority).

Im Berichtsjahr 2023 wurden 38 Fälle ins IMI eingetragen, an denen der HmbBfDI in 11 Fällen als lead authority und in 27 Fällen als concerned authority beteiligt ist. Dies ist eine deutliche Steigerung gegenüber dem Jahr 2022, in dem der HmbBfDI nur an 16 europäischen Verfahren (3 x federführend und 13 x betroffen) beteiligt war und der höchste Wert seit 2019.



Grenzüberschreitende Fälle mit Beteiligung des HmbBfDI im IMI

1.5 Stellungnahmen in Gesetzgebungsverfahren (Förmliche Begleitung bei Rechtsetzungsvorhaben)

Nach der „Richtlinie zur Beteiligung der/des HmbBfDI" ist die Hamburgische Datenschutzaufsichtsbehörde immer dann an Rechtssetzungsverfahren zu beteiligen, wenn Belange des Datenschutzes berührt sind. In der Regel geschieht dies dadurch, dass dem HmbBfDI im Rahmen einer sogenannten Senatsdrucksachenabstimmung die Möglichkeit zur Stellungnahme eingeräumt wird. Im Berichtsjahr 2023 war dies bei 98 Senatsdrucksachenabstimmungen der Fall, wobei 51 davon tatsächliche Rechtsetzungsverfahren waren. Dies bedeutet eine leichte Steigerung gegenüber den Zahlen aus 2022 (96 Beteiligungen, davon 44 Rechtssetzungsverfahren).

2. Einführung eines elektronischen Fallbearbeitungssystems

Seit März 2023 werden Eingaben beim HmbBfDI in einem Fallbearbeitungssystem rein elektronisch geführt.

Nach intensiver Vorarbeit konnte im Berichtsjahr beim HmbBfDI ein System eingeführt werden, mit dem die Fallakten rein elektronisch

geführt werden. Dadurch können Medienbrüche vermieden, bereits bestehende elektronische Schnittstellen aus Web-basierten Formularen besser genutzt und interne Abläufe optimiert werden.

Der HmbBfDI konnte sich dabei auf die vielfältigen Erfahrungen und die Expertise des IT-Dienstleisters Dataport stützen, der das verwendete System VIS bereits bei vielen öffentlichen Stellen insbesondere in den Trägerländern Schleswig-Holstein und Bremen einsetzt. Auch wenn VIS für hamburgische Behörden insoweit ein Novum darstellt, war die Einführung dieser komplexen und für den HmbBfDI unternehmenskritischen Anwendung daher mit vertretbarem Aufwand möglich.

Die ersten Monate der rein elektronischen Aktenführung zeigen ein insgesamt positives Gesamtbild. Die wesentlichen Erwartungen an Prozessökonomie, Verfügbarkeit auch unter Bedingungen des Home Office und Nutzungsakzeptanz wurden erfüllt. Dabei konnten in der ersten Stufe noch nicht alle Potenziale ausgeschöpft werden. Neben notwendigen anstehenden Ergänzungen z.B. im Bereich der Aktenarchivierung in Zusammenarbeit mit dem Staatsarchiv sind andere Erweiterungen angedacht, die den HmbBfDI weiter dabei unterstützen, das nach wie vor hohe Aufkommen an Beschwerden und sonstigen Eingängen gut und effizient bearbeiten zu können.

3. Aufgabenverteilung (Stand: 1.1.2024)

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

Dienststellenleiter:	Thomas Fuchs
Stellvertreter:	Ulrich Kühn
Vorzimmer:	Martina Coi

Pressereferentin, Internetangebot des HmbBfDI
Eva Zimmermann

Datenschutzkompetenzförderung und Medienbildung,
Öffentlichkeitsarbeit
Alina Schömig

EU-Projekt #DigitaleVorbilder
Lydia Roth, Isabel Schlosshauer

Verwaltungsleitung, BfH und Unternehmerpflichten,
Personal- und Organisationsleitung, Auskünfte nach HmbTG
Arne Gerhards

Haushaltsleitung, Haushaltsplanung und –bewirtschaftung,
Kennzahlen u. VZÄ-Controlling, Berichtswesen, DRiVe (Chief),
Gebühren- und Beschaffung (Grundsatz)
Robert Flechsig

Kennzahlenerhebung, Gebührensachbearbeitung
(einschl. Bußgelder), Beschaffung, Reisekostensachbearbeitung,
internes Vertragskataster
Rolf Nentwig

Geschäftszimmer, BMS-Recruiting, Aus- und Fortbildung, Meldungen nach Art. 33 DSGVO, EGVP, Altregistratur Eingaben
Ipek Sari

Geschäftszimmer, Registratur VIS, eZeit
Frau Vukšić

Geschäftszimmer, Gebäude- und Raumangelegenheiten, Registratur Sachakten und DSB
Annett Kolle

