TÄTIGKEITSBERICHT DATENSCHUTZ 2025

Der Hamburgische
Beauftragte für Datenschutz
und Informationsfreiheit

34. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2025

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 / Westend61
Foto Thomas Fuchs:	Bildwerkstatt Nienstedten
Layout:	Verena Münch
Druck:	Druckservice Nord Sedelky

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

---

vorgelegt im März 2026
Thomas Fuchs
(Redaktionsschluss: 31. Dezember 2025)

INHALTSVERZEICHNIS

Vorwort

Über 4.200 datenschutzrechtliche Beschwerden allein in Hamburg. Das ist die Zahl für 2025, gut sechzig Prozent mehr als im Vorjahr; der höchste Wert, den die Hansestadt je verzeichnet hat. Auch bundesweit, gemessen an der Bevölkerungszahl, mit Abstand ein Höchstwert, wobei auch viele andere Länder ähnliche Steigerungen melden.

Das mag zunächst erstaunen. Denn es scheint doch der Datenschutz in schlechtem Ruf zu stehen. Post-Privacy-Debatten erleben im Schatten von KI-Euphorie eine Renaissance, Datenschutzstandards werden politisch kritisch und oft eher als Hindernis gesehen. Wie passt das zusammen? Warum suchen so viele Bürger:innen bei der Hamburger Datenschutzaufsicht Schutz und Unterstützung?

Sicher trägt dazu bei, dass KI in der Mitte der Gesellschaft angekommen ist und z. B. Bürger:innen auch beim Formulieren ihrer Beschwerden hilft. Durch KI-Chatbots werden zudem mehr Menschen darauf aufmerksam, dass das von ihnen dargestellte Problem überhaupt einen Datenschutzbezug hat, und auch, dass es dafür eigene Aufsichtsbehörden gibt. Allerdings ist auch zu beobachten, dass die KI den Nutzern gerne nach dem Mund redet und sie so oft fälschlich in der Vermutung bestätigt, im Recht zu sein. Und natürlich trägt dazu bei, dass das tägliche Leben sich weiter in seiner Breite digitalisiert.

Diese naheliegende Erklärung – mehr KI und Digitalisierung, mehr Datenschutzfragen – erklärt den Trend, aber nicht den Sprung.

Eine weitere wesentliche Ursache ist m. E., dass der digitale Kundenservice vieler Unternehmen nicht gut ist und durch unausgereifte KI-Tools zurzeit eher noch schlechter wird. Unsere Zahlen bilden das ab. Beschwerden z. B. im Bereich der Sozialen Netzwerke haben sich beinahe verdreifacht. Auch und gerade sehr große Unternehmen gestalten

im Grunde einfache Prozesse, wie etwa die Kontolöschung, extrem kompliziert. Der Supportservice, der im Wesentlichen nur von ChatBots durchgeführt wird, tut sein Übriges. Der Nutzer landet in Schleifen, aus denen kein Ausweg führt. Er bittet um Hilfe und bekommt Textbausteine. Er fragt nach seinen Daten und wird auf FAQ-Seiten verwiesen, die seine Frage nicht beantworten. Nutzer werden nicht gehört, Kontexte werden nicht erfasst, Frustrationen nicht wahrgenommen, Ausnahmen nicht gewürdigt. Das klingt nach einem Fall für den Verbraucherschutz, und ist es auch, aber nicht nur. Denn der Nutzer hat hier nicht nur ein Problem mit einer Dienstleistung. Er kann nicht erfahren, welche Daten über ihn gespeichert sind. Er kann nicht korrigieren, was falsch ist. Er kann nicht löschen, was ihn betrifft. Er wird nicht als Subjekt behandelt, das Rechte hat – sondern als Objekt, das verarbeitet wird.

Dann wird es eben auch ein Datenschutzthema. Der Einzelfall mag nicht aufregend sein, aber in der Summe entdecken wir oft systematische Probleme. Und die sanktionieren wir dann auch, wie kürzlich mit einem sechsstelligen Bußgeld wegen kontinuierlich schlechten Umgangs mit berechtigten Auskunftsbegehren von Kunden durch ein Unternehmen.

Mit der zunehmenden Digitalisierung werden die Bürger:innen also ein Stück weit allein gelassen. Dabei ist der Beratungsbedarf hoch. Das zeigt sich exemplarisch an der elektronischen Patientenakte (ePA), deren Einführung fraglos kein Musterbeispiel gelungener Verbraucherinformation ist. Oder am zunehmenden Digitalzwang, etwa bei der Deutschen Bahn. Und es zeigt sich an dem sehr großen Interesse, die unsere bürgernahen Beratungsangebote erhalten. Mit einer inzwischen 14-tägigen Datenschutzsprechstunde erreichen wir zahlreiche Menschen, die von der Fotografie in Kitas bis eben zur ePA ganz praktische Fragen zum Datenschutz haben. Und dies zeigen auch die knapp 1.500 Beratungsanfragen, die uns zusätzlich zu den Beschwerden in 2025 erreicht haben.

Bürger suchen Orte, an denen sie nicht verwaltet, sondern gehört werden. Dass sie diese Orte bei den Datenschutzbehörden finden, ist kein Zufall. Es ist das Ergebnis föderaler Strukturen, die Nähe ermöglichen.

Vor diesem Hintergrund stimmt mich die laufende Debatte um eine Zentralisierung der Datenschutzaufsicht nachdenklich. Die Argumente dafür klingen vertraut: Effizienz, Einheitlichkeit, Skalierung. Es ist dieselbe Logik, die derzeit den Kundenservice in die Chatbot-Wüste führt. Effizienz vor Erreichbarkeit, Skalierung vor Einzelfall. Der Zentralismus kann die digitale Transformation vielleicht aus einer Hand steuern. Aber er kann keine Bürgernähe herstellen. Und wenn der Druck auf eine zentrale Behörde steigt, drohen dort dieselben Mechanismen zu greifen: Automatisierung, Standardisierung, am Ende vielleicht auch hier ein Chatbot.

Dann stünde der Bürger zweimal vor verschlossenen Türen – erst beim Unternehmen, das seine Rechte verletzt, dann bei der Aufsichtsbehörde, die ihn davor schützen soll. Das wäre fatal. Denn die digitale Transformation wird uns nur gelingen, wenn Bürger:innen nicht bloß verwaltet, sondern mitgenommen werden.

Thomas Fuchs

EINLEITUNG I.

Einleitung

Datenschutzreform in Deutschland und Europa – zwei Wege, ein Ziel?
Ohne Zweifel war 2025 das Jahr, in dem der Datenschutz so intensiv politisch debattiert wurde wie seit Geltungsbeginn der DSGVO im Jahr 2018 nicht mehr. Dabei ist interessant, dass eine deutsche und eine europäische Diskussion zunächst unabhängig voneinander entstanden – und nun ineinander münden. Gemeinsam ist beiden ein Ziel, nämlich Effizienzsteigerung durch Entbürokratisierung.

Zunächst lohnt sich ein kurzer Rückblick auf die parallelen Entwicklungen:

Der Blick aus Berlin
Der Startpunkt auf deutscher Seite war der Zwischenbericht der „Initiative für einen handlungsfähigen Staat", die im März 2025 – also kurz nach der Bundestagswahl und parallel zu den Koalitionsverhandlungen – Reformideen zur Modernisierung vorlegte. Der Schwerpunkt lag auf Entbürokratisierung und Digitalisierung des Staates. In diesem Kontext gab es ein eigenes Datenschutzkapitel, das u.a. eine Zentralisierung der Datenschutzaufsicht forderte, ein Ende des sog. Gold-Platings und mehr Opt-out-Modelle anstelle von Einwilligungen. Auffällig war in diesen Vorschlägen, dass die europäische Perspektive nahezu vollständig ausgeblendet wurde.

Elemente der Initiative fanden sich dann im Koalitionsvertrag der neuen Bundesregierung wieder: Die Bündelung von Kompetenzen der Datenschutzaufsicht bei der BfDI, mehr Opt-out-Modelle bei staatlichen Bürgerservices sowie Entbürokratisierung für kleine und mittlere Unternehmen (KMU).

Nachdem im Sommer die „Initiative" ihren Abschlussbericht vorgelegt hatte, folgte im Herbst der Reformen die Erarbeitung einer Reformagenda auf Bund-Länder-Ebene, die am 04. Dezember 2025 als „Föderale Modernisierungsagenda" vom Bundeskanzler zusammen mit den Regierungschefs der Länder beschlossen wurde. Diese bisher insgesamt recht wenig beachtete Agenda verdient einen genaueren Blick, in unserem Kontext auf das Datenschutzkapitel:

Nationale Reform der Datenschutzaufsicht
Das Papier betont das Ziel einer einheitlichen Rechtsauslegung- und -anwendung durch Bündelung von Kompetenzen. Die Modernisierungsagenda nimmt, anders als der Koalitionsvertrag, nicht nur die BfDI in den Blick, sondern sieht auch Bündelungsoptionen auf Länderebene, etwa durch Zuständigkeitskonzentration und / oder einen föderalen One-Stop-Shop. Damit greift es Positionen auf, die vom HmbBfDI in einem Drei-Punkte-Plan zur Modernisierung der föderalen Zusammenarbeit der Digitalaufsicht entwickelt wurden. Auch der Plan, das „Einer-für-Alle"-Prinzip (EfA) zu verankern, gehört in diesen Zusammenhang.

Deutsches Gold-Plating und Opt-Out
Der Gedanke, dass in Deutschland Datenschutzrecht besonders streng ausgelegt bzw. durch deutsche Gesetze noch verschärft wird, das sog. Gold-Plating, hat große Verbreitung gefunden, insbesondere im Kontext des Datenschutzes. Bei näherer Betrachtung erweist sich dieser Vorwurf jedoch als Fata Morgana. Es gibt faktisch nur eine Norm, welche die DSGVO durch Konkretisierung verschärft – § 38 Abs. 1 BDSG, der die Benennungspflicht für Datenschutzbeauftrage bei nichtöffentlichen Stellen normiert. Diese Regelung soll nun abgeschafft werden. Das heißt auch: Mehr an deutschem „Gold-Plating" wurde nicht gefunden.

Positiv zu bewerten sind zwei Weiterentwicklungen der ersten Vorschläge: Opt-Out-Modelle werden nun auf konkrete Einsatzfelder – insbesondere im Gesundheitsbereich – gerichtet, und nicht pauschal gefordert. Das ist richtig.

Und generelle Erleichterungen für KMU, die eben nur auf EU-Ebene erreicht werden können, werden mit einer Weiterentwicklung des EU-Datenrechts verknüpft.

Der Blick aus Brüssel: Simplification
Das bringt uns zur europäischen Seite. Hier stehen keine Staatsreformen im Vordergrund, sondern die materiellen Vereinfachungen des

Europarechts. Spätestens mit dem Draghi-Report ist deutlich geworden, dass das dichte Regulierungsgeflecht der EU auch zu ökonomischen Hemmnissen führt. Draghi stellt diese Beobachtung in vielen Bereichen heraus, wie im Umweltschutz oder in der Sicherheits- oder Finanzpolitik; der Bericht betrifft aber auch die Digitalrechtsakte. Aus dieser Erkenntnis ist in Europa ein Reformprozess entstanden, der Entbürokratisierung, also „Simplification", zum Gebot der Stunde macht. Ergebnis dieses Prozesses sind insgesamt 12 Reform-Pakete, aus denen drei Vereinfachungsrechtsakte hervorgehen: zwei davon auf die DSGVO gerichtet und ein dritter auf den AI Act, der sogenannte Digitale Omnibus.

Knackpunkt KI

Ein wichtiger Punkt ist die Vereinbarkeit von KI und DSGVO. Dabei ist insbesondere das Verhältnis der Rechtsakte KI-VO und DSGVO zueinander klärungsbedürftig.

Kurz vor der Veröffentlichung des Digital Omnibus hat der HmbBfDI, zusammen mit den norddeutschen Nachbarn aus Schleswig-Holstein, mit einem Papier einen Brückenschlag von KI-VO zu DSGVO aufgezeigt, der deutlich macht, dass die Einhaltung des spezifischen Fachrechts der KI-VO überwiegend auch zur Erfüllung von DSGVO-Rechtspflichten führt. KI und DSGVO können in der Praxis also gut zusammengedacht werden.

Mit Bezug auf die Entwicklung und Nutzung von KI-Systemen versucht die EU-Kommission nun, Erlaubnistatbestände vor allem für das Training von Modellen mit personenbezogenen Daten zu schaffen, platziert diese aber sowohl in der DSGVO als auch in der KI-VO. Das richtig erkannte Problem wird so verfehlt gelöst und zudem systematisch fragwürdig: Erleichterungen für die Datenverarbeitung im KI-Kontext sollten im spezifischen Fachrecht der KI-VO geregelt werden. Eine zusätzliche Verankerung in der technologieneutralen DSGVO ist nicht zielführend und droht eher Rechtsunsicherheit zu erzeugen als sie zu beseitigen.

„Simplification", aber mit welcher Vereinfachung?
Insgesamt ergibt sich ein widersprüchliches Bild der europäischen Entwürfe. Eine Auflösung der Grundfesten der DSGVO ist nicht wirklich zu erkennen, aber auch substanzielle Erleichterungen für KMU sind eher Mangelware. Als reines Vereinfachungsgesetz stößt der Omnibus einerseits keine große DSGVO Reform an. Andererseits sind einige vermeintlich kleine Punkte – wie die Neudefinition personenbezogener Daten im Kontext von Anonymisierung – so grundlegend, dass sie den Rahmen eines bloßen Entbürokratisierungspakets sprengen.

Die Hamburger Sicht: Auf dem Weg zum Ziel
Der Omnibus bleibt als Reformvorhaben also ambivalent. Was fehlt, ist eine konsistente Linie. Ein wirklich risikobasierter Ansatz würde bedeuten, bei hochriskanten Verarbeitungen – insbesondere durch marktstarke Unternehmen – konsequenter zu regulieren, während risikoarme Verarbeitungen deutlich entlastet werden. Denn unnötige Bürokratie entsteht dort, wo der Aufwand außer Verhältnis zum tatsächlichen Risiko steht. Klare gesetzliche Verbote und Gestattungen würden hierzu ebenfalls beitragen. Fragen der Auslegung und des Ermessens sollten sich hingegen auf echte Grenzfälle beschränken. Davon ist der Omnibus weit entfernt.

Die deutsche föderale Modernisierungsagenda zeigt dagegen gute Ansätze – hier bleibt noch offen, ob sich am Ende doch Zentralisierungsmodelle durchsetzen, deren Umsetzung Jahre kosten und deren Effizienz zweifelhaft ist.

Was beide Reformprozesse verbindet: Sie versprechen Vereinfachung, laufen aber Gefahr, neue Komplexitäten zu schaffen: Wenn erst neue Strukturen geschaffen werden sollen, um dann Vereinfachungen zu ermöglichen, bedeutet das nur, bestehende Herausforderungen zu überspringen anstatt sie anzugehen. Mitten in einer dynamischen digitalen Transformation ist das viel zu langsam.

Echte Vereinfachung liegt darin, bestehende Systeme funktionsfähiger zu machen: Statt zu zentralisieren, die föderale Zusammenarbeit verbessern; statt neue Fragezeichen zu normieren, Schnittstellen zwischen Rechtsakten erschließen.

Das ist das, was wir tun: Als Landesbehörden leben wir das „Einer-für-Alle"-Prinzip vor und stärken die DSK in der praktischen Zusammenarbeit. Wir erschließen die Schnittstellen zwischen DSGVO auf der einen, KI-VO, Data Act und DSA auf der anderen Seite. So finden wir Wege, um Bürger:innen zu schützen, Datennutzung zu ermöglichen und das Recht kohärent anzuwenden. Gute Reformprozesse sollten diesen Weg unterstützen.

PRÜFUNGEN II.

Prüfungen

1. Data Breaches im Gesundheitsbereich

Verletzungen des Schutzes personenbezogener Daten im Gesundheitsbereich stellen eine Herausforderung dar, da sie regelmäßig besonders sensible Informationen betreffen und gravierende Folgen für betroffene Patient:innen sowie die Daten verarbeitenden Einrichtungen selbst haben können. Der HmbBfDI erhält eine Vielzahl von Meldungen über solche Vorfälle und prüft in diesen Fällen die Einhaltung der Vorgaben der DSGVO.

Die dem HmbBfDI im Berichtsjahr 2025 gemeldeten Datenschutzverletzungen reichten vom Falschversand medizinischer Unterlagen über deren Verlust / Diebstahl oder den Verlust / Diebstahl von Datenträgern mit darauf gespeicherten Gesundheitsdaten bis hin zu unrechtmäßiger Verarbeitung von Patient:innendaten durch Mitarbeitende von Gesundheitseinrichtungen und technischen Problemen wie zum Beispiel Hard- oder Softwarefehlern sowie Hackerangriffen. Zu den Data Breaches mit technischem Schwerpunkt sei an dieser Stelle auf den Beitrag in diesem Tätigkeitsbericht in Kapitel III 24 verwiesen („Fastlane“ für Data Breaches mit technischem Schwerpunkt).

Die rechtlichen Anforderungen an den Umgang mit solchen Datenschutzverletzungen sind in der DSGVO geregelt. Eine Verletzung des Schutzes personenbezogener Daten liegt gemäß Art. 4 Nr. 12 DSGVO vor, wenn es zu einer Verletzung der Sicherheit kommt, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt. Dabei ist unerheblich, ob der Vorfall unbeabsichtigt oder unrechtmäßig erfolgt ist. Im Falle einer solchen Verletzung ist die verantwortliche Stelle grundsätzlich verpflichtet, den Vorfall unverzüglich, spätestens innerhalb von 72 Stunden, an die

zuständige Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 DSGVO). Aufgrund der erhöhten Schutzbedürftigkeit der im Gesundheitsbereich verarbeiteten Daten ist bei Datenschutzverletzungen nahezu immer von einer Meldepflicht auszugehen.

Zusätzlich sind die Betroffenen nach Art. 34 DSGVO zu benachrichtigen, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für deren persönlichen Rechte und Freiheiten zur Folge hat. Der HmbBfDI prüft diese Voraussetzung prioritär, wenn er von einem Data Breach Kenntnis erlangt. Art. 34 Abs. 3 DSGVO sieht bestimmte Ausnahmen von der Benachrichtigungspflicht vor, etwa wenn geeignete technische und organisatorische Maßnahmen getroffen wurden, die die Daten für Unbefugte unzugänglich machen, wie zum Beispiel eine dem Stand der Technik entsprechende Verschlüsselung.

Ein Beispiel aus dem Berichtsjahr verdeutlicht die Herausforderungen im Umgang mit der Benachrichtigungspflicht: In einer Gesundheitseinrichtung wurde ein kompletter Tresor entwendet, der unter anderem schriftliche Aufzeichnungen zu sensiblen Gesundheitsdaten enthielt. Aufgrund der fehlenden Möglichkeit, die Betroffenen zu ermitteln und individuell zu benachrichtigen, erfolgte die Benachrichtigung in Abstimmung mit dem HmbBfDI in Form einer Information auf der Webseite der Einrichtung und in Papierform ausgelegt am Empfang.

Darüber hinaus richtet der HmbBfDI den Blick auch auf die technischen und organisatorischen Maßnahmen, die die verantwortliche Stelle grundsätzlich – und speziell aufgrund der gemeldeten Datenschutzverletzung – ergriffen hat und ergreift, um die Sicherheit der Verarbeitung nach Art. 32 DSGVO zu gewährleisten.

Um Verantwortliche bei der Erfüllung ihrer Pflichten zu unterstützen, stellt der HmbBfDI ein Online-Formular zur Meldung von Datenschutzverletzungen auf seiner Webseite bereit (https://da-

tenschutz-hamburg.de/service-information/datenpanne-melden). Ergänzend finden sich dort auch weiterführende Informationen und Beispielfälle zur Meldepflicht (https://datenschutz-hamburg.de/news/data-breach-notifications-was-ist-zu-tun).

Die Vielzahl und Komplexität der gemeldeten Datenschutzverletzungen im Gesundheitsbereich unterstreichen die Notwendigkeit einer kontinuierlichen Sensibilisierung und Prävention. Die konsequente Umsetzung der datenschutzrechtlichen Anforderungen im Zusammenhang mit Datenschutzverletzungen ist unerlässlich, um das Vertrauen in die Verarbeitung von Gesundheitsdaten zu erhalten und die Sicherheit der Betroffenen zu gewährleisten. Die korrekte Handhabung von Datenpannen ist für die Privatsphäre der betroffenen Patient:innen einerseits und die Arbeitsfähigkeit sowie die Reputation der betroffenen Gesundheitseinrichtungen andererseits von zentraler Bedeutung.

2. Fehlende Anonymisierung bei der Evaluation des Beurteilungswesens

Die Anonymisierung der Beurteilungsdaten dient der DSGVO-konformen Evaluation des Beurteilungswesens, indem sie personenbezogene Identifikationsmerkmale ausschließt, statistische Auswertungen ohne Rückschlüsse auf Einzelpersonen ermöglicht und die Grundsätze der Datenminimierung sowie Zweckbindung wahrt.

Aus Sicht der Freien und Hansestadt Hamburg sind statistische Auswertungen von Beurteilungsdaten erforderlich, um die Qualität und Gleichmäßigkeit des Beurteilungssystems zu sichern und potenzielle Diskriminierungen aufzudecken. Entsprechend der Regelungen der § 94er Vereinbarung zum Beurteilungswesen und Anlagen (vom 22.03.2013) ist für die Evaluation durch das Personalamt vorgesehen, dass mit Abschluss des zu nutzenden elektronischen Beurteilungsformulars durch den Beurteiler automatisch eine E-Mail mit einem

anonymisierten Evaluationsbogen als Anhang erzeugt wird, welche an ein festgelegtes Funktionspostfach im Personalamt voradressiert ist und entsprechend abgesandt werden soll.

Im Frühjahr 2025 stellte der HmbBfDI fest, dass im Rahmen der Evaluation des Beurteilungswesens der Freien und Hansestadt Hamburg bei der elektronischen Übermittlung des Evaluationsbogens an das Personalamt – an das hierfür eingerichtete Funktionspostfach – personenbezogene Daten der beurteilten Beschäftigten übermittelt wurden, obwohl nach der maßgeblichen Ergänzungsvereinbarung zum Beurteilungswesen eine anonymisierte Auswertung vorgesehen ist. Bei einer stichprobenartigen Prüfung wurde festgestellt, dass insbesondere Vor- und Nachnamen sowie Geburtsdaten der betroffenen Beschäftigten in der zur Evaluation verwendeten XML-Datei enthalten waren, sodass von einer unzureichenden Anonymisierung im Widerspruch zum Schutzzweck der Dienstvereinbarung und den einschlägigen datenschutzrechtlichen Vorgaben auszugehen war. Hintergrund für die Aufnahme dieser Identifikationsdaten in die XML-Datei war ursprünglich die Absicht, eine doppelte Erfassung derselben Person zu vermeiden, um die statistische Auswertung der Beurteilungen nicht zu verfälschen.

Nach Hinweisen des HmbBfDI leitete das Personalamt zeitnah eine Überprüfung des Verfahrens ein, welche zu einer datenschutzfreundlichen Anpassung führte. Bereits knapp einen Monat später teilte das Personalamt mit, dass der Name und das Geburtsdatum aus der betreffenden XML-Datei entfernt worden sind und damit für das statistische Controlling nicht mehr zur Verfügung stünden. Das entsprechend überarbeitete Beurteilungsformular wurde im Personalportal im Bereich zum Beurteilungswesen veröffentlicht und steht den Dienststellen seitdem in aktualisierter Fassung zur Verfügung.

Gleichwohl verdeutlicht der Vorgang, dass bereits die Aufnahme von Identifikationsdaten in die für statistische Zwecke bestimmte Datei ein datenschutzrechtliches Risiko begründet, wenn eine Anonymisierung vorgesehen ist und aus Sicht der Betroffenen die Gefahr einer Personenbeziehbarkeit besteht. Vor diesem Hintergrund ist die nun vorge-

nommene Entfernung von Namen und Geburtsdaten aus der XML-Datei ein wichtiger Schritt zur datenschutzgerechten Ausgestaltung der Evaluation des Beurteilungswesens im Sinne der Ergänzungsvereinbarung und der datenschutzrechtlichen Grundsätze der Datenminimierung und Zweckbindung. Das Einschreiten des HmbBfDI führte dazu, dass im Rahmen der für den 1. Januar 2026 vorgesehenen Reform des Beurteilungswesens durch das Personalamt auch das Controlling und die Evaluation vollständig neu ausgerichtet und datenschutzkonformer gestaltet werden und stellt einen datenschutzrechtlichen Erfolg dar.

3. Unzulässige Weitergabe von Standortdaten durch Apps

Die Dating-App einer Hamburger Betreiberin übermittelte trotz nicht erteilter Einwilligung genaue Standortdaten an Werbepartner.

Im Berichtszeitraum hat der HmbBfDI eine in seine Zuständigkeit fallende Dating-App untersucht, die Nutzer:innen auf Basis der Standortdaten (Geopositionen) ihrer mobilen Geräte lokalisiert und miteinander in Kontakt bringt. Die Prüfung erfolgte nach der Veröffentlichung der Berichterstattung zu den sogenannten „Databroker Files" von netzpolitik.org und dem Bayerischen Rundfunk (https://netzpolitik.org/2024/databroker-files-firma-verschleudert-36-milliarden-standorte-von-menschen-in-deutschland). In den Recherchen wurde offengelegt, dass Datenhändler mit genauen Standortdaten von Personen handeln, durch welche die Personen eindeutig identifiziert werden können. Aus diesen Daten ergaben sich aus Sicht der Journalist:innen Rückschlüsse auf private Gewohnheiten, sensible Aufenthaltsorte und sogar auf Wohn- und Arbeitsadressen.

Die Weitergabe der Standortdaten findet dabei über hochkomplexe Prozesse im digitalen Werbeumfeld statt, das auf dem sogenannten Realtime-Bidding beruht. Beim Realtime-Bidding verbinden Werbenetzwerke Anbieter von Werbeplätzen auf Webseiten oder in Apps

und Werbetreibende, um Werbung möglichst zielgenau und gewinnbringend zu vermarkten. Die Vergabe der Werbeplätze erfolgt automatisiert und in Echtzeit an den jeweils Meistbietenden. Dafür werden große Mengen an (personenbezogenen) Nutzungsdaten, darunter auch Standortdaten, an eine Vielzahl von Akteuren im Werbeökosystem übermittelt.

Den journalistischen Recherchen war der Hinweis auf die App eines Anbieters mit Sitz in Hamburg zu entnehmen. Der HmbBfDI prüfte die Informationen, die den Nutzer:innen bei Installation und Nutzung dieser App bereitgestellt werden und analysierte den Datenverkehr der App während der Nutzung unter verschiedenen Einsatzbedingungen.

Bei den nach Artt. 12, 13 und 14 DSGVO erforderlichen klaren und verständlichen Informationen zur Weitergabe genauer Standortdaten an Werbepartner wurden durch den HmbBfDI Mängel festgestellt. Soweit entsprechende Informationen erteilt wurden, stimmten diese nicht mit den tatsächlichen Datenflüssen überein, in denen die Übermittlung von genauen Standortdaten an bestimmte Werbepartner eindeutig nachgewiesen werden konnte.

Die technischen Einstellungen in der App wiesen ebenfalls Mängel auf. Entgegen der nach Art. 25 Abs. 2 DSGVO zu wählenden datenschutzfreundlichen Voreinstellungen war die Erlaubnis zur Weitergabe von genauen Standortdaten an Werbedienste standardmäßig aktiviert. Nutzer:innen mussten der Weitergabe aktiv widersprechen. Dies war deshalb besonders kritisch, da die in der App eingebundenen Werbedienste automatisch diejenigen Berechtigungen erhielten, die Nutzer:innen der App erteilten. Im Falle einer Dating-App wird die Berechtigung für den Zugriff auf genaue Standortdaten regelmäßig erteilt, da sie essenziell für die Funktionalität der App ist, um sich mit Personen in räumlicher Nähe zu verbinden. Wurde diese Berechtigung erteilt, konnte sie damit automatisch auch von eingebundenen Werbediensten genutzt werden.

Nicht zuletzt aufgrund der Komplexität und Vielzahl an beteiligten Akteuren, zu denen neben der Appbetreiberin auch verschiedene Werbepartner- und Netzwerke mit einer undurchschaubaren Menge von Beteiligten gehörten, wurde es Nutzer:innen der App erschwert, die Kontrolle über ihre Daten zu behalten. Im Kontext einer Dating-App, bei der auch nach Art. 9 DSGVO besonders geschützte Daten an Dritte weitergegeben werden können, ist dies besonders bedenklich. Besonders schwerwiegend ist, dass die App – auch nach Entfernen des zuvor gesetzten Symbols zum „Akzeptieren" im eingesetzten Einwilligungsdialog – weiterhin genaue Standortdaten an Werbepartner übermittelte.

Mit den Prüfergebnissen konfrontiert, hat die Anbieterin der App die Ursache der Weitergabe genauer Standortdaten an Werbepartner zügig identifiziert und mittlerweile unterbunden. Zudem hat sie proaktiv Maßnahmen implementiert, mit welchen sie künftig Datenflüsse in der App überwachen und so den unzulässigen Abfluss an Werbenetzwerke unterbinden kann.

Die durch die Prüfung gewonnenen Erkenntnisse werden in die weitere Beratung und Kontrolle von App-Anbietern einfließen.

4. Anlasslose Webseitenprüfung

Bei einer umfassenden Prüfung von Webseiten hat sich gezeigt, dass viele Betreiber:innen von Websites die datenschutzrechtlichen Anforderungen beim Einbinden externer Dienste nicht hinreichend kennen oder umsetzen. Bei 185 der 1000 geprüften Websites mussten die Anbieter nachbessern.

Der HmbBfDI prüft Webseiten regelmäßig nach Beschwerden oder konkreten Hinweisen auf den Einsatz von Tracking-Technologien, die unerwünschtes Nachverfolgen des Nutzungsverhaltens ermöglichen. Solche unerwünschten Zugriffe auf Browser in Endgeräten wie Computern, Tablets oder Smartphones erfolgen dabei in der Regel durch die

Einbindung von Drittdiensten, die Cookies und vergleichbare Techniken (z. B. Web Beacons, Browser-Fingerprinting) einsetzen.

Das Speichern oder Abrufen von Informationen im Browser ist nach § 25 Abs. 1 TDDDG regelmäßig nur mit Einwilligung zulässig. Eine Ausnahme besteht nur, wenn ein Cookie unbedingt erforderlich ist (§ 25 Abs. 2 Nr. 2 TDDDG), z. B. für die Anmeldung im eigenen Account. Tracking zur Analyse oder zur Angebotsverbesserung kann zwar sinnvoll sein, ist aber für die reine Anzeige von Webseiteninhalten nicht unbedingt erforderlich. Die Pflicht, eine TDDDG-Einwilligung einzuholen, gilt unabhängig davon, ob personenbezogene Daten verarbeitet werden. Häufig ist jedoch ein Personenbezug gegeben, etwa durch individuelle Kennungen oder gespeicherte Präferenzen, sodass zusätzlich eine Einwilligung nach der DSGVO erforderlich ist.

Beschwerden im Berichtszeitraum zeigten, dass viele Betreiber:innen datenschutzrechtliche Anforderungen beim Einbinden von Drittanbietern, die Tracking-Techniken einsetzen, nicht ausreichend kennen oder umsetzen. Um proaktiv das Bewusstsein für diese Anforderungen zu schärfen, beschloss der HmbBfDI eine anlasslose Prüfung mit einem mehrstufigen Ansatz.

In der ersten Stufe wurden 1.000 zufällig ausgewählte Websites von Betreiber:innen mit Sitz in Hamburg automatisiert daraufhin geprüft, ob bereits beim erstmaligen Aufruf der Angebote Drittanbieter Cookies setzten oder Geräteinformationen auslasen, ohne dass die erforderlichen Einwilligungen vorlagen. Dabei wurde das Prüftool Website-Evidence-Collector (WEC) eingesetzt, das konkrete externe Dienste anhand typischer technischer Merkmale wie spezifischer Cookies, LocalStorage-Einträgen oder dem Aufruf bekannter Webadressen erkennen kann. Die Auswahl der Drittanbieter orientierte sich an der bisherigen Prüfpraxis des HmbBfDI.

Die Prüfung ergab, dass der Großteil der untersuchten Websites die Vorgaben aus TDDDG und DSGVO einhält. Bei 185 Angeboten wurden jedoch Mängel festgestellt: Tracking-Technologien von Drittanbie-

tern wurden so eingebunden, dass bereits beim initialen Aufruf der Webseite auf die Endgeräte der Betroffenen zugegriffen wurde, ohne dass hierfür Einwilligungen vorlagen – zu diesem Zeitpunkt hätten die Nutzer:innen auch bei einem eventuell eingebundenen Cookie-Banner noch keine Auswahl treffen können. Besonders häufig betroffen waren Zugriffe durch Google Analytics (110 Fälle), Google Maps (51), Google Ads (42), YouTube (20) und Facebook (15).

In einer weiteren Stufe wurden die Betreiber:innen der betroffenen Webseiten über die vorgefundenen Datenschutzmängel informiert und aufgefordert, die Defizite binnen sechs Monaten zu beseitigen. Das Schreiben enthielt umfangreiche Hinweise und Empfehlungen für eine datenschutzkonforme Gestaltung. Zur Unterstützung stellte der HmbBfDI zudem ein umfangreiches Beratungsangebot bereit, darunter schriftliche Informationen, Antworten auf die meistgestellten Fragen auf der Website und eine Telefonsprechstunde für Rückfragen.

In der dritten Stufe erfolgte nach Ablauf der eingeräumten Nachbesserungsfrist eine erneute Prüfung der betroffenen Webseiten. Dabei zeigt sich ein gemischtes Bild. Es ist erkennbar, dass viele Betreiber:innen bemüht sind, die Datenschutzvorgaben einzuhalten, ihnen dies aber nicht in allen Fällen vollständig gelungen ist. Einzelne Verantwortliche sind allerdings untätig geblieben oder haben die Datenschutzprobleme ihrer Angebote sogar vergrößert. Die Prüfungen dauern daher über den Berichtszeitraum hinaus an. Betroffene Betreiber:innen erhalten weiterhin Gelegenheit, das Beratungsangebot des HmbBfDI zu nutzen und die erforderlichen Anpassungen vorzunehmen.

Als Ergebnis der anlasslosen Prüfung kann der HmbBfDI feststellen, dass ein erheblicher Informations- und Beratungsbedarf bei Betreiber:innen von Webseiten besteht. Auch künftig wird der HmbBfDI daher auf eine Kombination aus technischer Prüfung, Beratung und – wo erforderlich – Einleitung von aufsichtsbehördlichen Maßnahmen setzen, um die Einhaltung von datenschutzrechtlichen Vorgaben zu gewährleisten und die Nutzer:innen der Internetangebote vor unzulässigen Trackingmaßnahmen zu schützen.

5. Werbliche Telefonanrufe im Zusammenhang mit Leistungen der Pflege- und Krankenkassen

Im Berichtszeitraum erreichten den HmbBfDI zahlreiche Beschwerden im Zusammenhang mit unerwünschten werblichen Telefonanrufen zu pflegerischen Produkten und Dienstleistungen, die gegenüber den Pflege- und Krankenkassen abgerechnet werden können. Der HmbBfDI konnte durch gezielte Ermittlungen und Interventionen Verbesserungen für die Betroffenen erreichen.

Die Beschwerden betrafen insbesondere die Vermittlung von Pflegeboxen, Hausnotrufsystemen und Online-Pflegekursen für pflegende Angehörige. Die Betroffenen wurden angerufen, ohne zuvor Kontakt mit den werbenden Unternehmen gehabt zu haben („Cold Call"). Ihnen wurden die Leistungen angeboten und mitgeteilt, dass die Pflege- oder Krankenkassen die Kosten hierfür übernehmen. In vielen Fällen handelte es sich um Leistungen, die für die Betroffenen nicht notwendig waren.

Die Anrufenden verfügten bereits vor der Kontaktaufnahme über personenbezogene Daten der Betroffenen, darunter Telefonnummern, Geburtsdaten, Versicherungsnummern und teilweise auch besonders schutzwürdige Informationen wie den Pflegestufengrad. Im Gespräch wurden von den Anrufenden teils weitere Daten erhoben. Im Anschluss an die Telefonate wurden Anträge, etwa zum Bezug monatlicher Pflegeboxen, über Online-Portale an die Anbieter der Pflegeleistungen übermittelt, die diese wiederum bei den zuständigen Kranken- oder Pflegekassen der Betroffenen einreichten.

Regelmäßig waren in den vorliegenden Fallkonstellationen mehrere Unternehmen und Dienstleister beteiligt: Die Beschwerden richteten sich gegen die Anbieter der Produkte oder Dienstleistungen, die beworben wurden. Diese – oftmals kleineren – Unternehmen organisierten ihren

Vertrieb über externe, bundesweit tätige Vertriebsmitarbeiter:innen, die im Namen der Anbieter agierten und sich teilweise irreführend als „von der Krankenkasse beauftragt“ ausgaben.

Allen Fällen war gemeinsam, dass die werblichen Telefonanrufe ohne vorherige ausdrückliche Einwilligung der betroffenen Personen erfolgten, obwohl eine solche nach § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) notwendig ist. Die Betroffenen hatten häufig bereits vergeblich versucht, ihre Betroffenenrechte – insbesondere das Auskunftsrecht über ihre personenbezogenen Daten sowie deren Löschung – gegenüber den verantwortlichen Unternehmen geltend zu machen.

Der HmbBfDI forderte die verantwortlichen Unternehmen mit Sitz in Hamburg zur Stellungnahme und zur Erfüllung von Betroffenenrechten – insbesondere zur Auskunftserteilung und Löschung – auf. Im Zuge der Ermittlungen gaben manche Unternehmen an, vom konkreten Vorgehen der Vertriebsmitarbeiter:innen keine Kenntnis gehabt zu haben. Einige Unternehmen stellten die Zusammenarbeit mit externen Vertriebsmitarbeiter:innen ein, nachdem diese die erforderliche Einwilligung für die werblichen Telefonanrufe nicht dokumentieren konnten. Darüber hinaus wurden Online-Portale der Unternehmen zur Vermeidung weiteren Missbrauchs angepasst, sämtliche Bestellungen storniert, Betroffenenrechte umgesetzt und Datenschutzbeauftragte bestellt.

Besonders problematisch waren Fälle, in denen personenbezogene Daten für die Vermittlung von Online-Pflegekursen über ein nicht in der Europäischen Union ansässiges Unternehmen erhoben wurden. Die betroffenen Personen sollen ihre Einwilligung für die werblichen Telefonanrufe angeblich im Rahmen von Online-Gewinnspielen erteilt haben, was jedoch von den Betroffenen bestritten wird. Die vom Unternehmen vorgelegten Einwilligungen konnten den Nachweis einer tatsächlich ausdrücklich abgegebenen Einwilligung im Rahmen einer Prüfung des HmbBfDI nicht erbringen. Die Ermittlungen in diesen Fällen sind noch nicht abgeschlossen.

Bei unerwünschten werblichen Telefonanrufen gibt es sowohl datenschutzrechtliche Zuständigkeiten der örtlich zuständigen Datenschutzaufsichtsbehörden als auch wettbewerbsrechtliche Zuständigkeiten der Bundesnetzagentur (BNetzA). Die Kontrolle und Sanktionierung von Verstößen gegen das Verbot unerlaubter Telefonwerbung obliegt der BNetzA, die nach § 20 Abs. 1 Nr. 1 UWG die Kompetenz zur Verhängung von Bußgeldern für Verstöße gegen Werbeverbote hat. Die DSGVO findet in diesem Zusammenhang keine Anwendung, da die ePrivacy-Richtlinie diesen Gegenstand abschließend regelt (zu werblichen E-Mails: Europäischer Gerichtshof (EuGH), Urteil vom 13. November 2025, Rechtssache C-654/23 – Inteligo Media). Beschwerden über Cold Calls können direkt bei der BNetzA eingereicht werden, die zu diesem Zweck ein Beschwerdeformular eingerichtet hat.

Falls die Betroffenen telefonisch in den Erhalt von Leistungen eingewilligt haben, können sie diese Einwilligung per E-Mail oder Brief widerrufen. Zu zivilrechtlichen Fragen in diesem Zusammenhang beraten die Verbraucherzentralen und stellen weiterführende Informationen zur Verfügung.

Der HmbBfDI ist insbesondere zuständig, wenn es um die Erhebung und Speicherung von personenbezogenen Daten und die Erfüllung von Betroffenenrechten nach der DSGVO geht. Sollte der Geltendmachung von Betroffenenrechten von den Verantwortlichen nicht oder nicht ordnungsgemäß innerhalb eines Monats (Art. 12 Abs. 3 Satz 1 DSGVO) entsprochen werden, unterstützt der HmbBfDI die Durchsetzung der Rechte der betroffenen Personen gegenüber den Werbetreibenden.

6. Google Street View und Google Earth

Das Beschwerdeaufkommen mit Bezug auf den Dienst Street View von Google ist seit 2023 deutlich zurückgegangen. Schwerpunkte bei Beschwerden waren Aufnahmen von Personen und von privaten Wegen/Straßen. Auch die Zulässigkeit von 3D-Luftbildansichten im Dienst Google Earth hatte der HmbBfDI im Berichtszeitraum zu beurteilen.

Im Jahr 2025 verzeichnete HmbBfDI einen merklichen Rückgang von Beschwerden, die im Zusammenhang mit dem Dienst Google Street View stehen. Der Dienst wurde im Jahr 2023 von Google mit vollständig neuen Bildern neu aufgelegt, worüber bereits im Tätigkeitsbericht 2023 (vgl. 32. TB III 20 Google Street View) berichtet wurde. Es zeigte sich, dass Bürger:innen hinsichtlich der Abbildung ihrer eigenen Person in Google Street View weiterhin sensibel sind. Der Frage, wie Google bei Kamerafahrten für Google Street View gewährleistet, dass private Wege nicht befahren und Aufnahmen hiervon nicht veröffentlicht werden, ging der HmbBfDI anlässlich einiger dahingehender Beschwerden nach. Auch der Abbildung von Grundstücken in der 3D-Ansicht von Google Earth standen Beschwerdeführende skeptisch gegenüber.

Zum Teil erreichten den HmbBfDI Beschwerden, in denen Betroffene beanstandeten, dass sie oder ihre Kinder auf den Bildern in Google Street View erkennbar abgebildet seien. Zwar sind die Gesichtszüge in aller Regel verpixelt, jedoch wurde beanstandet, dass die physischen Merkmale und der Kontext der Abbildung trotz Verpixelung eine Identifizierung durch Dritte wahrscheinlich machten, was zu einer besonderen Belastung führe. Ein Beispiel hierfür ist die Beschwerde einer Person, die in der Nähe ihres Arbeitsplatzes in Street View abgebildet wurde. Obwohl das Gesicht verpixelt war, sah die betroffene Person sich durch die erkennbaren Merkmale leicht identifizierbar abgebildet und bemängelte, dass Google trotz ihres Antrags hierauf

nicht rechtzeitig und vollumfänglich ihre gesamte Person unkenntlich gemacht habe.