IT-Leitung und -Steuerung, Akkreditierung und Zertifizierung, IMI-Koordination
Herr Schneider

IT-Sachbearbeitung, Datenpflege HaSI, Intranet/SharePoint, Koordination Tätigkeitsberichte
Martin Schemm

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

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

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

Informationsfreiheit (HmbTG, UIG, VIG), Grundsatzfragen
Art. 58 DSGVO, Sanktions- und Abhilfebescheide,
themenübergreifende Einzelfallbearbeitung (Front Office)
Swantje Wallbraun

Informationsfreiheit (HmbTG, UIG, VIG), Grundsatzfragen
Art. 58 DSGVO, Sanktions- und Abhilfebescheide,
themenübergreifende Einzelfallbearbeitung (Front Office)
Dr. Markus Wünschelbaum

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

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

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

Projekt Datenschutz in der Ausländerverwaltung
Dr. Matthias Eichfeld

Stellvertretender Hamburgischer Datenschutzbeauftragter,
Akkreditierung und Zertifizierung
Ulrich Kühn

Akkreditierung und Zertifizierung, Presse und Rundfunk,
Telekommunikation
Katja Weber

ePrivacy, TTDSG und KI, Strategie und Planung
Wolfram Felber

Tracking und Cookies, Apps
Amina Merkel

Werbung und Adresshandel, TTDSG
Joelle Kremser

Entwicklung von Prüftools, Prüfung verantwortlicher Stellen (insb. Webseiten und Apps), technische Unterstützung bei der Fall- und Sachbearbeitung
Maike Friedrichs

Werbung und Adresshandel, E-Mail- und Spieleanbieter, Cloud-Dienste
Lisa Grunenberg

Akkreditierung und Zertifizierung, Grundsatzfragen des Kapitel VII der DSGVO, Koordination der Tätigkeiten mit Europabezug der Behörde sowie Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII der DSGVO
Frau Jacobson

Suchmaschinen (insb. Google, NorthData), Google Street View, Bewertungsportale
Dr. Jutta Hazay

Soziale Netzwerke (insb. Meta/Facebook, XING und Twitter), Datingportale (insb. Parship)
Sophie Engelhardt

Soziale Netzwerke, grenzüberschreitende Fälle (IMI), Data-Breach-Meldungen
Viviane Messan-Lawson

Soziale Netzwerke, grenzüberschreitende Fälle (IMI), Data-Breach-Meldungen
Anna-Mareike Werth

Grundsatzfragen Wirtschaft, Grundsatzfragen Verwaltung, Internationaler Datenverkehr
Dr. Jens Ambrock

Beschäftigtendatenschutz
Oksan Karakus

Themen- und fachbereichsübergreifende Einzelfallbearbeitung
Christopher Schack

Kreditwirtschaft, Vermieter/Immobilien
Viola Büchl

Gewerbliche Dienstleistungen, Industrie, Versicherungswirtschaft, Sicherheitsdienste, Beschäftigtendatenschutz
Pieter Jauernig

Stationärer Handel, Videoüberwachung nicht-öffentlicher Stellen
Bianka Albers-Rosemann

Versandhandel, Inkasso, Auskunfteien, Markt- und Meinungsforschung, grenzüberschreitende Fälle (IMI)
Eggert Thode

Behördenübergreifende Verfahren, Hochschulen, Demokratie (Wahlen, Parlamente, Parteien), Geodaten
Alexander Schiermann

Bildung (Schulen und Hochschulen), Forschung, Rechtsanwälte und Notare, Kammern, Kultur und Religionsgemeinschaften
Simone Hoffmann

Verkehr, Smart City
Pauline Mattern

Soziales, Gesundheit, Versorger (Strom, Gas, Abfall)
Sebastian Reich

Gesundheit, Medizinforschung
Sabine Siekmann

Behördenübergreifende Verfahren, Bezirke, Bauen und Wohnen (öffentlich), Umwelt und Landwirtschaft
Felix Wagner

Finanz- und Steuerwesen, Steuerberater, Wirtschaftsprüfer, Sport, Vereine und Stiftungen
Heike Wolters

Technisch-organisatorische Beratung und Prüfung
Farid Mehr

Technische Grundsatzfragen bei Biometrie, KI, Videoüberwachung, Konzeption und Betrieb des Prüflabors, technisch-organisatorische Beratung und Prüfung
Eike Kleinfeld

Technisch-organisatorische Beratung und Prüfung
Jutta Nadler

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

Technische Grundsatzfragen bei E-Government und OZG-Umsetzung, Konzeption und Betrieb des Prüflabors, technisch-organisatorische Beratung und Prüfung
Dr. Christian Burkert

STICHWORTVERZEICHNIS

Stichwortverzeichnis

F

G

H

I

J

K

T

U

V

W

Z