Der HmbBfDI vertritt hierzu die Auffassung, dass Google sicherzustellen hat, dass bei der Veröffentlichung von Aufnahmen im Dienst Street View Personen nicht anhand ihrer Gesichtszüge erkennbar sind. Zudem muss Google betroffenen Personen die Möglichkeit einräumen, Aufnahmen ihrer Person vollständig unkenntlich machen zu lassen und einen entsprechenden Antrag von Einzelpersonen zeitnah umsetzen.

Seit 2023 sind vereinzelt Beschwerden beim HmbBfDI dahingehend erhoben worden, dass Google-Fahrzeuge private Wege bzw. Straßen befahren und das Unternehmen die Aufnahmen sodann auch in Street View veröffentlicht hatte. Google hat auf Aufforderung des HmbBfDI in der Folge detailliert dargelegt, welche technischen und organisatorischen Maßnahmen das Unternehmen einsetzt, um derartige Fälle zu vermeiden. So seien die Fahrer:innen angewiesen, in dem Fall, in dem sie die unzulässige Befahrung bemerken, die Aufnahme umgehend zu stoppen, etwaig bereits erfolgte Aufnahmen im Bilderfassungstool zu markieren und zusätzlich Vorgesetzte per E-Mail über die unzulässige Aufnahme zu informieren. Derartige Meldungen würden von einem Backoffice-Team bearbeitet, damit es nicht zu einer Veröffentlichung komme. Da in den den Beschwerden zugrundeliegenden Fällen die Wege z. T. nicht mit Schildern als Privatwege gekennzeichnet waren, sagte Google zu, seine Mitarbeitenden noch einmal verstärkt darauf-hin zu schulen, zu erkennen, wann ein privater Weg bzw. eine private Straße vorliegt.

Ein weiterer Anlass für Beschwerden waren die 3D-Luftbildansichten im Google Dienst „Earth". Hier beantragten einzelne Beschwerdeführende, dass Google ihre Grundstücke in den Ansichten verpixelt, da sie befürchten, dass die Luftbildansicht Rückschlüsse auf die Nutzung oder Ausstattung ihres Grundstücks zulassen. Die Ansichten in Google Earth beruhen auf Luftbildern, die aus großer Entfernung von Satelliten oder Flugzeugen aufgenommen werden. Die 3D-Ansichten entstehen durch die Kombination von Aufnahmen aus unterschiedli-

chen Perspektiven. Die Nutzung des Luftraums und die Veröffentlichung solcher Aufnahmen sind rechtlich zulässig und die Bilder sind so gestaltet, dass keine detaillierten Einblicke in Grundstücke oder Häuser möglich sind. Zwar lassen die Ansichten z.T. Rückschlüsse auf die Nutzung oder Ausstattung eines Grundstücks zu (z. B. ob ein Wintergarten oder Gartenpool vorhanden ist) und zusätzlich bieten die 3D-Ansichten eine noch anschaulichere räumliche Visualisierung. Doch ermöglichen die Aufnahmen keine in solchem Maße stärker detaillierte Ansicht, dass die Zulässigkeit anders zu beurteilen wäre als die Zulässigkeit herkömmlicher Luftbildaufnahmen. Einblicke in Wohnhäuser sind nicht möglich und die geringe Bildauflösung verhindert konkrete Rückschlüsse auf die privaten Lebensverhältnisse der Bewohner:innen. Das öffentliche Interesse an der Möglichkeit einer Orientierung in der räumlichen Umgebung mittels Geoinformationen überwiegt insofern in der Regel. Dies gilt nach der Einschätzung des HmbBfDI auch für die 3D-Luftbildansichten von Google Earth.

Anders ist dies für den Dienst Google Street View zu beurteilen, in welchem Google Häuserfassaden auf Antrag von Eigentümer:innen oder Mieter:innen unkenntlich zu machen hat. Dies beruht darauf, dass die Aufnahmen aus unmittelbarer Nähe erfolgen und dadurch Rückschlüsse auf den Zustand des Hauses, Modell und Zustand auf dem Grundstück abgestellter Fahrzeuge oder ggf. sogar Einblicke in Wohnbereiche möglich sein können.

Der HmbBfDI sieht es als seine fortwährende Aufgabe, den Ausgleich zwischen dem Schutz der Privatsphäre und dem öffentlichen Informationsinteresse bei Google Street View zu sichern und die Rechte der Betroffenen nachhaltig zu stärken.

BERICHTE III.

Berichte

1. Einführung einer Regelanfrage zur Prüfung der Verfassungstreue: Datenschutzrechtliche Bewertung des HmbBfDI

Der HmbBfDI hat im Rahmen zweier Behördenabstimmungen zum Gesetzentwurf zur Einführung einer sog. Regelanfrage beim Landesamt für Verfassungsschutz (LfV) Stellung genommen. Während einige datenschutzrechtliche Anregungen des HmbBfDI übernommen wurden, bestehen weiterhin grundlegende Bedenken hinsichtlich der Verhältnismäßigkeit und der Ausgestaltung der geplanten Abfrage.

Im Rahmen der geplanten Änderung des Hamburgischen Sicherheitsüberprüfungs- und Geheimschutzgesetzes (HmbSÜGG) soll in § 34a HmbSÜGG eine sog. Regelanfrage eingeführt werden. Dabei soll vor einer Einstellung in den öffentlichen Dienst sowie bei weiteren Personalmaßnahmen, wie zum Beispiel der Verlängerung oder Entfristung eines Beschäftigungsverhältnisses, beim LfV abgefragt werden, ob dort Informationen vorliegen, die Zweifel an der Verfassungstreue der jeweiligen Person begründen. Die Entscheidung über die Personalmaßnahme – z. B. die Einstellung in den öffentlichen Dienst – trifft die jeweils für die Personalmaßnahme zuständige Stelle. Die geplante Regelanfrage soll für fast alle Beschäftigten des öffentlichen Dienstes der Freien und Hansestadt Hamburg gelten, sie betrifft Beamt:innen und Tarifbeschäftigte gleichermaßen. Damit wird ein sehr weiter Anwendungsbereich geschaffen. Eine flächendeckende und anlasslose Abfrage beim Nachrichtendienst ist bislang einmalig im Bundesgebiet. In anderen Bundesländern gibt es vergleichbare Regelungen bislang nur für besonders sicherheitsrelevante Bereiche oder – wie in Hamburg bisher – bestimmte Berufsgruppen.

Im Rahmen des Gesetzgebungsprozesses erfolgten zwei Behördenabstimmungen, in denen der HmbBfDI jeweils Gelegenheit zur Stellungnahme erhielt. Obwohl die Einführung einer Regelanfrage zum Zweck der Gewährleistung der freiheitlichen demokratischen Grundordnung verfassungsrechtlich möglich und legitim erscheint, meldete der HmbBfDI mehre datenschutzrechtliche Bedenken gegen die konkrete Ausgestaltung an. Dabei mahnte der HmbBfDI zur Einhaltung der Bestimmtheit und Normenklarheit des Gesetzesentwurfs und zur Klarstellung des Verhältnisses zwischen § 27 Hamburgisches Verfassungsschutzgesetz (HmbVerfSchG) und § 34a HmbSÜGG-E, die nunmehr beide die Übermittlung an öffentliche Stellen unter verschiedenen Voraussetzungen regeln. Zudem lagen Bedenken vor im Hinblick auf die Sicherstellung des sog. Trennungsgebots. Das Trennungsgebot regelt die organisatorische, rechtliche und informationelle Abgrenzung zwischen Polizei (Strafverfolgung) und Nachrichtendiensten (z. B. Verfassungsschutz). Es dient dazu, die unterschiedlichen Aufgabenbereiche – die präventive Informationsgewinnung durch Nachrichtendienste und die operative Gefahrenabwehr / Strafverfolgung durch die Polizei – klar voneinander zu trennen und eine Vermischung der Zuständigkeiten zu verhindern.

Die von § 34a Abs. 2 und 3 HmbSÜGG-E beabsichtigte Legitimierung von Regelanfragen erscheint im Ergebnis nach Auffassung des HmbBfDI insbesondere aber nicht vereinbar mit den in ständiger Rechtsprechung des Bundesverfassungsgerichts (BVerfG) entwickelten Anforderungen an die Übermittlung von Erkenntnissen von Nachrichtendiensten an inländische öffentliche Stellen. Das Gericht hat in mehreren Urteilen klargestellt, dass die Weitergabe von Informationen durch Verfassungsschutzbehörden an andere öffentliche Stellen nicht ohne sorgfältige Prüfung und nur unter bestimmten Bedingungen zulässig ist. Entscheidend ist dabei, dass die Übermittlung von Daten verhältnismäßig sein muss und nur dann erfolgen darf, wenn ein konkretes Risiko oder ein besonderes Gefahrenpotenzial vorliegt. Das Gericht hat zwar eingeräumt, dass bei Eignungsprüfungen im öffentlichen Dienst die Anforderungen gelockert werden können. Dies gilt aber nur für besonders sensible Arbeitsbereiche innerhalb der öffentlichen Verwaltung mit entsprechend hohem Schutzbedarf.

Die geplante Regelanfrage in Hamburg berücksichtigt diese Einschränkungen nicht ausreichend, da sie unabhängig von der Art der Tätigkeit oder dem Beschäftigungsfeld erfolgt. Die allgemeine Pflicht zur Verfassungstreue reicht nach Auffassung des BVerfG nicht aus, um die strengen Voraussetzungen für eine Datenübermittlung zu erfüllen. Deshalb bestehen erhebliche Zweifel daran, dass die Regelung mit dem Grundgesetz vereinbar ist.

Um den Anwendungsbereich der Regelanfrage auf ein verfassungsverträgliches Maß einzugrenzen, erscheint eine Anknüpfung an die in § 34a Abs. 2 Sätze 5 ff. HmbSÜGG-E definierten „besonders schützenswerten öffentlichen Bereiche“ denkbar. Diese Bereiche zeichnen sich durch ein erhöhtes Risiko aus. Eine solche Einschränkung würde den Anforderungen des Bundesverfassungsgerichts eher gerecht werden und die Rechte der Betroffenen besser schützen.

Im Rahmen der zweiten Behördenabstimmung wurden vom HmbBfDI vorgeschlagene Änderungen, insbesondere zur Sicherstellung des Trennungsgebots sowie zur Verbesserung der Bestimmtheit und Normklarheit des Gesetzentwurfs, berücksichtigt. Weitere vorgebrachte datenschutzrechtliche Bedenken wurden zwar zur Kenntnis genommen, jedoch wurden keine entsprechenden Änderungen vorgenommen. Insbesondere erfolgte keine Beschränkung der Regelanfrage auf sicherheitsrelevante Bereiche.

Der HmbBfDI begrüßt die im Gesetzgebungsverfahren erfolgten Anpassungen zur Sicherstellung des Trennungsgebots und zur Normklarheit, sieht jedoch weiterhin erheblichen datenschutzrechtlichen Klärungsbedarf hinsichtlich der Reichweite und Ausgestaltung der Regelanfrage.

2. Automatisierte Transkription und Protokollierung von Videokonferenzen

Die geplante Einführung der Nutzung automatisierter Transkriptionen zur anschließenden Erstellung von Protokollen von Videokonferenzen mittels LLMoin, welche bereits in verschiedenen IT-Gremien der Freien und Hansestadt Hamburg (FHH) pilotiert wird, wirft komplexe datenschutzrechtliche Fragen auf. Der HmbBfDI hat dieses Vorhaben kritisch begleitet und auf Widersprüche mit bestehenden Dienstvereinbarungen sowie Anforderungen der DSGVO hingewiesen.

Die fortschreitende Digitalisierung der öffentlichen Verwaltung führt zu einer verstärkten Nutzung digitaler Kommunikationsmittel, insbesondere auch von Videokonferenzen. Im Zuge dessen wird die Einführung automatisierter Transkriptions- und Protokollierungslösungen, etwa durch die Nutzung von Microsoft Teams (MS Teams) und die anschließende Protokollerstellung mittels eines Large Language Model (LLM), in verschiedenen IT-Gremien der Freien und Hansestadt Hamburg pilotiert. Ziel ist es, die wesentlichen Inhalte dienstlicher Besprechungen effizient und nachvollziehbar zu dokumentieren.

Der HmbBfDI hat die bisherige Umsetzung der Transkription im Rahmen der Pilotphase durch die Senatskanzlei datenschutzrechtlich begleitet und gegenüber der Senatskanzlei Bedenken geäußert, die insbesondere die Wahrung der Vertraulichkeit und den Schutz der freien Meinungsäußerung der Teilnehmenden betreffen.

Mit der Einführung von NGN (Next Generation Network) und UC-Leistungsmerkmalen (Unified Communication) wurden neue Möglichkeiten zur Unterstützung der Anrufsteuerung, der Präsenzinformationen sowie der Durchführung von Videokonferenzen geschaffen, die in der Vereinbarung nach § 94 HmbPersVG a.F. auf dem Gebiet der Telekommunikation noch nicht erfasst waren und daher schrittweise in

Ergänzungsvereinbarungen nach § 93 HmbPersVG geregelt wurden. Die geltende 3. Ergänzungsvereinbarung „NGN und einzelne Leistungsmerkmale Videokonferenz“ legt in Anlage 2 Ziffer 11 organisatorische Vorgaben für die Durchführung von Videokonferenzen sowie Aufzeichnungen von Veranstaltungsinhalten fest. Diese Regelung verbietet ausdrücklich die Aufzeichnung von Videokonferenzen und soll sicherstellen, dass Beschäftigte auch im Rahmen von dienstlichen Besprechungen, die in Form von Videokonferenzen abgehalten werden, frei und unbefangen in den inhaltlichen Austausch treten und ihre Meinung äußern können, ohne eine Aufzeichnung der einzelnen Wortbeiträge befürchten zu müssen. Funktionen zur Aufzeichnung von Bild- und Toninhalten sollen daher auch nicht angeboten werden. Die wesentlichen Inhalte einer dienstlichen Besprechung per Videokonferenz können wie bei herkömmlichen Besprechungen in Präsenz in Ergebnisprotokollen festgehalten werden.

Der HmbBfDI hat die Senatskanzlei auf die Problematik hingewiesen. Im Zuge dessen schilderte die Senatskanzlei, dass im Pilotbetrieb vorgesehen ist, dass Teilnehmende durch die Aktivierung von Kamera und Mikrofon in einem MS-Teams-Meeting ihre Einwilligung dazu erteilen, dass ihre gesprochenen Wortbeiträge transkribiert werden. Der so erstellte Text wird zur Fertigung eines Protokolls mittels „LLMoin“ weiterverarbeitet. Durch die Deaktivierung von Kamera und Mikrofon sollte diese Einwilligung widerrufen werden können. Nach einem Widerruf erfolgte keine weitere Transkription, es sei denn, das Mikrofon wurde erneut eingeschaltet. Bereits erzeugte Transkripte sollten bis zur Fertigstellung des Protokolls gespeichert und anschließend gelöscht werden. Die Senatskanzlei begründete dieses Vorgehen damit, dass die Einwilligung freiwillig erfolge, da die Teilnehmenden nicht verpflichtet seien, sich mündlich zu äußern, und zudem die Möglichkeit hätten, das Protokoll im Nachgang einzusehen und gegebenenfalls zu korrigieren.

Die Senatskanzlei ist zudem der Auffassung, dass die Transkription von Audioinhalten durch MS Teams nicht als Aufzeichnung im Sinne der 3. Ergänzungsvereinbarung zu verstehen sei, da keine synchrone

Speicherung von Ton und Bild in wiedergabefähiger Form erfolge. Die Umwandlung von Ton in Text sei vergleichbar mit manueller Mitschrift und daher zulässig. Zudem wird argumentiert, dass die Einwilligung freiwillig sei, da die Teilnahme an der Videokonferenz auch ohne Einwilligung möglich ist, wenn auch mit eingeschränkten Beteiligungsmöglichkeiten. Die Teilnehmenden würden künftig umfassend über die Transkription informiert und könnten ihre Einwilligung jederzeit durch Deaktivierung von Kamera und Mikrofon widerrufen.

Aus Sicht des HmbBfDI liegt hier jedoch eine Aufzeichnung im Sinne der Vereinbarung vor, da die Mitarbeitenden dem Zweck der Regelung nach davor geschützt werden sollten, dass ihre Wortbeiträge wörtlich festgehalten werden. Die von der Senatskanzlei zuvor genannten Anforderungen, dass keine synchrone Speicherung von Ton und Bild in wiedergabefähiger Form erfolge, ist keine Anforderung, die sich aus der 93er Vereinbarung herleiten lässt. Sie ist insofern technologieneutral formuliert. Darüber hinaus ist noch in Klärung, ob durch die Aufzeichnung und Verarbeitung von Stimmen ggf. auch biometrische Daten im Sinne von Art. 9 DSGVO erzeugt werden. Dies sollte sich aus der Datenschutzdokumentation ergeben, die auch die mit der Nutzung von LLMoin verbundenen Risiken berücksichtigen muss.

Die Verarbeitung muss entweder auf einer spezifischen gesetzlichen Grundlage (Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit einer bereichsspezifischen Norm) oder auf einer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) beruhen.

Die derzeitig gewählte Einwilligungslösung begegnet Bedenken. Die Aktivierung von Kamera und Mikrofon kann kaum als freiwillige Einwilligung interpretiert werden, wenn Beschäftigte dies tun, um in Ausübung ihrer dienstlichen Aufgabe Wortbeiträge abzugeben, und die einzige Alternative im Schweigen und gegebenenfalls Wortbeiträgen im Chat besteht. In Ausnahmekonstellationen, in denen sich kleine Arbeitsgruppen aus sich heraus entschließen, zur Ergebnissicherung eine Transkriptionsfunktion zu nutzen, mag eine freiwillige Einwilligung möglich sein. Als Rechtsinstrument für den großflächigen Einsatz in

wiederkehrenden Besprechungsrunden mit großem Teilnehmendenkreis steht die Einwilligung auf tönernen Füßen.

Dem Senat ist vor diesem Hintergrund zu raten, eine FHH-weite Dienstvereinbarung mit den Spitzenorganisationen der Gewerkschaften zu schließen und damit eine Rechtsgrundlage zu schaffen. Die Fragestellung, in welcher Art von Besprechung welcher Umfang der Inhaltsaufzeichnung notwendig und zielführend ist, ohne den freien Meinungsaustausch zu behindern, bedarf einer konkreten und differenzierten Beantwortung. Ausgewogene Vereinbarungen nach § 93 HmbPersVG bieten dafür den richtigen und rechtssicheren Rahmen.

3. KoPers 2027

Im Projekt KoPers 2027 wird das bestehende IT-Fachverfahren KoPers auf die neue IT-Infrastruktur LogaHR umgestellt. Der HmbBfDI begleitet das Vorhaben seit September 2024 und hat insbesondere die Nutzung von Originaldaten im parallelen Testbetrieb kritisch geprüft.

Das Projekt sieht vor, das bisherige KoPers-Verfahren, welches bislang als On-Premise-Installation bei Dataport betrieben wird und auf einer Oracle-SQL-Datenbank basiert, auf die neue IT-Infrastruktur LogaHR von P&I mit PostgreSQL-Datenbank zu migrieren. Die neue Produktionsumgebung wird als Appliance der P&I im Dataport-Rechenzentrum betrieben.

Um die Praxistauglichkeit, Stabilität und einen ordnungsgemäßen Betrieb des neuen Systems vor der geplanten Produktivsetzung sicherzustellen, ist ein zwölfmonatiger Parallelbetrieb von LogaHR und dem bisherigen KoPers-Verfahren geplant. Hierfür soll eine 1:1-Kopie der Produktivdaten aus dem Mandanten 430 auf die neue Projektumgebung übertragen werden. Das Zentrum für Personaldienste (ZPD) hat nach eigener Prüfung festgestellt und dargelegt, dass ergänzend zu

durchzuführenden Tests mit Testdaten ein Parallelbetrieb der Verfahren notwendig sei. Ohne diesen direkten und umfassenden Vergleich auf der Basis von Originaldaten könnten Fehler oder Schwachstellen erst nach der Umstellung erkannt werden, was erhebliche Störungen verursachen könnte.

Im Rahmen der Regelabstimmung im März 2025 äußerte der HmbBfDI datenschutzrechtliche Bedenken. Er verwies auf die § 93er-Vereinbarung zu KoPers, die im Rollen- und Berechtigungskonzept (Anlage 5) ausdrücklich festlegt, dass Entwicklungs- und Testsysteme keine Echtdaten enthalten dürfen. Zudem steht die geplante Vorgehensweise im Widerspruch zur Freigaberichtlinie, die den Einsatz von Originaldaten zu Testzwecken nur in Ausnahmefällen erlaubt. Ende Juli 2025 bestätigte das ZPD, dass die bisherige Fassung der Anlage 5 der § 93er-Vereinbarung zu KoPers die Verarbeitung von Echtdaten außerhalb der Produktionsumgebung nicht vorsieht, informierte den HmbBfDI aber, dass eine Änderung geplant ist, um künftig die Verarbeitung von Echtdaten auch in produktionsähnlichen Umgebungen zu ermöglichen. Im Oktober 2025 wurde der HmbBfDI über ein Änderungsverfahren informiert, das die Streichung des entsprechenden Passus vorsieht. Die Gewerkschaften erhoben keine Einwände, sodass die Änderung als genehmigt gilt. In der Regelabstimmung im Dezember 2025 teilte die Projektgruppe zudem mit, dass seit November 2025 eine neue Freigaberichtlinie gelte, deren Voraussetzungen erfüllt seien. Damit konnten die anfänglichen datenschutzrechtlichen Bedenken hinsichtlich der bisherigen Verbotsvorschrift ausgeräumt werden.

Die neue inhaltliche Ausrichtung der Regelungsänderung wirft jedoch weiterhin datenschutzrechtliche Bedenken auf. Die bloße Streichung des Verbots der Echtdatennutzung in Testsystemen genügt den Anforderungen der DSGVO nicht. Tests mit Echtdaten müssen auf ein absolutes Minimum beschränkt bleiben und setzen voraus, dass die Testung nicht anders durchführbar ist. Zudem sind die Grundsätze der Zweckbindung und Datenminimierung gemäß Art. 5 Abs. 1 lit. b DSGVO zu beachten. Eine Verarbeitung zu Testzwecken bedarf einer eigenständigen Rechtsgrundlage nach Art. 6 Abs. 4 DSGVO und muss

im Einzelfall begründet werden. Die geänderte Vereinbarung schafft zwar eine organisationsrechtliche Grundlage, ersetzt aber nicht die erforderliche datenschutzrechtliche Prüfung und Dokumentation jedes einzelnen Testfalls.

Aus diesem Grund hat der HmbBfDI in seiner letzten Stellungnahme im Dezember 2025 daraufhin hingewiesen, dass bei Tests mit echten Personalfällen die Verhältnismäßigkeit weiterhin gewahrt bleiben muss. Da auch die neue Freigaberichtlinie der FHH ausdrücklich vorsieht, dass bei der Durchführung und Auswertung der Tests die schutzwürdigen Belange der Betroffenen sowie die Datensicherheit angemessen berücksichtigt werden, muss sichergestellt sein, dass nur Personen mit Vertraulichkeitsverpflichtungen Zugriff auf die Daten erhalten und ausschließlich die mit der Fehlerbehebung und Durchführung des Tests betrauten Personen die Daten nutzen dürfen. Es darf nicht passieren, dass Daten aus dem Parallelbetrieb in die Produktion oder an Dritte gelangen. Die Verwendung von Originaldaten muss revisionssicher dokumentiert werden, und Fortschreibungen des KoPers-Berechtigungs- und Sicherheitskonzepts sind zeitnah zu kommunizieren. Das KoPers-Berechtigungs- und Sicherheitskonzept bleibt weiterhin gültig und wird im Projekt fortentwickelt. Dies ist aus Sicht des HmbBfDI nur eingeschränkt nachvollziehbar, da es sich um ein neues Verfahren mit neuer Datenbank und neuen Schnittstellen handelt. Zudem ist davon auszugehen, dass im Testbetrieb andere Berechtigungen gelten als in der Produktion, beispielsweise für Testpersonen statt Sachbearbeitende. Es bleibt daher abzuwarten, wie die Konzepte konkret fortentwickelt werden.

Nach den vorgelegten Unterlagen erfolge der Parallelbetrieb mit Originaldaten nicht unter Produktionsbedingungen, sondern in einer produktionsnahen Umgebung innerhalb eines produktionsvorbereitenden Systems. Abweichungen von den Produktionsbedingungen müssen nachvollziehbar dokumentiert, begründet und hinsichtlich des daraus jeweils resultierenden Risikos bewertet werden. Der HmbBfDI empfahl daher, dass dieses denselben Sicherheitsmaßnahmen unterliegen soll wie das Produktionssystem.

Der HmbBfDI wird das Projekt KoPers 2027 weiterhin eng begleiten und steht für einen konstruktiven Dialog zur Sicherstellung eines datenschutzkonformen Umgangs mit den Personaldaten zur Verfügung.

4. Elektronisches Posteingangsbuch (EPob)

Den gesamten Briefposteingang einer Stadt zentral zu erfassen und zu scannen kann eine sinnvolle Maßnahme zur Entlastung der Verwaltung sein. Es stellen sich dabei aber auch einige Herausforderungen für den Datenschutz, z. B. wenn besonders sensible Daten im Sozialbereich betroffen sind.

Das Verfahren der Elektronischen Posteingangsbearbeitung (ePob) der Freien und Hansestadt Hamburg, bei dem die Kasse Hamburg als zentraler Scan-Dienstleister fungiert, wurde vom HmbBfDI umfassend datenschutzrechtlich bewertet. Wie bereits in den vorangegangenen Tätigkeitsberichten dargestellt, ist Ziel des Projekts das zentrale Einscannen von Papierposteingängen aus öffentlichen Stellen der FHH. Der HmbBfDI hat das Vorhaben bewertet im Hinblick auf die bisherige Ausbaustufe, insbesondere auf den Scanprozess in der Kasse Hamburg, nicht jedoch auf die nachgelagerten Verarbeitungsschritte.

Die erneute Besichtigung der Scanstraße im Berichtszeitraum bestätigte einen insgesamt guten Eindruck der Arbeitsabläufe, wobei der Fokus der datenschutzrechtlichen Diskussion auf der Mandantentrennung und der differenzierten Behandlung von Schutzstufen liegt. Die Kasse.Hamburg hat mit allen beteiligten Stellen Auftragsverarbeitungsverträge geschlossen und verfolgt das Ziel, durchgehend hohe Schutzbedarfsanforderungen zu erfüllen, ohne jedoch eine separate Trennung der Scanaufträge oder der Mitarbeitenden vorzunehmen. Lediglich für Postzustellungsurkunden im OWi-Verfahren wurde eine Siegelung integriert. Alle Mitarbeitenden sind zur Verschwiegenheit verpflichtet, auch jene der Elbe Werkstätten, die im Projekt mitwirken.

Die Mandantentrennung bei der Aufbewahrung der Papieroriginale ist jedoch nur eingeschränkt umgesetzt, da eine organisatorische und räumliche Trennung nicht realisiert wird.

Zur Verantwortlichkeit wird festgehalten, dass die Kasse Hamburg als Auftragsverarbeiterin agiert und die Fachbehörden als Verantwortliche gelten. Von Bestrebungen, der Kasse Hamburg eine eigenständige Verantwortlichkeit einzuräumen, z. B. durch eine gesetzliche Verantwortlichkeitszuweisung, rät der HmbBfDI ab. Eine eigenständige datenschutzrechtliche Rechtsgrundlage für die Kasse Hamburg fehlt zum einen, weshalb die Auftragsverarbeitungsverträge unter Gesichtspunkten der Rechtmäßigkeit essenziell sind. Insbesondere im Bereich des Sozialdatenschutzes ist zum anderen eine getrennte Verantwortlichkeit problematisch, da die Verarbeitung dort auf spezifischen gesetzlichen Befugnissen beruht. Die Beibehaltung der Auftragsverarbeitungsverträge wird daher ausdrücklich empfohlen.

Die TR Resiscan, eine technische Richtlinie des BSI zum rechtsicheren ersetzenden Scannen, bildet die Grundlage für die Umsetzung technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO. Das Verfahren orientiert sich an einem hohen Schutzbedarf, da sensible Datenkategorien, darunter Gesundheits- und Sozialdaten, verarbeitet werden. Die Entscheidung, eine einzige Scanstraße mit hohen Schutzanforderungen zu betreiben, wird begrüßt, da eine differenzierte Behandlung verschiedener Schutzstufen organisatorisch schwierig wäre. Die TR Resiscan fordert unter anderem Zugangsbeschränkungen, Protokollierung und regelmäßige Auditierungen, um Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen.

Während die Zutrittsbeschränkungen und Verschwiegenheitsverpflichtungen als ausreichend bewertet werden, besteht erheblicher Verbesserungsbedarf bei der Aufbewahrung der Papieroriginale. Diese werden derzeit in offenen Regalen zwar in Kartons nach laufenden Vorgangsnummern sortiert, aber ohne Mandantentrennung im eigentlichen Sinne gelagert. Diese Praxis verletzt den Grundsatz der Zweckbindung und Vertraulichkeit. Ein kontrollierter, protokollierter

Zugang, etwa durch eine Registratur, die nur auf Anfrage hin Zugang gewährt, wird als praktikable und notwendige Maßnahme empfohlen, um unbefugten Zugriff zu verhindern und die Anforderungen der TR Resiscan zu erfüllen.

Die Protokollierung der Scanvorgänge und die regelmäßige Auditierung der Informationssicherheitsmaßnahmen sind bislang unzureichend umgesetzt. Insbesondere wird eine externe Auditierung empfohlen, um die Einhaltung der hohen Schutzanforderungen unabhängig zu überprüfen und dauerhaft nachweisbar gewährleisten zu können. Weitere Maßnahmen bei hohen Vertraulichkeits- und Integritätsanforderungen umfassen die Sensibilisierung der Mitarbeitenden, die Verhinderung ungesicherter Netzzugänge, den Einsatz kryptographischer Verfahren zum Integritätsschutz sowie eine erweiterte Qualitätssicherung der Scanprodukte. Aktuell findet keine systematische Qualitätskontrolle statt und die im Qualitätssicherungskonzept vorgesehene Stichprobenprüfung konnte nicht nachgewiesen werden.

Die übermittelten Unterlagen, darunter die Strukturanalyse und das Berechtigungskonzept, weisen Lücken auf. Die Strukturanalyse ist unvollständig, insbesondere fehlen Angaben zu eingesetzten IT-Systemen und Netzwerken. Das Berechtigungskonzept wurde an die neue Authentisierungsrichtlinie der FHH angepasst, jedoch wird die dort angenommene Multifaktor-Authentifizierung durch den Besitz eines Dienstrechners vom HmbBfDI nicht als ausreichend anerkannt, da dieser nicht individuell einer Person zugeordnet ist. Die Verantwortung für zusätzliche Authentifizierungsmaßnahmen wird unklar auf die nutzenden Behörden verlagert, was angesichts der zentralen Rolle der Kasse Hamburg im Verfahren kritisch gesehen wird.

Die Verfahrensbeschreibung wurde um die eingesetzte KI-Komponente IRIS / xTract ergänzt, jedoch fehlen detaillierte Angaben zum Einsatz und zur Datenverarbeitung. Die Vernichtung der Papierunterlagen erfolgt nach datenschutzrechtlichen Empfehlungen, wobei aufgrund fehlender Trennung aller Unterlagen nach der höchsten Vertraulichkeitsstufe vernichtet werden müssen.

Zusammenfassend ist das Verfahren ePob grundsätzlich datenschutzgerecht umsetzbar und für die Nutzung durch öffentliche Stellen der FHH geeignet, auch bei hohem Schutzbedarf der Daten. Allerdings erfüllt das aktuelle Verfahren die hohen Schutzanforderungen insbesondere hinsichtlich der Aufbewahrung der Papieroriginale, der Protokollierung, Auditierung und Qualitätssicherung nicht vollständig. Die Umsetzung der TR Resiscan und die vertragliche Absicherung der Schutzmaßnahmen sind essenziell, um die rechtliche Gleichwertigkeit der digitalen Kopien zu gewährleisten und die Vernichtung der Papieroriginale zu rechtfertigen. Der HmbBfDI sieht in den vorgeschlagenen Maßnahmen praktikable Lösungsansätze und wird die Umsetzung der Empfehlungen im Jahr 2026 überprüfen.

5. M365 in der öffentlichen Verwaltung

Der Senat führt M365 für die überwiegende Zahl der Dienstrechner in der FHH ein. Der HmbBfDI hat das Projekt beratend begleitet. Auf Basis der gegenüber Microsoft erwirkten vertraglichen Verbesserungen und der mit dem Senat abgestimmten Einstellungen ist der Einsatz bei nichtsensiblen Daten vertretbar. Bei Daten mit hohem Schutzbedarf sind hingegen noch zahlreiche Fragen zum Schutzkonzept offen.

Auch im Jahr 2025 wurde das Projekt BestCloudBasis der Senatskanzlei Hamburg (SK) datenschutzrechtlich intensiv begleitet. Ziel des Projekts ist die Einführung von Microsoft 365 (M365) zur Verarbeitung personenbezogener Daten mit normalem Schutzbedarf. Die datenschutzrechtliche Begleitung durch den HmbBfDI begann Mitte 2023 mit der Prüfung eines Nutzungskonzepts und wurde durch mehrere Workshops und kontinuierlichen Austausch bis Ende September 2025 fortgeführt.

Die Prüfung konzentrierte sich auf die Einhaltung der Verarbeitungsgrundsätze gemäß Art. 5 DSGVO für nicht sensible Daten. Aufgrund

der Komplexität von M365, das vielfältige Cloud-Dienste und komplexe Datenströme umfasst, war ein besonderes Augenmerk auf ein umfassendes Risikomanagement und die Einhaltung der Weisungsbefugnis nach Art. 28 DSGVO erforderlich. Die Verarbeitung von Daten mit hohem Schutzbedarf oder sensiblen Kategorien (Art. 9 DSGVO) wurde bislang noch nicht abschließend bewertet, da die Konkretisierungen der dahingehenden Schutzmaßnahmen bei der Senatskanzlei noch in Klärung sind. Die Thematik bleibt Gegenstand weiterer Prüfungen.

Im Rahmen der Begleitung wurden umfangreiche Dokumentationen bereitgestellt, darunter eine Datenschutzfolgeabschätzung, detaillierte Verarbeitungstätigkeitsbeschreibungen sowie Feinkonzepte zu zentralen Anwendungen wie SharePoint, Teams und OneDrive. Ergänzt wurden diese durch Sicherheits- und Governancekonzepte, die eine risikozentrierte Prüfung und die Erfüllung der Rechenschaftspflichten ermöglichen. Aufgrund geplanter Erweiterungen, etwa durch die Integration von Copilot Chat und MS Forms, ist eine umfassende Überarbeitung der Dokumentation für Ende 2025 vorgesehen.

Die Verantwortlichkeitsverteilung zwischen der Senatskanzlei als zentrale IT-Infrastrukturverantwortliche und den Fachbehörden als Verantwortliche für die Verarbeitung ihrer jeweiligen Inhaltsdaten ist derzeit noch nicht abschließend geklärt. Die SK sieht sich gemäß § 14 HmbVwDiG als Verantwortliche für die zentrale IT-Infrastruktur, während die Fachbehörden für die inhaltliche Datenverarbeitung zuständig bleiben. Diese Aufteilung könnte mit der DSGVO zwar grundsätzlich vereinbar sein, bedarf jedoch noch einer abschließenden datenschutzrechtlichen Dokumentation und Prüfung der zugrundeliegenden Rechtsgrundlagen.

Ein wesentlicher Bestandteil der datenschutzrechtlichen Absicherung ist der Auftragsverarbeitungsvertrag (AVV) mit Microsoft, der durch eine Zusatzvereinbarung ergänzt wurde. Diese Zusatzvereinbarung adressiert zentrale datenschutzrechtliche Bedenken und regelt die Rechte und Pflichten beider Parteien im Rahmen der Auftragsverarbeitung. Microsoft verpflichtet sich darin, ausschließlich im Auftrag

und nach Weisung der SK tätig zu werden. Die Zusatzvereinbarung enthält unter anderem folgende wichtige Regelungen:

- Einschränkungen bei einseitigen Vertragsänderungen durch Microsoft, um eine nachträgliche Verschlechterung der Datenschutzbedingungen zu verhindern.
- Klare Zusicherungen zur Einhaltung der DSGVO, insbesondere hinsichtlich der Verarbeitung personenbezogener Daten und der Umsetzung technischer und organisatorischer Maßnahmen.
- Ausschluss der Nutzung von Kundendaten für das Training von Künstlicher Intelligenz (KI), um eine unautorisierte Weiterverwendung der Daten zu verhindern.
- Stärkung der Weisungsbefugnis der Freien und Hansestadt Hamburg (FHH) gegenüber Microsoft, um die Kontrolle über die Datenverarbeitung sicherzustellen.
- Vorrang des EU-Rechts bei Drittstaatenübermittlungen, insbesondere im Hinblick auf den Zugriff durch Behörden außerhalb der EU.
- Ausweitung des EU Data Boundary, sodass die Datenverarbeitung und -speicherung ausschließlich innerhalb der EU erfolgt, um den Schutz personenbezogener Daten zu gewährleisten.

Bezüglich der Verarbeitung von Daten zu eigenen Zwecken durch Microsoft konnte glaubhaft dargelegt werden, dass Microsoft ausschließlich pseudonymisierte Telemetrie- und Diagnosedaten verarbeitet. Diese dienen der Verbesserung der Dienste und der Fehlerbehebung. Inhaltsdaten der Kunden werden nicht für eigene Zwecke verarbeitet. Die Telemetriedaten umfassen technische Informationen zur Nutzung und Leistung der Dienste und werden in aggregierter und anonymisierter Form ausgewertet. Die Prozesse zur Erstellung von Reports sowie zur Anonymisierung und Aggregation der Daten wurden erläutert, wobei noch Detailfragen offen sind, insbesondere hinsichtlich der Kriterien und Verfahren zur Genehmigung der Reports. Die Rückführbarkeit der Telemetriedaten auf einzelne Personen wird als sehr gering eingeschätzt, was das Risiko einer Identifikation minimiert. Dennoch wird eine weitere Klärung der genauen

Anonymisierungsverfahren und der Kontrollmechanismen empfohlen, um Transparenz und Datenschutzkonformität sicherzustellen.

Die Drittstaatenübermittlung, insbesondere in die USA, wird durch die EU Data Boundary von Microsoft, das EU-US Data Privacy Framework sowie die vertraglichen Schutzmaßnahmen im AVV zumindest derzeit ausreichend adressiert. Dabei gilt es, die politischen Entwicklungen in den USA im Blick zu halten (siehe Kap. VI 1). Auf Aufforderung des HmbBfDI hin hat die Senatskanzlei eine Exit-Strategie für den Fall entwickelt. Diese setzt sich mit dem möglichen Szenario auseinander, dass sich der kurzfristige Bedarf ergibt, die Daten aus der Microsoft-Cloud zurückzuholen oder dass Microsoft die Dienstleistung für die Stadt Hamburg abrupt beendet. Nach derzeitigem Stand werden allerdings keine Backups bei Dataport erstellt, sodass bei plötzlichen und unvorhergesehenen Maßnahmen durch Microsoft die Verfügbarkeit der Daten gefährdet wäre. Zudem stünde im Fall des Exits keine Software zur Verfügung, die langfristig und in gleichem Leistungsumfang den nahtlosen Weiterbetrieb der Datenverarbeitungen in der FHH gewährleisten würde.

Die SK verzichtet auf die Microsoft Customer Lockbox zugunsten eines vergleichbaren Zugriffsverbots im Servicevertrag mit Dataport, um unautorisierten Zugriff auf Kundendaten zu verhindern. Zudem wird eine belastbare Exit- und Backup-Strategie empfohlen, um auf mögliche politische Veränderungen flexibel reagieren zu können.

Die Liste der Microsoft-Unterauftragsverarbeiter wurde aktualisiert und entspricht den Anforderungen für die Verarbeitung von Daten mit normalem Schutzbedarf. Die Konfigurationsmöglichkeiten für verbundene Erfahrungen („connected experiences“) wurden verbessert, sodass eine feingranulare Deaktivierung möglich ist. Die SK deaktiviert Microsoft-Dienste, die als eigenständige Verantwortliche auftreten, soweit dies datenschutzrechtlich erforderlich ist. Gleichzeitig werden barrierefördernde Funktionen wie die Transkription in Teams unter Beachtung der Rechtsgrundlagen genutzt.

Die technische Konfiguration von M365 ist teilweise noch unvollständig dokumentiert, insbesondere fehlen Feinkonzepte für Kernanwendungen wie Word oder Excel. Die SK arbeitet an einer besseren Dokumentation und Transparenz der Konfigurationen, um die Rechenschaftspflicht zu gewährleisten. Vorgestellte Sicherheitsprofile sollen auch für den normalen Schutzbedarf angemessene Sicherheitsniveaus bieten.

Telemetrie-Messungen zur Analyse der durch M365 ausgelösten Datenströme zeigen keine Auffälligkeiten und werden regelmäßig wiederholt, was als risikominimierend bewertet wird.

Insgesamt wurde der Stand des Projekts zum 30. September 2025 als datenschutzrechtlich vertretbar bewertet. Die Verarbeitungsgrundsätze des Art. 5 DSGVO für Daten mit normalem Schutzbedarf werden in angemessenem Maße eingehalten. Die Zusatzvereinbarung mit Microsoft schafft eine solide Grundlage zur Minimierung der Risiken aus der Auftragsverarbeitung und Drittstaatenübermittlung. Offene Fragen, insbesondere zur Reporterstellung und zur Verarbeitung verbundener Erfahrungen, bleiben bestehen und werden weiterverfolgt. Die Bewertung steht unter dem Vorbehalt der angekündigten Dokumentationsüberarbeitungen und weiterer Rückmeldungen.

Zunächst vom Senat ausgeklammert war die Frage des Umgangs mit Behörden und Arbeitsplätzen, die Daten mit hohem Schutzbedarf verarbeiten. Dies können beispielsweise Rechner der Polizei oder von Sozialträgern sein. Die dort anfallenden Informationen sind besonders zu sichern gegen die missbräuchliche Einsichtnahme oder Verwendung durch Unberechtigte. Zum einen sind Maßnahmen gegen das versehentliche Teilen sensibler Informationen in einem unbeabsichtigt weiten Empfängerkreis vorzusehen. Dies kann mittels strikter Voreinstellungen erreicht werden. Zum anderen sind Schutzvorkehrungen wie resistente Multi-Faktor-Authentifizierung gegen Phishing-Angriffe von außen vorzusehen. Es gilt den Angriffsvektor zu minimieren, dass sich Kriminelle durch einen Phishing-Angriff Zugang zu dem Profil einzelner Beschäftigter verschaffen, die als Einfallstor für die Daten anderer Arbeitsplätze und auch Behörden genutzt werden können. Die

Senatskanzlei hat erst spät mit dem Prozess begonnen, entsprechende konkrete technische Maßnahmen auszuwählen und zu spezifizieren. Sie beabsichtigt derzeit, den jeweiligen einsetzenden Behörden die Wahl zwischen zwei Varianten zu überlassen, dem Sicherheitsprofil Standard und dem Sicherheitsprofil Plus. Nach Einschätzung der Senatskanzlei sollen beide Profile für die Verarbeitung von Daten mit hohem Schutzbedarf geeignet sein. Dieses Ziel ist zu begrüßen, jedoch sind die Planungen, welche Maßnahmen in welcher technischen Umsetzung in den jeweiligen Sicherheitsprofilen integriert sein können, noch relativ abstrakt. Auch die Kosten, die auf die jeweiligen Behörden bei der Wahl des höheren Sicherheitsprofils entfallen, sind noch nicht bekannt. Aus diesen Gründen hat der HmbBfDI erwirkt, dass ein für den November 2025 geplanter Beschluss des behördenübergreifenden Anwendergremiums ITAB zurückgestellt wurde. Dieser sah eine Vorfestlegung der voraussichtlichen Geeignetheit auch des Standardprofils für hohen Schutzbedarf vor.

Der HmbBfDI setzt seine regelmäßige Workshopreihe mit dem Senat fort und konzentriert sich darin auf die zu ergreifenden Maßnahmen bei hohem Schutzbedarf. Die Senatskanzlei ist derzeit damit befasst, diese weiter auszuarbeiten und zeigt sich offen für die Übernahme konkreter Vorschläge des HmbBfDI.

6. Begriff des Schutzbedarfs

Der Begriff des Schutzbedarfs und seine Feststellung wird bei vielen IT-Projekten auch im datenschutzrechtlichen Kontext verwendet. Die Begriffsherkunft aus dem Bereich der IT-Sicherheit ist jedoch nicht vollständig deckungsgleich mit der datenschutzrechtlichen Begriffswelt. Daher bedurfte es einer Begriffsklärung.

Der Begriff „Schutzbedarf“ ist im Datenschutzrecht nicht explizit definiert, sondern stammt primär aus dem IT-Sicherheitsmanagement. Im

Kontext der DSGVO wird stattdessen das „Schutzniveau“ gemäß Art. 32 als Maßstab für die Sicherheit der Verarbeitung personenbezogener Daten herangezogen, das sich an der Risikobewertung für die Rechte und Freiheiten betroffener Personen orientiert. Diese Risikobewertung ist insbesondere in Art. 35 DSGVO geregelt, der eine Datenschutz-Folgenabschätzung (DSFA) bei voraussichtlich hohem Risiko verlangt. Die Pflicht zur Schutzbedarfsfeststellung ergibt sich somit implizit aus der Verpflichtung zur Risikoanalyse und zur Dokumentation der Schutzmaßnahmen, ohne dass Art. 32 eine eigenständige, über Art. 35 hinausgehende Pflicht begründet.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verwendet den Begriff Schutzbedarf im Rahmen des IT-Grundschutzes, der auf die Schutzinteressen der Institution und deren IT-Assets abzielt. Die Schutzbedarfsfeststellung nach BSI erfolgt anhand der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit und klassifiziert den Schutzbedarf in die Kategorien „normal“, „hoch“ und „sehr hoch“. Dabei werden Schadensszenarien wie finanzielle Auswirkungen oder Beeinträchtigung der Aufgabenerfüllung berücksichtigt. Datenschutzrechtlich ist diese Methode nur bedingt geeignet, da sie den Schutz der Rechte und Freiheiten natürlicher Personen nur indirekt über die IT-Sicherheitsziele abbildet. Eine Schutzbedarfsfeststellung nach IT-Grundschutz kann jedoch als ergänzender Beitrag zur Bestimmung des erforderlichen Schutzniveaus dienen.

Das Standarddatenschutzmodell (SDM) der Datenschutzkonferenz (DSK) bietet eine datenschutzrechtlich spezifische Methodik zur Schutzbedarfsfeststellung, die auf sieben Gewährleistungszielen basiert, darunter neben Vertraulichkeit, Integrität und Verfügbarkeit auch Datenminimierung, Transparenz und Intervenierbarkeit. Das SDM definiert den Schutzbedarf als das Risiko für die Rechte und Freiheiten der betroffenen Personen vor technischen und organisatorischen Maßnahmen. Die Schutzbedarfsfeststellung erfolgt hier durch eine systematische Risikoanalyse, die sowohl die Daten als auch die IT-Systeme und Prozesse umfasst. Das SDM berücksichtigt auch Risiken der IT-Sicherheit und empfiehlt bei Widersprüchen zwischen

SDM und IT-Grundschutz den höheren Schutzbedarf zugrunde zu legen. Aufgrund seiner datenschutzrechtlichen Ausrichtung gilt das SDM als geeigneteres Instrument zur Feststellung des erforderlichen Schutzniveaus.

Spezialgesetzliche Regelungen, wie die eIDAS-Verordnung zur elektronischen Identifizierung oder Geheimschutzvorschriften, können zusätzliche oder abweichende Schutzbedarfsbewertungen vorgeben, die im Rahmen der datenschutzrechtlichen Schutzbedarfsfeststellung zu berücksichtigen sind. Diese spezialgesetzlichen Vorgaben können einerseits eine Abkürzung für die Risikobewertung darstellen, andererseits aber auch zu Wertungswidersprüchen führen, die durch eine umfassende Risikobewertung aufgelöst werden müssen.

Zur Operationalisierung existiert beispielsweise das Schutzstufenkonzept des Landes Niedersachsen, das Schutzstufen anhand von Datenkategorien und Risiken tabellarisch darstellt. Für Hamburg wird eine Weiterentwicklung dieses Ansatzes vorgeschlagen, die auch die Zuordnung technisch-organisatorischer Maßnahmen (TOM) umfasst. Eine Darstellung mit beispielhafter Beschreibung von möglichen TOMs sieht dann wie folgt aus:

- **Schutzstufe A (normal):**
  - Daten: Öffentlich zugängliche personenbezogene Daten (z. B. Telefonverzeichnis, frei zugängliche Webseiten, soziale Medien).
  - Schadenspotenzial: Keine besondere Beeinträchtigung zu erwarten.
  - Maßnahmen: Grundlegende Zugangskontrollen (Passwörter), Mitarbeiterschulungen, einfache Firewall-Konfiguration, Basis-Datenschutzrichtlinien.

- **Schutzstufe B (normal):**
  - Daten: Nicht frei zugängliche, aber geringfügig schädliche Daten (z. B. beschränkt zugängliche öffentliche Dateien, Grundbucheinsicht, nicht frei zugängliche soziale Medien).

  - » Schadenspotenzial: Geringfügig.
  - » Maßnahmen: Zusätzlich zu A regelmäßige Backups, Standardverschlüsselung, grundlegende Zugangs- und Zugriffskontrollen.

- **Schutzstufe C (hoch):**
  - » Daten: Daten, deren unsachgemäße Handhabung das Ansehen oder wirtschaftliche Verhältnisse beeinträchtigen kann (z. B. Einkommen, Grundsteuer, Ordnungswidrigkeiten).
  - » Schadenspotenzial: Überschaubar.
  - » Maßnahmen: Multi-Faktor-Authentifizierung, regelmäßige Sicherheitsaudits, stärkere Verschlüsselungsstandards, umfassendere Schulungen, detaillierte Protokollierung und Überwachung.

- **Schutzstufe D (hoch):**
  - » Daten: Daten mit erheblicher Beeinträchtigungspotenz (z. B. Gesundheitsdaten, biometrische Daten, Sozialdaten, dienstliche Beurteilungen, Daten nach Art. 9 DSGVO, Daten Minderjähriger).
  - » Schadenspotenzial: Substantiell.
  - » Maßnahmen: Ergänzend zu C Penetrationstests, Red-Teaming, VLAN-Trennung, Intrusion Prevention System (IPS).

- **Schutzstufe E (sehr hoch):**
  - » Daten: Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit gefährdet (z. B. Zeugenschutzprogramm, Opferdaten strafbarer Handlungen).
  - » Schadenspotenzial: Sehr hoch.
  - » Maßnahmen: Physikalische Abschottung (Air-Gapping), Penetrationstests, Red-Teaming, kontinuierliche Überwachung durch CERT-Teams, KI-basierte Advanced Threat Detection, hochsichere Authentifizierung, strenge Zugriffskontrollen, Echtzeitalarme.

– **Schutzstufe F (sehr hoch):**
  » Daten: Nicht personenbezogene, aber geheimhaltungspflichtige Daten (z. B. Verschlusssachen).
  » Schadenspotenzial: Sehr hoch.
  » Maßnahmen: Wie bei E.

Dabei ist zu beachten, dass Schutzbedarfsfeststellungen stets einzelfallbezogen und iterativ erfolgen müssen, sich auf die zu verarbeitenden Daten und nicht auf die gesamte Stelle beziehen und dass ein hoher Schutzbedarf für einzelne Datenbereiche das gesamte IT-System entsprechend absichern muss.

Abschließend wird festgehalten, dass die DSGVO keine eigenständige Schutzbedarfsfeststellung verlangt, sondern eine risikoadäquate Verfahrensgestaltung und Risikoanalyse fordert. Die Schutzbedarfsfeststellung nach IT-Grundschutz ist für den Datenschutz nur ergänzend relevant, während das SDM als datenschutzrechtlich fundierte Methode zu bevorzugen ist. Die Aufsicht durch den HmbBfDI beschränkt sich auf die Überprüfung der risikoadäquaten Verfahrensgestaltung im Sinne des Datenschutzes; rein IT-sicherheitsbezogene Schutzbedarfsfeststellungen ohne Bezug zu den Rechten und Freiheiten Betroffener sind nicht Gegenstand der Aufsicht.

7. Überwachung bei IPad Nutzung an Schulen

Lehrkräfte müssen im analogen wie auch im digitalen Unterricht die Möglichkeit haben, zu überprüfen, ob die Schüler:innen dem Unterricht folgen oder sich mit unterrichtsfernen Dingen beschäftigen. Dabei sind die Überwachungsmöglichkeiten, die digitale Geräte wie Tablets bieten, datenschutzkonform auszugestalten.

Im Juli 2025 hat der HmbBfDI durch eine Presseanfrage davon erfahren, dass die Apple App „Classroom“ in den Jahrgangstufen 10

bis 12 an einem Hamburger Gymnasium eingesetzt wird. Diese App soll es Lehrkräften ermöglichen, den Unterricht auf Schülergeräten zu verwalten, zu steuern und zu überwachen. Mit dieser App können die Lehrkräfte Zugriff auf die privaten iPads der Schüler:innen nehmen. So soll kontrolliert werden, ob dies während des Unterrichts für unterrichtsfremde Zwecke genutzt werden.

Der konkrete Fall oder vergleichbare Fälle waren dem HmbBfDI bis dahin nicht bekannt. Er hat die Presseanfrage daher zum Anlass genommen, den konkreten Softwareeinsatz an der fraglichen Schule näher zu beleuchten.

Während das Ansinnen der Schulen, unterrichtsferne Nutzungen privater Endgeräte während der Unterrichtsstunde zu unterbinden, grundsätzlich nachvollziehbar und nach hiesiger Einschätzung auch datenschutzkonform umsetzbar sein kann, sind aber gewisse Rahmenbedingungen einzuhalten. Es ist sicherzustellen, dass der Zugriff durch die Lehrkräfte ausschließlich während des laufenden Unterrichts erfolgen darf. Auch im Rahmen des Unterrichts ist sicherzustellen, dass keine privaten Inhalte wie z. B. in Ordnern gespeicherte Dateien eingesehen werden können. Ausschließlich die geöffneten Fenster dürfen sichtbar sein, weil diese bei regelkonformer Nutzung nur Unterrichtsinhalte enthalten können. Zudem sollte eine lückenlose Vollkontrolle vermieden werden, bei der die Lehrkräfte jederzeit an jedem Unterrichtstag alle Aktivitäten der betreffenden Schüler:innen live verfolgen. Stichproben bzw. anlassbezogene Aufschaltungen des Lehrpersonals sind nicht zu beanstanden.

Im Rahmen der Prüfung wurde zunächst die fragliche Schule, vertreten durch die Schulleitung, angehört und die Möglichkeit zur Stellungnahme gebeten. Die Schulleitung teilte dem HmbBfDI mit, dass aufgrund der Anzahl der Schüler pro Klasse eine analoge Überprüfung der Endgeräte organisatorisch nicht möglich sei. Die Nutzung von privaten Geräten für den Unterricht sei zudem freiwillig. Alternativ könnten die Schüler:innen schuleigene Geräte benutzen. Daher entstünden Schüler:innen, die keine eigenen Geräte für den Unterricht nutzen möchten, keine Nachteile.

Durch die von der Schule ergriffenen technischen und organisatorischen Maßnahmen sei sichergestellt, dass ein aktives Sichten privater Dateien der Schüler:innen durch Lehrkräfte nicht möglich sei. Lehrkräfte könnten nur Einsicht in die Geräte der Schüler:innen nehmen, wenn diese im WLAN der Schule eingeloggt seien und sich in Bluetooth-Reichweite des Geräts der kontrollierenden Lehrkraft befinden. Die Schüler:innen erhielten dabei automatisch eine Information, wenn sich eine Lehrkraft zugeschaltet hat.

Es sei allerdings möglich, dass eine Lehrkraft das Öffnen einer App auf einem Schülergerät veranlassen könnte und dabei private Daten der Schüler:innen, die direkt beim Öffnen der App – z. B. einer Foto App – sichtbar werden, einsehen könnte. Um dies zu verhindern, wurden die Schüler:innen und Eltern aufgefordert, entsprechende Änderungen in den Einstellungen der Geräte vorzunehmen, damit die Daten bei Öffnen einer App erst nach einer Bestätigung durch die Schüler:innen angezeigt werden. Eine lückenlose Vollkontrolle der Geräte der Schüler:innen werde durch die vorgenannten Maßnahmen effektiv verhindert.

Nach Ansicht des HmbBfDI sind die von der Schulleitung getroffenen Maßnahmen ausreichend, um ein ausreichendes Schutzniveau für die Daten der Schüler:innen zu gewährleisten.

Allerdings konnte die Schulleitung zum Zeitpunkt der Anhörung keine vollständige datenschutzrechtliche Dokumentation vorlegen. Diesbezüglich haben wir die Datenschutzbeauftragte der Behörde für Schule, Familie und Berufsbildung kontaktiert. Diese wird die Schulleitung im nächsten Schritt bei der Erstellung einer entsprechenden Dokumentation unterstützen.

8. NEMO GS – Nutzung des telefonischen Hamburg Service zur Aktenauskunft in der Grundsicherung

Die Schaffung einer zentralen Infrastruktur für die Leistung zentraler Verwaltungsdienste wie den Telefondienst kann zur Entlastung der fachlichen Sachbearbeitung beitragen, erfordert aber einige Schutzmaßnahmen zur Gewährleistung des Sozialdatenschutzes.

Im Rahmen des Projekts „Neuausrichtung und Modernisierung der Verwaltungsarbeit für Grundsicherung und Soziales" (NEMO GS) wird der Telefonische Hamburg Service (THS) bezirksamtsübergreifend in die Telefonie der Fachämter Grundsicherung und Soziales eingebunden, um Aufgaben wie telefonische Beratungen, Beantwortung von telefonischen Sachstandsanfragen, Dokumentenversand und Terminkoordination zu übernehmen. Hierdurch soll die telefonische Erreichbarkeit verbessert und zudem eine Entlastung im Backoffice erreicht werden. Für diese Aufgabe erhalten alle Mitarbeitenden des THS umfassende Zugriffsrechte auf die Fachverfahren Open / Prosoz, DTMS (digitales Terminmanagementsystem), SharePoint Lists sowie die Service Center Application (SCA) für sämtliche Grundsicherungsämter- und Sozialämter der Bezirksämter Hamburgs, ohne amtsbezogene Beschränkungen. Aus datenschutzrechtlicher Perspektive steht das Vorgehen im Spannungsfeld zum Sozialdatenschutz gemäß §§ 67 ff. SGB X und dem Grundsatz der engen Informationsbindung („need to know"), der eine Beschränkung des Zugriffs auf Sozialdaten auf die unmittelbar zuständigen Sachbearbeitenden und unterstützende Stellen fordert. Die vorgesehene umfassende Zugriffsgewährung widerspricht grundsätzlich dieser „informationellen Gewaltenteilung" und stellt ein datenschutzrechtliches Ungleichgewicht dar.

Um dieses Ungleichgewicht auszugleichen, werden von Seiten des HmbBfDI technische und organisatorische Maßnahmen vorgeschlagen: Eine vollständige Protokollierung aller Zugriffe einschließlich lesen-

der Zugriffe auf die Fachverfahren soll die Nachvollziehbarkeit und Überprüfbarkeit der Zugriffe sicherstellen. Ergänzend sind regelmäßige Stichprobenkontrollen sowie eine besondere Verschwiegenheitspflicht der THS-Mitarbeitenden vorzusehen. Zudem wird empfohlen, den Zugriff auf Einzelfallakten ausschließlich über die Eingabe eines Aktenzeichens zu ermöglichen, um unbefugte Zugriffe zu verhindern. Dieses Aktenzeichen muss als Authentifizierungsmerkmal so gestaltet sein, dass es nicht aus allgemein bekannten personenbezogenen Daten ableitbar ist, um eine sichere Identifikation der Anrufenden zu gewährleisten. Das vorgestellte Authentifizierungsverfahren wird grundsätzlich als geeignet bewertet, sofern diese Anforderungen erfüllt sind.

Im Hinblick auf den Auftragsverarbeitungsvertrag zwischen den sieben Bezirksämtern und dem Bezirksamt Wandsbek als Betreiber des THS bestehen noch Unklarheiten. Insbesondere ist unklar, wie sichergestellt wird, dass ausschließlich und direkt nur die Fachabteilung Telefonie GS Anrufe im Bereich Grundsicherung entgegennimmt und keine Befassung durch andere THS-Bereiche erfolgt. Zudem sind die Beschreibungen der Aufgaben des THS und die hierfür zu etablierenden Prozesse und Ausgestaltung von Berechtigungen z. T. noch unpräzise und in sich nicht stimmig dargestellt. Weiterhin ist die Rolle einer geplanten fachlichen Leitstelle zur Administration des Anliegenmanagements im FHH Portal sowie eines verknüpften Auswertungsdashboards (MS Power BI) unklar und bedarf der Erläuterung. Zur vorgesehenen Nutzung von SharePoint Lists liegen hinsichtlich der Ausgestaltung der vorgesehenen vordefinierten Formulare und den getroffenen technischen Schutzmaßnahmen noch keine ausreichenden Unterlagen vor, welche daher nachgefordert wurden. Gleiches gilt für Informationen zur ServiceCenterApplication

Insgesamt wird die Einbindung des THS in den Prozess als grundsätzlich möglich erachtet, jedoch nur unter der Voraussetzung, dass das datenschutzrechtliche Ungleichgewicht durch geeignete technische und organisatorische Maßnahmen ausgeglichen wird und die offenen Fragen zum Auftragsverarbeitungsvertrag sowie zu den Schutzmaßnahmen geklärt werden.

9. Geschlechtliche Vielfalt ist auch ein Datenschutzthema

In der digitalen Kommunikation mit der richtigen Geschlechtsidentität angesprochen zu werden, ist Teil der informationellen Selbstbestimmung und führt zu einem Rechtsanspruch. Dem gerecht zu werden, ist nicht nur Ausdruck von Respekt, sondern auch eine rechtliche Pflicht von Unternehmen und Behörden.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 10. Oktober 2017 festgestellt: Es gibt drei Geschlechter – weiblich, männlich und divers. Davon geht auch das am 1. November 2024 in Kraft getretene Selbstbestimmungsgesetz aus, das zudem als vierte Option vorsieht, im Personenstandsregister kein Geschlecht zu erfassen. In rechtlicher Hinsicht ist die Frage damit eindeutig geklärt. Das hat auch praktische Auswirkungen auf die Verarbeitung personenbezogener Daten.

Wenn personenbezogene Daten verarbeitet werden, muss sichergestellt werden, dass die richtigen Informationen erhoben und falsche Inhalte im Datenbestand korrigiert werden. Datenverarbeitende Stellen wie etwa Handelsunternehmen, Vermieter:innen oder Behörden, die Angaben über das Geschlecht verarbeiten, müssen daher in der Lage sein, neben den Attributen weiblich und männlich auch die Angabe divers in ihren Systemen zu vermerken. Anreden in Geschäftsbriefen müssen so ausgestaltet werden, dass auch eine geschlechtsneutrale Ansprache möglich ist. Für den Bereich des Onlinehandels haben Oberlandesgerichte diese Anforderung bestätigt (OLG Karlsruhe vom 14. Januar 2021, OLG Frankfurt vom 21. Juni 2022).

Das Datenschutzrecht bietet Betroffenen einen Rechtsanspruch auf Berichtigung ihrer Daten. Dafür müssen sie darlegen und gegebenenfalls nachweisen, dass die gespeicherten Informationen unrichtig sind. Der Anspruch greift auch, wenn die Geschlechtsangabe bei ih-

rer Erhebung noch korrekt war, sich aber später auf Grundlage des Selbstbestimmungsgesetzes verändert hat. Maßgeblich für die Frage, welches Geschlecht eine Person nach juristischen Maßstäben hat, ist die Eintragung in das Personenstandsregister. Diese Wertung ergibt sich aus § 10 des Gesetzes über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SBGG). Selbstverständlich kann es unabhängig vom Rechtsanspruch sinnvoll sein, individuelle Bedürfnisse der Betroffenen zu respektieren und gegebenenfalls auf ausdrücklichen Wunsch hin vom Personenstandsregister abweichende Geschlechtsangaben zu speichern.

Ob die Abfrage des Geschlechts überhaupt erforderlich ist, hängt von der jeweiligen Konstellation ab. So darf beispielsweise im Onlinehandel das Geschlecht nur abgefragt werden, wenn diese Information „objektiv unerlässlich" für den entsprechenden Vertrag ist.

Der Europäische Gerichtshof hat am 9. Januar 2025 entschieden, dass dies für den Verkauf von Bahnfahrkarten grundsätzlich nicht der Fall ist (Rechtssache C-394/23). Beförderungsleistungen können auch angeboten werden, wenn die Bahngesellschaft das Geschlecht ihrer Kund:innen nicht kennt. Eine personalisierte Ansprache sieht der Gerichtshof nicht als hinreichenden Erhebungsgrund an, da für eine höfliche Anrede auch inklusive Formulierungen zur Verfügung stünden.

Der HmbBfDI beanstandet nicht, wenn zu Zwecken einer respektvollen und geschäftsüblichen Kommunikation in Kund:innenformularen Anredeoptionen abgefragt werden. In der Regel dürfen diese infolge der Gerichtsentscheidung jedoch nicht als Pflichtfeld ausgestaltet sein. Kund:innen ist neben der Angabe Frau/Herr/divers auch die Option einzuräumen, keine Angabe zu machen. In dem Fall ist eine geschlechtsneutrale Anredeform zu verwenden. Die verpflichtende Abfrage des Geschlechts ist nur erlaubt, wenn dies konkret erforderlich ist, was beispielsweise bei einer medizinischen Behandlung oder der Belegung von Mehrbettzimmern in einem Hostel der Fall sein kann.

Der HmbBfDI achtet bei seinen Routineprüfungen darauf, dass die richtige Speicherung der Geschlechtsidentität möglich ist und wirkt auf entsprechende Änderungen hin.

10. Digitalisierung des Check-In Vorgangs bei Hotels

Die Einführung (voll-)automatisierter Check-in-Systeme in Hotels bietet erhebliche Chancen für die Digitalisierung des Gastgewerbes. Mit Änderungen des Beherbergungsmeldegesetzes (BMG) zum Januar 2025 ergeben sich neue datenschutzrechtliche Herausforderungen. Der HmbBfDI hat die zentralen Problemfelder analysiert und gibt klare Empfehlungen für eine datenschutzkonforme Umsetzung, an der sich sowohl Verantwortliche, als auch Gäste orientieren können.

Die Digitalisierung des Check-in-Vorgangs in Hotels hat in den vergangenen Jahren, insbesondere nach der Pandemie, stark an Bedeutung gewonnen. Automatisierte Systeme ermöglichen Gästen, ihr Zimmer ohne Interaktion mit dem Personal zu beziehen. Während diese Entwicklung aus Sicht der Effizienz und des Komforts begrüßenswert ist, zeigt sich in der behördlichen und datenschutzrechtlichen Praxis ein erhebliches Maß an Unsicherheit bezüglich der datenschutzrechtlichen Anforderungen, die an solche Systeme zu stellen sind. In der Praxis des HmbBfDI kommt es zu Problemen, etwa wenn Beherbergungsbetriebe davon ausgehen, verpflichtet zu sein, personenbezogene Daten ihrer Gäste zu erfassen. Wechselnde gesetzliche Regelungen erschweren hierbei eine fortlaufende Orientierung aller Beteiligten:

Das Bundesmeldegesetz (BMG) regelt die Registrierung von Gästen in Beherbergungsstätten und die Übermittlung dieser Daten an die zuständigen Meldebehörden. Bis einschließlich Dezember 2024 waren Hotels verpflichtet, von ihren Gästen umfangreiche Meldescheine ausfüllen zu lassen und diese Informationen zu dokumentieren. In der Praxis wurde vielfach angenommen, dass ein Abgleich oder sogar die

Anfertigung einer Kopie von Personalausweisen oder Reisepässen zulässig sei. Mit den Änderungen des BMG, die zum 01. Januar 2025 in Kraft getreten sind, hat sich die Rechtslage vereinfacht. Zwar bestand bereits vor der Gesetzesänderung keine rechtliche Verpflichtung zur Anfertigung einer Kopie des deutschen Personalausweises; daran hat sich auch durch die Neuregelung nichts geändert. Die Anfertigung einer Kopie ist weiterhin unzulässig. Allerdings entfällt nunmehr grundsätzlich die Pflicht zur Erstellung eines Meldescheins. Es genügt, dass der (deutsche) Gast seine Staatsangehörigkeit angibt und diese nur bei berechtigten Zweifeln nachweist. Eine generelle Pflicht zur Vorlage eines Ausweisdokuments besteht folglich nicht mehr. Deutsche Gäste müssen keinen Personalausweis oder Reisepass mehr vorzeigen, kopieren oder scannen lassen. Dennoch zeigt sich in der Praxis vereinzelt, dass viele Hotels weiterhin eine Kopie- oder Scanpflicht des Personalausweises als Voraussetzung für den Zugang zum Zimmer verlangen. Diese Praxis verstößt gegen mehrere grundlegende Datenschutzprinzipien. Das zentrale Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO besagt, dass personenbezogene Daten nur in dem Umfang erhoben und verarbeitet werden dürfen, wie dies für den jeweiligen Zweck erforderlich ist.

Für Hotels bedeutet dies konkret: Wenn ein Gast erklärt oder nachweist, dass er deutscher Staatsbürger ist, genügt dies für die Erfüllung der melderechtlichen Anforderungen. Weitere Daten, etwa aus dem Personalausweis wie Augenfarbe oder Körpergröße, sind nicht erforderlich und dürfen daher zwar verarbeitet aber nicht verifiziert werden. Adressdaten dürfen nur verifiziert werden, wenn die Bezahlung per Rechnung im Nachgang erfolgt. Das BMG erstreckt sich nicht auf die Erhebung von Personalausweiskopien oder umfassenden biometrischen Daten. Eine Einwilligung der Gäste wäre somit in diesem Zusammenhang nicht wirksam, da sie regelmäßig an die Erfüllung einer notwendigen Leistung gekoppelt wäre (Kopplungsverbot nach Art. 7 Abs. 4 DSGVO). Die Pflicht, den Personalausweis zu scannen, um das Zimmer zu betreten, ist ein solcher Fall. Der Aufenthalt ist auch ohne diese Datenerfassung möglich und rechtskonform, wenn der Gast versichert oder bestätigt, dass er deutscher Staatsbürger

ist. Hotels müssen also ein System vorhalten, das zwischen deutschen und ausländischen Staatsbürgern differenziert und nur bei Letzteren die Meldepflicht durchsetzen.

Hotels argumentieren mitunter, dass bei autonomen Check-in-Systemen eine technische Überprüfung der Identität des Gastes erforderlich sei, da kein Personal vor Ort ist. Dieses Argument ist datenschutzrechtlich nicht überzeugend. Die Meldepflicht nach BMG verlangt nur die minimalen Informationen, die für die Registrierung notwendig sind. Zulässige Alternativen sind beispielsweise die einfache Selbstauskunft des Gastes, Plausibilitätsprüfungen anhand der bei der Buchung angegebenen Daten oder eine nachträgliche Kontrolle im Verdachtsfall. Die Speicherung von Ausweisbildern „für später" wäre nicht zweckmäßig. Daten dürfen nur so lange gespeichert werden, wie sie für den Zweck erforderlich sind. Die datenschutzrechtlichen Anforderungen unterscheiden sich nicht danach, ob an der Rezeption ein Mensch sitzt oder ein System. In einem traditionellen Hotel genügt die mündliche Bestätigung des Gastes, dass er deutscher Staatsbürger ist. Ein automatisiertes System muss diese Logik abbilden und darf keine technisch intensivere Datenerhebung verlangen.

Der HmbBfDI empfiehlt Hoteliers, bestehende Systeme zu überprüfen und gegebenenfalls anzupassen, die Prozesse zu vereinfachen und die Gäste transparent zu informieren. Bei der Einführung neuer Check-in-Systeme sollte eine Datenschutz-Folgenabschätzung durchgeführt werden. Softwareanbieter sind aufgefordert, Datenminimierung als Standard umzusetzen, keine Ausweisscans zu erzwingen und ihre Kunden entsprechend zu schulen. Die Digitalisierung des Check-in-Vorgangs ist datenschutzrechtlich möglich. Sie ist jedoch nur dann datenschutzkonform umsetzbar, wenn die gesetzlichen Anforderungen der einschlägigen Gesetze beachtet werden. Hotels und Softwareanbieter tragen gemeinsam Verantwortung für die Einhaltung der Datenschutzvorgaben und sollten die Vereinfachungen des neuen BMG als Chance für eine datenschutzfreundliche Digitalisierung begreifen.

11. Weitergabe von Beschäftigtendaten in Konzernstrukturen

Werden Matrixstrukturen als Organisationsmodell für die personelle Zusammenarbeit in Unternehmensgruppen und Konzernen genutzt, müssen die Datenübertragungsvorgänge von Beschäftigtendaten auf eine Rechtsgrundlage gestützt werden.

Im Berichtszeitraum hatte der HmbBfDI über zwei Beschwerden zur Weitergabe von Beschäftigtendaten in Konzernstrukturen zu entscheiden. Dabei wurden Beschäftigtendaten konzernintern übermittelt, um eine einheitliche Vergütungsstruktur und gleiche Arbeitsbedingungen im Konzern zu schaffen. Übermittelt wurden Gehaltslisten mit Angaben zu Namen, Gehalt, Tarif / AT, Eintritts- / Austrittsdatum, Abteilung und Position.

Der HmbBfDI stellte in seiner rechtlichen Bewertung eine unrechtmäßige Verarbeitung personenbezogener Daten gemäß Art. 5 DSGVO fest, da keiner der in Art. 6 Absatz 1 DSGVO genannten Tatbestände erfüllt war und keine Einwilligung der Beschäftigten vorlag.

Art. 6 Abs. 1 lit. b DSGVO kam als Rechtsgrundlage nicht in Betracht, weil die Weiterleitung der Daten für die Zwecke des Beschäftigungsverhältnisses nicht erforderlich war.

Die Verarbeitung konnte auch nicht auf Art. 6 Absatz 1 lit. f DSGVO gestützt werden. Sie wäre nur dann 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 überwiegen. Zu den berechtigten Interessen des Verantwortlichen oder Dritten zählen neben rechtlichen auch tatsächliche, wirtschaftliche oder ideelle Interessen, nicht jedoch bloße Allgemeininteressen. Die in den Erwägungsgründen 47-50 der DSGVO genannten Beispiele – etwa die Verarbeitung im

Rahmen konzerninterner Übermittlungen – verdeutlichen, dass vielfältige und unterschiedliche Interessen berücksichtigt werden können. In den beiden Beschwerden waren die zugrunde liegenden Interessen dem Grunde nach als berechtigt anzusehen.

Es fehlte jedoch an der Erforderlichkeit. Der EuGH hat im Hinblick auf die Erforderlichkeit klargestellt, dass Ausnahmen und Beschränkungen beim Schutz der personenbezogenen Daten auf das absolut Notwendige beschränkt sein müssen. Daher ist stets zu prüfen, ob das berechtigte Interesse nicht ebenso wirksam mit milderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen.
Der Zweck der Verarbeitung lag hier in der Schaffung einheitlicher Vergütungsstrukturen und gleicher Arbeitsbedingungen im Konzern. Dieser Zweck kann auch dann erreicht werden, wenn die Daten in pseudonymisierter Form übermittelt werden, ohne dass die einzelnen Beschäftigten identifizierbar sind. Durch eine solche Pseudonymisierung werden die datenschutzrechtlichen Risiken für die Beschäftigten reduziert, was zugleich dem Grundsatz der Datenminimierung nach Art. 5 Absatz 1 lit. c DSGVO entspricht.

Der HmbBfDI weist darauf hin, dass Arbeitgeber:innen bei der Übermittlung von Beschäftigtendaten an andere Konzerngesellschaften eine ausreichende Rechtsgrundlage nachweisen müssen. Zudem sind die Beschäftigten über diese Weitergabe umfassend zu informieren.

12. Meldung von Mieter:innendaten an Grundversorger

Durch eine Änderung der Abrechnungspraxis im Strommarkt ist die Übermittlung von Mieter:innendaten an Grundversorger neu zu bewerten. Der HmbBfDI hat sich intensiv mit den datenschutzrechtlichen Anforderungen auseinandergesetzt und maßgeblich an einem bundesweiten Beschluss der Datenschutzkonferenz mitgewirkt, der nun Rechtssicherheit für Vermieter:innen, Mieter:innen und Grundversorger schafft.

Der Wechsel von Mieter:innen in einer Wohnung bringt regelmäßig Herausforderungen für die Stromversorgung mit sich. Bislang konnten Mieter:innen nach Einzug innerhalb von sechs Wochen rückwirkend einen Stromlieferanten wählen, der dann auch den bereits erfolgten Verbrauch abrechnete. Diese Möglichkeit entfällt seit dem 06. Juni 2025 aufgrund der „Festlegung einheitlicher Geschäftsprozesse und Datenformate zur Abwicklung der Belieferung von Kunden mit Elektrizität" (Beschluss der 6. Beschlusskammer der Bundesnetzagentur vom 21. März 2024). Ab diesem Zeitpunkt kann ein Wechsel des Stromlieferanten nur noch mit Wirkung für die Zukunft erfolgen. Der Zeitraum zwischen Einzug und Vertragsabschluss wird nun stets über den Grundversorger abgerechnet. Diese Änderung hat unmittelbare Auswirkungen auf die Praxis der Datenübermittlung: Der Grundversorger muss wissen, wer seine Vertragspartner:innen sind, um die erbrachte Leistung korrekt in Rechnung stellen zu können.

In der Regel meldet sich die alte Mietpartei zum Auszug beim Stromlieferanten ab. Die neue Mietpartei ist gesetzlich verpflichtet, die Stromentnahme und ihre Kontaktdaten dem Grundversorger mitzuteilen (§ 2 Abs. 2 StromGVV). In der Praxis ist diese Pflicht jedoch vielen Mieter:innen nicht bekannt und wird daher selten erfüllt. Der Grundversorger hat keinen Einblick in das Mietverhältnis und wendet sich

daher häufig an die Eigentümer:innen, um die notwendigen Daten zu erhalten. Bislang war die Übermittlung von Mieter:innendaten durch Vermieter:innen an den Grundversorger datenschutzrechtlich umstritten, insbesondere weil Mieter:innen in den ersten Wochen nach Einzug noch einen anderen Versorger hätten wählen können.

Mit der neuen Abrechnungspraxis entfällt diese Unsicherheit. Der HmbBfDI hat die Situation zum Anlass genommen, im Rahmen der Datenschutzkonferenz und nach Gesprächen mit dem Hamburger Grundversorger Vattenfall eine rechtssichere Lösung zu erarbeiten. Die Datenschutzkonferenz hat in ihrem Beschluss „Meldung von Mieter:innendaten an Grundversorger" vom 28. Mai 2025 klargestellt, dass die Übermittlung von Mieter:innendaten durch Vermieter:innen oder beauftragte Verwalter:innen an den jeweiligen Grundversorger ab dem Zeitpunkt der Wohnungsübergabe durch ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 S. 1 lit. f DSGVO gerechtfertigt ist. Voraussetzung ist, dass die betroffenen Mieter:innen nach Art. 13 DSGVO rechtzeitig vorab über die beabsichtigte Datenübermittlung informiert werden. Die Datenschutzkonferenz empfiehlt, diese Information bereits bei Vertragsschluss schriftlich zu erteilen.

Der Beschluss der Datenschutzkonferenz schafft damit bundesweit Klarheit und Rechtssicherheit für alle Beteiligten. Vermieter:innen und Verwalter:innen können nun im berechtigten Interesse die notwendigen Daten an den Grundversorger übermitteln, sofern die Mieter:innen ordnungsgemäß informiert wurden. Gleichzeitig wird sichergestellt, dass die datenschutzrechtlichen Anforderungen gewahrt bleiben und die Rechte der Mieter:innen geschützt werden.

13. Neues Arbeitsplatzsystem (nextKAS) am UKE

Über die Einführung eines neuen Krankenhausarbeitsplatzsystems (KAS) im Universitätsklinikum Hamburg-Eppendorf (UKE) war bereits in den Tätigkeitsberichten der vergangenen drei Jahre zu lesen. Grund für die Einführung ist das Ende des technischen Supports für das aktuell noch in weiten Teilen des UKE-Konzerns zur Patient:innen-Verwaltung genutzte System „Soarian".

Ursprünglich drohte die Unterstützung des bestehenden Systems bereits zum Ende des Jahres 2024 wegzufallen. Durch die Vereinbarung einer Verlängerung des Supports für das Altsystem bis zunächst Ende 2026 wurde Zeit gewonnen – auch um datenschutzrechtlichen Anforderungen Genüge zu tun.

In 2024 war der Go-Live des neuen KAS unter der Bezeichnung NAVIS erst einmal nur in einem Teilbereich des Altonaer Kinderkrankenhauses (AKK) gestartet. Die Inbetriebnahme in weiteren Bereichen des AKK war in das Jahr 2025 verschoben worden. Im Berichtsjahr hat das UKE den HmbBfDI dann darüber informiert, dass Ende Juni 2025 NAVIS im restlichen und somit letztendlich im gesamten AKK in Betrieb genommen wurde.

Dabei wurde und wird das UKE weiterhin durch ein externes Beratungsunternehmen unterstützt, das insbesondere auch die mit der Inbetriebnahme von NAVIS in weiteren Häusern des UKE-Konzerns einhergehenden Risiken und die zu deren Bewältigung vorzusehenden technischen und organisatorischen Abhilfemaßnahmen in den Blick nehmen kann. Gleiches gilt für die aus datenschutzrechtlicher Sicht ebenfalls wichtigen Themen Rollen- und Berechtigungskonzept, Löschen und Aufbewahren oder Betroffenenrechte.

Im Oktober 2025 hat das UKE dem HmbBfDI zur Kenntnis gegeben, dass der ursprünglich für Februar 2026 angedachte Go-Live im ersten Teilbereich des UKE nicht wie vorgesehen stattfinden kann. Das UKE arbeitet an einem angepassten Projektplan, der zum Zeitpunkt des Redaktionsschlusses für diesen Tätigkeitsbericht noch nicht vorlag.

Auch wenn der HmbBfDI seine Beratung zu diesem Projekt beendet hat (vgl. 33. TB, Kapitel III 7), wird er mit dem UKE zur weiteren Umsetzung des Projekts im Austausch bleiben und für konkrete datenschutzrechtliche Fragestellungen weiterhin zur Verfügung stehen.

14. ePA und TI-Modellregion

Die elektronische Patientenakte (ePA) für alle wurde beginnend zum 15. Januar 2025 in der Telematik-Infraktruktur (TI) Modellregion Hamburg und Umland getestet – auch unter Berücksichtigung der Ende 2024 bekannt gewordenen Sicherheitslücken. Seit dem 29. April 2025 kann die ePA für alle bundesweit von Praxen, Krankenhäusern und Apotheken genutzt werden. Seit dem 01. Oktober 2025 ist die Befüllung verpflichtend.

Das Jahr 2024 endete für die ePA für alle damit, dass im Rahmen des 38th Chaos Communication Congress' des Chaos Computer Clubs (CCC) vorgestellt wurde, wie unberechtigte Personen den Behandlungskontext einer versicherten Person simulieren und so Zugang zu deren ePA für alle erlangen konnten (vgl. 33. TB, Kapitel III 9). Zu Beginn des Berichtsjahres ging es daher vorrangig darum, die Sicherheitslücken zu schließen, die einen solchen unberechtigten Zugriff möglich machten. Zu dieser Thematik hat der HmbBfDI direkt im Januar 2025 Kontakt zur TI-Modellregion Hamburg und Umland aufgenommen und haben in der Folge Gespräche auch mit der gematik GmbH stattgefunden, die die Gesamtverantwortung für die TI trägt. Mit der Sozialbehörde als der fachpolitischen Koordination im Projekt TI-Mo-

dellregion Hamburg und Umland hat der HmbBfDI sich ebenfalls zu der Problematik ausgetauscht.

Damit die ePA für alle in den TI-Modellregionen – neben Hamburg und Umland auch Franken – planmäßig ab dem 15. Januar 2025 getestet werden konnte, war es zunächst wichtig, dass geeignete Maßnahmen ergriffen wurden, um einen Zugriff durch andere als die testenden leistungserbringenden Institutionen zu verhindern. Das ist mittels einer sogenannten Allow-Liste im ePA-Aktensystem gelungen, in die diese Leistungserbringer-Institutionen aufgenommen, von der gematik GmbH geprüft und verifiziert wurden. Nur die am Test teilnehmenden (Zahn-)Arztpraxen, psychotherapeutischen Praxen, Apotheken, Krankenhäuser konnten so auf die elektronischen Patientenakten ihrer Patient:innen zugreifen.

Für den bundesweiten Roll-out der ePA für alle mussten aber zusätzliche Schritte unternommen werden, um einen sicheren Betrieb zu gewährleisten. Diese Maßnahmen wurden zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und der gematik GmbH abgestimmt. Dazu zählten unter anderem eine Anpassung und Verbesserung des Nachweises für den Behandlungskontext, eine Mengenbegrenzung für Zugriffe auf die ePA je Leistungserbringer-Institution oder Überwachungsmaßnahmen wie eine Anomalie-Erkennung. Mit diesen und weiteren Sicherheitsmaßnahmen ist die ePA für alle ab dem 29. April 2025 bundesweit ausgerollt worden. Zum selben Zeitpunkt wurde die Begrenzung auf die positiv-gelisteten Leistungserbringer in den Modellregionen aufgehoben.

Allerdings wurde zeitgleich zum bundesweiten Roll-out seitens des CCC erneut auf eine Möglichkeit für unberechtigte Zugriffe auf die elektronische Patientenakte hingewiesen, und zwar mittels elektronischer Ersatzbescheinigungen von Versichertenkarten, über die in Kombination mit der Versichertennummer, einem Codierungsschlüssel, einem Praxisausweis (SMC-B) und einem Anschluss an die TI wiederum der Behandlungskontext simuliert und Zugriff auf die ePA von Versi-

cherten genommen werden konnte. Dabei ist darauf hinzuweisen, dass die für die Offenlegung der Sicherheitslücke notwendige Beschaffung eines Praxisausweises durch ein unzulässiges Anbieten dieses Ausweises eines Praxisbetreibers ermöglicht wurde. Darauf wurde seitens der gematik GmbH reagiert und auch diese Sicherheitslücke konnte erst einmal geschlossen werden. Die Implementierung einer endgültigen technischen Lösung für die bislang skizzierten Angriffsszenarien in dem Sinne, dass digital und ortsungebunden nachgewiesen werden kann, dass sich eine versicherte Person in einer medizinischen Versorgungssituation – dem so genannten Behandlungskontext – befindet, steht für 2026 noch aus. Die Sicherheit der ePA wird somit auch zukünftig weiterhin zu betrachten und zu begleiten sein.

Die TI-Modellregionen Hamburg und Umland sowie Franken haben zur Durchführungsphase der ePA für alle-Pilotierung vom 15. Januar bis zum 30. Juni 2025 einen Abschlussbericht erstellt, vorrangig zur technischen Funktionsfähigkeit sowie zur Integration der ePA für alle in den Versorgungsalltag der teilnehmenden Leistungserbringenden (s. https://www.gematik.de/media/gematik/Medien/ePA_fuer_alle/Abschlussbericht_Modellregionen/gematik_TI-Modellregionen_Abschlussbericht_Link_02.pdf).

Nächstes Pilotprojekt in der TI-Modellregion Hamburg und Umland ist die sogenannte Pilotierung-Pflege. Jenes Projekt soll die Zusammenarbeit zwischen Pflegeeinrichtungen und deren Kommunikationspartner:innen – wie Arztpraxen, Apotheken und Kliniken – betrachten und verbessern, auch durch den Einsatz von TI-Anwendungen. Seit dem 22. September 2025 befindet sich die Modellregion in der Durchführungsphase der Pilotierung-Pflege (https://timo-hamburg-umland.de/pflegeeinrichtungen/).

Der HmbBfDI wird weiterhin als Ansprechpartner zu datenschutzrechtlichen Themen für die TI-Modellregion Hamburg und Umland zur Verfügung stehen.

15. Weitere Umsetzung des Gesundheitsdatennutzungsgesetzes

Am 26. März 2024 ist das Gesundheitsdatennutzungsgesetz (GDNG) in Kraft getreten. Eine Weitergabe der personenbezogenen Daten an Dritte in diesem Kontext ist danach grundsätzlich untersagt. Die jeweils zuständige Datenschutzaufsichtsbehörde kann unter bestimmten Voraussetzungen jedoch einer solchen zustimmen. Diesbezüglich hat der HmbBfDI neben weiteren Datenschutzaufsichtsbehörden an der Erstellung eines Antragsformulars mitgewirkt. Ferner wurde eine Orientierungshilfe zur vereinfachten Abstimmung mit den Datenschutzaufsichtsbehörden verabschiedet.

Hinsichtlich des GDNG hat der HmbBfDI im Jahre 2025 an den Terminen der eigens eingerichteten Unterarbeitsgruppe (UAG) GDNG teilgenommen. Die UAG GDNG ist der Taskforce Forschungsdaten zugeordnet.

§ 6 Abs. 3 Satz 4 GDNG bestimmt u.a., dass unter bestimmten Voraussetzungen eine Weitergabe von personenbezogenen Daten an Dritte möglich ist, wenn zuvor die jeweils zuständige Datenschutzaufsichtsbehörde zugestimmt hat. Die UAG GDNG hat diesbezüglich im Jahre 2025 ein Antragsformular entwickelt, woran auch der HmbBfDI mitgewirkt hat, das für das Ersuchen der Zustimmung der Aufsichtsbehörden zur Weitergabe von personenbezogenen Daten an (bestimmte) Dritte im Forschungskontext zur Anwendung kommen soll. Das Antragsformular ist auf der Homepage des HmbBfDI verfügbar.

Das Antragsformular hat den Zweck, das Verfahren auf Zugang zu Gesundheitsdaten für datenverarbeitende Gesundheitseinrichtungen (vgl. die Legaldefinition in § 2 Nr. 7 GDNG) möglichst zu standardisieren. Wie dabei das Verhältnis von § 6 Abs. 3 Satz 4 GDNG zu § 12 Hamburgisches Krankenhausgesetz ist, wonach ebenfalls eine

Weitergabe von personenbezogenen Daten an Dritte möglich ist, ist dabei nach wie vor Gegenstand der Bearbeitung. Überhaupt taten sich im Rahmen der Termine der UAG GDNG diverse rechtliche Fragestellungen auf, deren Beantwortung sich derzeit noch in Ausarbeitung in der UAG GDNG befindet.

Schließlich wurde von der Datenschutzkonferenz (DSK) im Dezember 2025 die „Orientierungshilfe zur Zusammenarbeit mehrerer Aufsichtsbehörden im Rahmen von § 5 GDNG" verabschiedet. An deren Erstellung hatte der HmbBfDI im Rahmen seiner Teilnahme an den Sitzungen der UAG GDNG mitgewirkt. In ihr geht es um eine Veranschaulichung, wann einerseits aus Sicht der Datenschutzaufsichtsbehörden des Bundes und der Länder bei gemeinsamen Vorhaben der Gesundheitsforschung mehrerer verantwortlicher Stellen die Voraussetzungen für die Übertragung der Federführung auf eine Aufsichtsbehörde und wann andererseits die Voraussetzungen für die Übertragung der alleinigen Zuständigkeit auf eine Aufsichtsbehörde vorliegen. Ebenfalls werden in der Orientierungshilfe die Rechtsfolgen der jeweiligen Übertragung dargestellt. Im Falle der Übertragung der Federführung auf eine Aufsichtsbehörde (vgl. § 5 Abs. 1-3 GDNG) hat die federführende Aufsichtsbehörde die Aufgabe, die Tätigkeiten und Maßnahmen der beteiligten Datenschutzaufsichtsbehörden zu koordinieren und eine Zusammenarbeit zu fördern sowie auf eine gemeinsame Entscheidung hinzuwirken. Die aufsichtsrechtlichen Befugnisse der betroffenen Datenschutzaufsichtsbehörden bleiben jedoch letztlich von einer solchen Übertragung unberührt (vgl. § 5 Abs. 3 Satz 2 GDNG). Im Falle der Übertragung der alleinigen Aufsicht (vgl. § 5 Abs. 4 GDNG) hingegen, welche nur bei nicht öffentlichen Stellen möglich ist, liegt die Zuständigkeit ab dem maßgeblichen Zeitpunkt ausschließlich bei der sodann allein zuständigen Datenschutzaufsichtsbehörde.

Zweck des § 5 GDNG ist es, mit der Möglichkeit der Übertragung der Federführung oder der alleinigen Zuständigkeit auf eine Aufsichtsbehörde die Verfahren zur Abstimmung mit den Datenschutzaufsichtsbehörden zu vereinfachen. Dieser Ansatz wird vom HmbBfDI ausdrücklich unterstützt und ist ein wichtiger Schritt um bei bundeslandübergrei-

fenden Verfahren einen sachgerechten Mechanismus zu finden, um doppelte Prüfungen und divergierende Entscheidungen im Sinne der Rechtssicherheit zu vermeiden.

16. Datenschutz bei der Terminverwaltung durch Heilberufspraxen

Patient:innen, die bereits von einer Heilberufspraxis über eine Weitergabe ihrer personenbezogenen Daten an ein Terminverwaltungsunternehmen, informiert wurden, müssen grundsätzlich nicht um ihre Zustimmung ersucht werden. Es können aber nur für medizinische Behandlungen erforderliche Datenverarbeitungen ohne Zustimmung der Patient:innen auf Terminverwaltungsunternehmen ausgelagert werden. Das Versenden von Terminnachrichten ist deshalb nur nach ausdrücklicher Einwilligung der Patient:innen gestattet.

Die Weitergabe von personenbezogenen Daten durch Heilberufspraxen an Terminverwaltungsunternehmen wirft immer wieder Fragen bei Betroffenen auf. Dies kann sich beim HmbBfDI sowohl in eingehenden Beschwerden als auch in Rechtsberatungsanfragen betroffener Personen äußern. Und auch Heilberufspraxen selbst treten mitunter mit diesbezüglichen Fragen an den HmbBfDI heran. Aus diesem Grund hat die Datenschutzkonferenz (DSK) am 16. Juni 2025 das Positionspapier „Datenschutz bei der Terminverwaltung durch Heilberufspraxen – Positionspapier zum datenschutzrechtlichen Einsatz von Dienstleistern für Online-Terminbuchungen und das Terminmanagement“ beschlossen. Das Positionspapier wurde unter anderem auch vom HmbBfDI miterarbeitet.

Im Positionspapier wird zunächst festgehalten, dass die Auslagerung von Datenverarbeitungsprozessen von Heilberufspraxen auf externe Dienstleister als Auftragsverarbeitung nach § 28 DSGVO grundsätzlich zulässig sein könne. Jedoch müsse dabei die Informationspflicht

nach Art. 13 f. DSGVO beachtet werden. Das beinhalte, dass dabei insbesondere das jeweilige Terminverwaltungsunternehmen konkret zu bezeichnen sei. Weiter seien nur Datenverarbeitungen, die für medizinische Behandlungen erforderlich sind, ohne Einwilligung auf Terminverwaltungsunternehmen im Rahmen einer Auftragsverarbeitung auslagerbar. Dies rührt daher, dass Heilberufspraxen auch im Falle einer Datenverarbeitung durch unmittelbar sie selbst dies nur dann ohne Einwilligung tun können, wenn die Voraussetzungen von Art. 6 Abs. 1 lit. b) und Art. 9 Abs. 2 lit. h) DSGVO vorliegen, wo jeweils der Begriff der „Erforderlichkeit" fällt. Das Vereinbaren von Terminen ist für eine medizinische Behandlung erforderlich (von Notfallsituationen einmal abgesehen, die gesondert zu betrachten wären). Das Versenden von Terminnachrichten (z. B. Terminerinnerungen) hingegen sei für die medizinische Behandlung selbst nicht erforderlich. Das Versenden von Terminnachrichten solle daher nur nach ausdrücklicher Einwilligung der Patient:innen gestattet sein. Die Heilberufspraxis müsse zudem nachweisen können, dass eine solche Einwilligung vorliege.

Wenn eine Heilberufspraxis einmal Kenntnis davon erlangen sollte, dass das jeweilige Terminverwaltungsunternehmen personenbezogene Daten von Patient:innen zu eigenen Zwecken verarbeitet, trifft die betroffene Heilberufspraxis die Pflicht, dafür zu sorgen, dass der Dienstleister wieder einen datenschutzkonformen Zustand herstellt. Denn die Verarbeitung der Daten hat sich nach den Weisungen der Heilberufspraxis und nach dem zwischen Heilberufspraxis und Terminverwaltungsunternehmen abzuschließenden Auftragsverarbeitungsvertrag im Sinne von Art. 28 DSGVO zu richten. Schließlich sollen die Heilberufspraxen durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass die Vorgaben des Datenschutzes auch bei der Verarbeitung von personenbezogenen Daten zum Zwecke der Terminvergabe eingehalten werden. Dies ist auch dann zu beachten, wenn ein Terminverwaltungsunternehmen als Auftragsverarbeiter eingebunden wird. Das führt dazu, dass bei den Heilberufspraxen schon im Vorfeld der Beauftragung eines Terminverwaltungsunternehmens bestimmte Prüfpflichten entstehen, z. B. ob die Vertraulichkeit durch den Dienstleister gewährleistet ist oder ob Löschvorgaben umgesetzt werden.

Das Positionspapier stellt somit letztlich eine Reaktion auf Fragen aus der Praxis dar und bietet sowohl den Patient:innen als auch den Heilberufspraxen sowie den Terminverwaltungsunternehmen eine Orientierung.

17. Videoüberwachung

Ein Tätigkeitsschwerpunkt des HmbBfDI liegt in der Prüfung und Beratung der Einhaltung gesetzlicher Vorgaben bei der Inbetriebnahme von Kameras. Ziel ist es, sicherzustellen, dass der Einsatz solcher Systeme mit den geltenden datenschutzrechtlichen Vorgaben im Einklang steht. In diesem Zusammenhang ist ein erhöhtes Aufkommen an Beschwerden zu verzeichnen, die insbesondere Fälle betreffen, in denen private Verantwortliche Videoüberwachung einsetzen. Jede Beschwerde wird sorgfältig geprüft, um die Einhaltung der Datenschutzbestimmungen zu gewährleisten und gegebenenfalls aufklärende oder aufsichtsrechtliche Maßnahmen zu ergreifen. Außerdem führt der HmbBfDI zahlreiche Gespräche mit Privatpersonen, um durch vorherige Beratungen Klarheit über die datenschutzkonforme Positionierung der Kameras zu schaffen.

Videoüberwachung war früher ein Privileg großer Unternehmen und vermögender Privatpersonen, da die Technologie kostspielig und komplex in der Installation war. Mittlerweile hat sich das grundlegend gewandelt: Die Preise für Kameras, Speicherlösungen und komplette Überwachungssysteme sind massiv gefallen, während die technischen Leistungen erheblich zugenommen haben. Moderne Systeme bieten hochauflösende Bilder, kontinuierliche Aufzeichnung, Netzwerkintegration, cloudbasierte Speicherung und sogar Gesichtserkennungsfunktionen – Möglichkeiten, die früher undenkbar oder unbezahlbar waren.

Die niedrigen Anschaffungskosten und die leichte Zugänglichkeit der Technologie führen dazu, dass immer mehr Privatleute Überwachungskameras an ihren Häusern, Eingängen, Garagen oder in ihren Gärten in-

stallieren. Dies hat zur Folge, dass die Datenschutzbehörden vermehrt mit Beschwerden und Anfragen konfrontiert werden. Der Grund: Oft erfassen die Kameras auch öffentliche Flächen oder Nachbargrundstücke, wodurch sich betroffene Personen in ihren Privatsphäre- und Persönlichkeitsrechten beeinträchtigt fühlen.

Viele Menschen entscheiden sich heute im privaten Bereich aus unterschiedlichen Gründen für den Einsatz von Überwachungskameras. Ein zentraler Beweggrund ist der Wunsch, das eigene Eigentum – sei es das Haus, das Grundstück, die Parzelle im Kleingartenverein oder das Auto – besser zu schützen und potenzielle Diebstähle oder Beschädigungen zu verhindern. Ebenso spielt das Bedürfnis nach Sicherheit und dem Schutz der eigenen körperlichen Unversehrtheit eine wichtige Rolle, etwa um sich vor Übergriffen oder unbefugtem Betreten zu schützen. Darüber hinaus nutzen Eigentümer Kameras, um ihr Hausrecht wirksam durchzusetzen und den Zugang zu ihrem privaten Bereich zu kontrollieren.

Nutzende von Kameras verbinden mit deren Einsatz hohe Erwartungen an die Sicherheit ihres Eigentums. Tatsächlich bewirken Kameras vor allem ein erhöhtes subjektives Sicherheitsgefühl, tragen aber nicht immer zur Verhinderung von Vorfällen oder Straftaten bei, können aber bei der nachträglichen Aufklärung Unterstützung leisten.

Videoüberwachung bezeichnet die automatisierte Verarbeitung personenbezogener Daten – insbesondere von Bild-, Video- und Audiodaten – mithilfe optisch-elektronischer Einrichtungen. Da hierbei personenbezogene Informationen im Sinne der Datenschutz- Grundverordnung verarbeitet werden, gelten die Datenschutzvorschriften der DSGVO und des BDSG.

Bei Prüfungen des HmbBfDI wird oft argumentiert, Kameras würden nicht aufzeichnen und seien daher rechtlich unbedenklich. Tatsächlich greift bereits die Betrachtung von Livebildern (Echtzeitüberwachung bzw. Monitoring) als Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO.

Unter den Begriff der optisch-elektronischen Einrichtungen fallen nicht nur handelsübliche Überwachungskameras, sondern sämtliche Geräte, die zur längerfristigen Beobachtung eingesetzt werden und damit einem Überwachungszweck dienen. Unerheblich ist dabei, ob die Kamera stationär installiert oder mobil einsetzbar ist. Somit umfasst der Begriff sowohl festmontierte als auch frei bewegliche Geräte mit Kamerasystemen. Eine Videoüberwachung liegt daher auch dann vor, wenn Aufnahmen beispielsweise mit Dashcams, Drohnen, Wildkameras, Smartglasses, Action-Kameras oder Tür- und Klingelkameras erfolgen.

Die Datenschutzvorschriften gelten nicht, wenn eine Videoüberwachung ausschließlich zu privaten oder familiären Zwecken erfolgt, zum Beispiel zur Sicherung des eigenen Wohnhauses oder der eigenen Wohnung. Entscheidend ist, dass mit Bild- und Videodaten allein der eigene private Bereich erfasst wird (z. B. nur das eigene Grundstück, der eigene Wohnbereich oder die eigene Parzelle) und die Kamera nicht den öffentlichen Raum, fremde Grundstücke oder Gemeinschaftsflächen (Treppenhaus, Hof, Keller und Tiefgaragen) überwacht. Sobald faktisch die Grenzen des eigenen Grundstücks überschritten werden und keine persönlich familiäre Beziehung zum Betroffenen besteht oder die Videoüberwachung in einem beruflichen oder geschäftlichen Zusammenhang steht (z.B. Laden, Büro, Praxis), gilt diese Ausnahme nicht mehr und die DSGVO ist anwendbar.

Auch Kameraattrappen sind von der Anwendung der Datenschutzvorschriften ausgenommen, da keine personenbezogenen Daten verarbeitet werden. Ihr Zweck liegt regelmäßig in der Verhaltenslenkung durch Abschreckung. Auch wenn die Datenschutzaufsichtsbehörden bei Kameraattrappen nicht eingreifen können, kann bereits der bloße Anschein einer Beobachtung durch derartige Vorrichtungen einen erheblichen Überwachungsdruck erzeugen und damit zivilrechtliche Ansprüche, insbesondere wegen einer Beeinträchtigung des allgemeinen Persönlichkeitsrechts, begründen. In solchen Fällen steht den Betroffenen der Zivilrechtsweg zur Wahrung und Durchsetzung ihrer Rechte offen. Dies gilt gleichermaßen für aktive Überwachungskameras, wenn

diese nach den Kriterien der Rechtsprechung einen entsprechenden Überwachungsdruck verursachen. Ein wesentlicher Vorteil zivilrechtlicher Abwehr gegen Kameras ist, dass Betroffene einen Anspruch auf Entfernung oder Neuausrichtung der Kamera haben können.

Privatpersonen dürfen eine Videokamera nur dann einsetzen, wenn die Verarbeitung personenbezogener Daten auf einer gesetzlichen Grundlage beruht. Da die Datenschutz-Grundverordnung keine speziellen Regelungen für private Videoüberwachungen enthält, kommt in der Regel Art. 6 Abs. 1 Satz 1 lit. f) DSGVO als Rechtsgrundlage in Betracht.

Danach ist eine Videoüberwachung zulässig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und keine überwiegenden schutzwürdigen Interessen oder Grundrechte der betroffenen Personen entgegenstehen.

Eine Überwachung über die eigene Grundstücksgrenze hinaus kann also ausnahmsweise zulässig sein, wenn beim Eigentümer zuvor tatsächlich Schäden an der Hausfassade, etwa durch Graffiti oder Schmierereien, entstanden sind. Dabei darf der überwachte Bereich einen Streifen von höchstens einem Meter Breite, gemessen ab der Hauswand, nicht überschreiten.

Türklingelkameras und digitale Türspione dürfen eingesetzt werden, soweit die Kamera nur bei einem Klingelereignis aktiviert wird und ausschließlich den unmittelbaren Eingangsbereich erfasst. Sie muss sich nach kurzer Zeit automatisch wieder deaktivieren. Es darf technisch nicht möglich sein, Bereiche außerhalb der eigenen Grundstücksgrenze oder Mietfläche dauerhaft und anlasslos zu filmen. Der Einsatz von Drohnen von Privatpersonen, die mit Kameras ausgestattet sind und öffentliche Bereiche oder fremde Grundstücke überwachen, ist datenschutzrechtlich kaum möglich, da in der Mehrzahl der Fälle das Interesse der Betroffenen überwiegt.

Dashcams sind im fließenden Verkehr erlaubt, wenn sie nur kurzzeitig und anlassbezogen aufzeichnen. Im Rahmen der datenschutzrechtlichen Prüfung wird zunächst der Zweck des Dashcam-Betriebs festgestellt – etwa, ob die Aufnahmen zur Beweissicherung bei Unfällen oder zur Veröffentlichung in sozialen Medien verwendet werden sollen. Anschließend wird vom HmbBfDI geprüft, ob die Dashcam über eine Pre-Recording-Funktion verfügt und unter welchen Bedingungen das automatische Überschreiben der Aufnahmen beendet wird (z. B. bei Erschütterung oder Aufprall). Zudem wird kontrolliert, wie lange die Aufzeichnungen einschließlich des Pre-Recordings gespeichert bleiben und ob eine sofortige Löschung tatsächlich erfolgt. Liegt eine Nutzung zur Veröffentlichung vor oder erfolgt eine anlasslose Speicherung über mehr als 30 Sekunden, kann dies als rechtswidrige Nutzung bewertet werden. Grundsätzlich kann sich die Rechtmäßigkeit einer Videoüberwachung aber auch aus anderen Tatbeständen des Art. 6 Absatz 1 Satz 1 DSGVO ergeben, etwa wenn die betroffene Person eingewilligt hat oder die Verarbeitung zur Erfüllung rechtlicher Verpflichtungen erforderlich ist.

Die Überwachung darf das angrenzende Nachbargrundstück dann miterfassen, wenn der Nachbar und alle potenziell betroffenen Personen ausdrücklich eingewilligt oder dies ausdrücklich gewünscht haben. Das Einverständnis sollte in jedem Fall schriftlich festgehalten werden, um einen entsprechenden Nachweis zu sichern. Jedenfalls sind Tonaufnahmen grundsätzlich unzulässig. Das heimliche Abhören oder Aufzeichnen nichtöffentlich gesprochener Worte ist strafbar. Bei Videoüberwachungssystemen mit Audiofunktion muss diese dauerhaft und unwiderruflich deaktiviert sein.

Kenntnisse über das Vorhandensein, die Ausrichtung sowie Hersteller und Modell einer Kamera lassen für Betroffene nicht eindeutig erkennen, ob und welche Bereiche überwacht werden. Der Kamerabetreibende kann einzelne Bereiche der Überwachung mittels Software ausblenden, die Kamera könnte abgeschaltet sein oder es könnte sich um eine Attrappe handeln. Der HmbBfDI empfiehlt zunächst den direkten Kontakt mit den Kameranutzenden, um den Sachverhalt ggf.

einvernehmlich zu klären. Insoweit besteht auch die Möglichkeit gem. Art. 15 DSGVO schriftlich Auskunft von diesen zu verlangen. Jedenfalls besteht ein unmittelbares Beschwerderecht bei der Datenschutzaufsichtsbehörde.

Eine kleine Info zuletzt: Die Bürgernahen Beamten (BünaBes) in Hamburg, auch als Besonderer Fußstreifendienst (BFS) bekannt, sind Polizisten, die zu Fuß oder per Fahrrad direkt in ihren Stadtteilen präsent sind, um als Ansprechpartner zu dienen, Vertrauen aufzubauen und bei Problemen zu vermitteln. Der HmbBfDI bedankt sich bei allen Polizist:innen, die mitgeholfen haben, einen datenschutzkonformen Zustand bei den in Hamburg installierten Kameras herzustellen.

18. Fotografie und Datenschutz: Fallbearbeitung und Beratungsangebot

Die Anfertigung und Veröffentlichung von Personenfotografien berühren zentrale datenschutzrechtliche Fragen. Der HmbBfDI erhält regelmäßig Beschwerden zu Internetveröffentlichungen von Personenbildern und stellt ein großes Informationsbedürfnis in der Bevölkerung und bei Verantwortlichen fest. Um Unsicherheiten zu begegnen, baut der HmbBfDI sein Informationsangebot aus und bietet Veranstaltungen für verschiedene Zielgruppen an.

Fotografien von Menschen sind mehr als bloße Bildaufnahmen. Sie enthalten personenbezogene Daten im Sinne der DSGVO, sobald die abgebildete Person identifizierbar ist. Dies gilt unabhängig davon, ob die Identifizierung durch das Gesicht, besondere Merkmale oder den Kontext erfolgt. Die fortschreitende Entwicklung von Gesichtserkennungssoftware und die Verknüpfung mit weiteren Datenquellen erhöhen die Wahrscheinlichkeit, dass Personen auf Fotos erkannt und mit

weiteren Informationen verknüpft werden können. Damit unterliegen sowohl das Anfertigen als auch das Veröffentlichen von Personenbildern den Vorgaben der DSGVO.

Der HmbBfDI erhält regelmäßig Beschwerden von Bürger:innen, die sich durch die Veröffentlichung von Fotos im Internet in ihren Rechten verletzt sehen. Dabei geht es regelmäßig um Bilder, die ohne Einwilligung auf öffentlich zugänglichen Webseiten oder in sozialen Netzwerken geteilt werden. Auch im Rahmen des Projekts #MoinDigitaleVorbilder zeigt sich, dass das Thema Fotografie und Datenschutz in Bildungs- und Beratungsangeboten stark nachgefragt wird. Viele Verantwortliche sind unsicher, welche Vorgaben sie im Umgang mit Personenbildern beachten müssen. Um diesem Bedarf gerecht zu werden, hat der HmbBfDI in den vergangenen Monaten mehrere Veranstaltungen für unterschiedliche Zielgruppen durchgeführt – darunter Eltern, pädagogische Fachkräfte und Vereine. Die Erfahrungen aus diesen Formaten werden in die geplante praxisnahe Weiterentwicklung des Informationsangebots auf der Homepage einfließen.

Verantwortliche, die Personen fotografieren oder solche Bilder veröffentlichen möchten, müssen die datenschutzrechtlichen Anforderungen der DSGVO beachten. Grundsätzlich ist für jede Verarbeitung – also sowohl für das Fotografieren als auch für die Veröffentlichung – eine Rechtsgrundlage erforderlich. Die relevantesten Rechtsgrundlagen sind die Einwilligung der abgebildeten Person (Art. 6 Abs. 1 lit. a DSGVO) oder ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO), das im Einzelfall gegen die Interessen der betroffenen Person abgewogen werden muss. Bei Kindern ist die Einwilligung der Sorgeberechtigten erforderlich, wobei das Kind, abhängig von seiner Einsichtsfähigkeit, angemessen beteiligt werden sollte.

Die Einwilligung muss freiwillig, informiert und eindeutig erfolgen. Sie kann jederzeit widerrufen werden, was im Regelfall dazu führt, dass die betreffenden Bilder gelöscht werden müssen. Bei Veröffentlichungen im Internet ist besonders zu beachten, dass Bilder weltweit abrufbar sind und ihre Verbreitung schwer kontrollierbar ist. Die Risiken von

Missbrauch, auch durch Bildbearbeitung oder automatisierte Auswertung, sind erheblich. Verantwortliche sollten daher vor einer Veröffentlichung sorgfältig prüfen, ob die abgebildeten Personen ausreichend informiert wurden und ob die Veröffentlichung wirklich notwendig ist. Im Rahmen des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DSGVO können laut der Rechtsprechung die Wertungen des Kunsturhebergesetzes (KUG) als Maßstab für die Interessenabwägung herangezogen werden. Das KUG sieht vor, dass eine Veröffentlichung von Personenbildern grundsätzlich nur mit Einwilligung erlaubt ist, es sei denn, eine der dortigen Ausnahmen greift. Hierzu gehören Bilder der Zeitgeschichte, also Fotos von Personen, die wegen ihrer Stellung oder eines besonderen Ereignisses im öffentlichen Interesse stehen. Hier kommt eine Veröffentlichung ohne Einwilligung in Frage, sofern ein berechtigtes Informationsinteresse der Allgemeinheit besteht. Sind Personen als „Beiwerk" nur am Rande und nicht als Hauptmotiv auf einem Foto abgebildet, etwa als Passant:innen auf einem Stadtbild, kann die Veröffentlichung ebenfalls ohne Einwilligung zulässig sein. Das gleiche gilt bei Bildern von Versammlungen oder öffentlichen Veranstaltungen, sofern nicht einzelne Personen herausgestellt werden. Alle diese Ausnahmen gelten jedoch nur, wenn durch die Veröffentlichung keine berechtigten Interessen der abgebildeten Person verletzt werden. Insbesondere bei Bildern aus dem privaten oder intimen Bereich, bei Kindern oder bei erkennbar schutzbedürftigen Personen überwiegen die Interessen der Betroffenen zumeist.

Ausnahmen gelten etwa im journalistischen oder künstlerischen Bereich, wo die DSGVO in weiten Teilen nicht anwendbar ist und der HmbBfDI keine Befugnisse zu Prüfungen und Maßnahmen hat.

Der HmbBfDI empfiehlt, bei Veranstaltungen und in öffentlichen Räumen auf das Fotografieren und die geplante Verwendung von Bildern hinzuweisen, etwa durch Aushänge oder Informationen in Einladungen. Bei Unsicherheiten sollten die Personen im Zweifel unkenntlich gemacht werden. Die Betroffenen haben das Recht auf Auskunft, Berichtigung und gegebenenfalls Löschung ihrer Daten sowie auf Widerspruch gegen die Verarbeitung.

Die Vielzahl der Anfragen und Beschwerden zeigt, dass das Thema Fotografie und Datenschutz weiterhin hohe praktische Relevanz hat. Der HmbBfDI wird daher sein Informationsangebot weiter ausbauen und die Öffentlichkeit durch gezielte Bildungs- und Beratungsmaßnahmen unterstützen, um Betroffene zu unterstützen und Verantwortlichen Orientierung zu bieten.

19. Fotografie in der Kita

In vielen Kindertagesstätten werden regelmäßig Fotos angefertigt. Der HmbBfDI hat sich im Rahmen eines Beschwerdeverfahrens umfangreich mit der Zulässigkeit von Fotoanfertigung im Kontext der Kinderbetreuung in Kindertagesstätten auseinandergesetzt und zudem im Januar 2025, anlässlich des Europäischen Datenschutztages, einen Leitfaden zum Thema veröffentlicht.

Den HmbBfDI erreichte eine Beschwerde über eine Hamburger Kindertagesstätte. Bei der Betreuung soll es zu Fotoanfertigungen durch eine Mitarbeiterin im Qualitätsmanagement gekommen sein, ohne dass hierfür eine wirksame Einwilligung der Sorgeberechtigten eingeholt worden ist. Nach Anhörung der Einrichtung durch den HmbBfDI wurde deutlich, dass sich die Kindertagesstätte nicht hinreichend mit der eigenen Praxis der Fotoanfertigung auseinandergesetzt hatte. Es wurden unterschiedliche, sich widersprechende Gründe für die erfolgte Fotoanfertigung betreuter Kinder vorgetragen. Teilweise wurde argumentiert, dass die Anfertigung mit einer Einwilligung der Sorgeberechtigten erfolgt war. Zudem hieß es, dass die Anfertigung Teil einer erforderlichen Entwicklungsdokumentation und der Portfolioarbeit sei. In diesem Zusammenhang müssten kindliche Entwicklungsprozesse auch bildlich dokumentiert werden. Später wurde angeführt, dass die konkreten Fotos im Rahmen der eigenen Qualitätsentwicklung angefertigt wurden.

Für beträchtliche Irritation sorgte der zwischenzeitliche Vortrag, dass es sich bei den im Einwilligungsformular aufgeführten Zwecken der Datenverarbeitung um „Quasi - Bedingungen" für die Betreuung der Kinder in der Kindertageseinrichtung handele. Wenn Eltern diesen nicht zustimmten, werde kein Betreuungsvertrag abgeschlossen. Für eine Differenzierung der einzelnen Zwecke sei kein Raum. Die Zwecke umfassten unter anderem auch die Veröffentlichung von Fotos in Medien, wie „z. B. Webseiten". Das für die Fotoanfertigung verwendete Einwilligungsformular wies darüber hinaus zahlreiche weitere Mängel auf.

Die Erfahrungen aus dem vorstehend skizzierten Verfahren zeigen, wie wichtig es für Kindertagesstätten ist, vor der Anfertigung von Fotos ein klares Konzept zum Umgang mit Fotos zu erstellen, um diesbezüglich den Sorgeberechtigten bereits bei Vertragsschluss Rede und Antwort stehen zu können und den eigenen Mitarbeitenden einen rechtssicheren Rahmen für die Arbeit geben zu können. Die Kita bzw. sämtliche Ansprechpartner der Sorgeberechtigten und solche Mitarbeiter:innen, die Fotos anfertigen, müssen wissen, für welche Anlässe Fotoaufnahmen angefertigt werden sollen und wie die Verarbeitung erfolgen soll. Dabei kann eine wirksame Rechtsgrundlage zur Anfertigung nur eine Einwilligung der Sorgeberechtigten sein (Näheres hierzu kann der Veröffentlichung vom 28.01.2025 entnommen werden: https://datenschutz-hamburg.de/news/zum-europaeischen-datenschutz-tag-so-geht-fotografie-in-der-kita).

Natürlich darf es nicht sein, dass Kitas die Einwilligung zur Bedingung der Betreuung machen. In dem Fall wäre die Einwilligung unwirksam, da sie nicht freiwillig (vgl. Art. 4 Nr. 11 DSGVO), sondern unter dem Druck der Kitaplatzvergabe erteilt wurde. Die Drucksituation von Sorgeberechtigten bei der Suche einer Kita darf nicht für die eigenen Interessen der Kindertagesstätte ausgenutzt werden. Eine gesetzliche Grundlage im Sinne von Art. 6 Absatz 1 Satz 1 lit. e DSGVO, die das Fertigen von Fotos für die Entwicklungsdokumentation vorsieht oder begründen könnte, findet sich im Übrigen in den einschlägigen Fachgesetzen nicht.

Der HmbBfDI konnte im weiteren Verlauf des Verfahrens auf Seiten der verantwortlichen Stelle eine Sensibilisierung für die datenschutzrechtlichen Aspekte bei der Fotoanfertigung in Kindertagesstätten erwirken und die Einrichtung bei der Überarbeitung des Einwilligungsformulars unterstützen. Eine Fotoanfertigung zu einem feststehenden Zweck soll nunmehr nur noch bei vorliegender Einwilligung der Sorgeberechtigten erfolgen. Der Mehraufwand, der der Kita entsteht, ist hinzunehmen.

Die Zusammenfassung der wesentlichen Anforderungen findet sich in der Veröffentlichung des HmbBfDI „Fotografie in der Kindertagesstätte“ vom 28.01.2025.

20. Unerwünschte Werbung und mangelhafte Umsetzung von Betroffenenrechten

Die im Berichtszeitraum beim HmbBfDI eingegangenen Beschwerden zu unerwünschter Werbung bezogen sich nicht nur auf den Erhalt von postalischen, elektronischen oder telefonischen Werbenachrichten selbst, sondern betrafen in erheblichem Umfang auch die unzureichende oder fehlerhafte Bearbeitung von Betroffenenrechten gemäß den Art. 12 bis 23 DSGVO.

Im Bereich Werbung verzeichnete der HmbBfDI auch 2025 einen deutlichen Anstieg von Beschwerden, insbesondere im Zusammenhang mit E-Mail-Werbung. Nach den Erkenntnissen des HmbBfDI stammen die für Werbezwecke genutzten E-Mail-Adressen und die damit verbundenen personenbezogenen Daten – wie der Vor- und Nachname – häufig aus öffentlich zugänglichen Quellen, etwa von Internetpräsenzen der betroffenen Personen. Bei der Erhebung der Daten werden vorrangig automatisierte Verfahren durch Tools zum großflächigen Auslesen von Daten aus dem Internet (sog. „Scraping“), insbesondere aus sozialen Netzwerken, eingesetzt.
Über diese Thematik wurde bereits im Tätigkeitsbericht des HmbBfDI

2024 (vgl. 33. TB, Kap. II 10) ausführlich berichtet. Die anhaltend hohe Zahl der Eingaben beim HmbBfDI lässt darauf schließen, dass das Unrechtsbewusstsein bei den verantwortlichen Unternehmen in diesem Bereich weiterhin unzureichend ausgeprägt zu sein scheint.

Da es sich bei diesen E-Mail-Adressen und den zugehörigen Daten um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO handelt, unterliegt deren Verarbeitung den Vorgaben der DSGVO. Jede Verarbeitung – einschließlich der Erhebung und Speicherung – bedarf einer entsprechenden Rechtsgrundlage. Bereits bei der Erhebung personenbezogener Daten sind die Informationspflichten nach Art. 13 und 14 DSGVO zu erfüllen. Auch wettbewerbsrechtliche Vorgaben sind zu beachten. Datenschutzrechtlich relevante Aspekte sind bereits am Anfang der Planung von Werbemaßnahmen sorgfältig zu prüfen. Gegebenenfalls sollte frühzeitig fachkundige Beratung eingeholt werden.

Ein weiteres zentrales Problemfeld war die nicht oder nicht ordnungsgemäß erfolgte Bearbeitung von Betroffenenrechten. Insbesondere Werbewidersprüche wurden häufig nicht umgesetzt, was dazu führte, dass betroffene Personen weiterhin Werbenachrichten erhielten. Technische Fehler in den eingesetzten CRM-Systemen trugen dazu bei, dass Widersprüche nicht korrekt verarbeitet wurden.

Auch bei Auskunftsersuchen nach Art. 15 DSGVO kam es zu Versäumnissen: Auskünfte wurden entweder gar nicht, verspätet oder unvollständig erteilt. Auffällig war, dass die Bearbeitung von Betroffenenanfragen oftmals durch nicht ausreichend datenschutzrechtlich qualifizierte Mitarbeiter:innen im Kundendienst oder, insbesondere bei kleineren Unternehmen, direkt durch die Geschäftsführung selbst erfolgte, was zu fehlerhaften oder irreführenden Auskünften führte. In vielen Fällen hätten ordnungsgemäß bearbeitete Anfragen Beschwerden beim HmbBfDI verhindern können.

Der HmbBfDI weist darauf hin, dass Unternehmen, die personalisierte

Werbemaßnahmen – sei es per E-Mail, Post oder Telefon – planen, damit rechnen müssen, dass Werbeempfänger ihre Betroffenenrechte geltend machen. Unternehmen sollten sicherstellen, dass Anfragen von Betroffenen an entsprechend geschulte Mitarbeiter weitergeleitet und fristgerecht bearbeitet werden. Die Bearbeitung von Betroffenenanfragen muss fristgerecht innerhalb eines Monats erfolgen (Art. 12 Abs. 3 DSGVO) und Auskünfte sollten sämtliche nach Art. 15 DSGVO erforderlichen Informationen enthalten und vollständig sein.

Es ist unerlässlich, die internen Prozesse zur Bearbeitung von Betroffenenanfragen im Vorfeld von Werbemaßnahmen zu überprüfen und gegebenenfalls in Abstimmung mit dem Datenschutzbeauftragten oder externer Rechtsberatung anzupassen.

Im Rahmen der Bearbeitung von Beschwerden stellte der HmbBfDI im Bereich Werbung wiederholt Verstöße gegen diese datenschutzrechtlichen Vorgaben fest. Im Berichtszeitraum wurden diesbezüglich 17 Maßnahmen nach Art. 58 Abs. 2 DSGVO verhängt, davon vier Bußgelder. Der HmbBfDI wird hier auch künftig die Einhaltung der datenschutzrechtlichen Vorgaben aufmerksam überwachen und bei Verstößen konsequent einschreiten.

21. Transparenz bei Online-Bestellungen mit Bonitätsabfrage

Beschwerden zur mangelnden Transparenz im Online-Bestellprozess eines großen Versandhandelsmarktplatzes haben den HmbBfDI veranlasst, sich mit der Frage zu beschäftigen, ob die Kundschaft über die Übermittlung personenbezogener Daten an Wirtschaftsauskunfteien zum Zwecke von Bonitätsprüfungen hinreichend transparent informiert wird und ob sich die bestehenden Informationsprozesse weiter verbessern lassen.

Im Berichtszeitraum erreichten den HmbBfDI wiederholt Beschwerden,

die sich auf die Durchführung von Bonitätsprüfungen bei Bestellungen auf einem großen Online-Versandhandelsmarktplatz bezogen.

Wird bei einer Bestellung eine sogenannte „unsichere" Zahlungsart wie Rechnungskauf oder Ratenzahlung ausgewählt, so entsteht für das Unternehmen ein kreditorisches Risiko. Der Hintergrund ist, dass die bestellte Ware versandt wird, bevor der Kaufpreis bezahlt wurde. Das Unternehmen ist daher darauf angewiesen, dass die bestellende Person sowohl bereit als auch in der finanziellen Lage ist, den Kaufpreis nachträglich oder in Ratenform zu begleichen.

Kann das Unternehmen das Risiko eines Zahlungsausfalls bei Bestellungen mit „unsicherer" Zahlungsart nicht selbst abschätzen, besteht grundsätzlich in datenschutzrechtlich zulässiger Weise eine Berechtigung, den Bonitätsscore der bestellenden Person bei einer Wirtschaftsauskunftei – etwa der Schufa Holding AG – abzurufen. Der Abruf erfolgt in Echtzeit durch Übermittlung der hierfür erforderlichen Daten der bestellenden Person; zudem werden Datum und Anlass einer solchen Anfrage bei der Wirtschaftsauskunftei gespeichert. Häufen sich entsprechende Anfragen, kann dies den Bonitätsscore der bestellenden Person negativ beeinflussen.

Im Mittelpunkt der Prüfung stand insoweit nicht die Rechtmäßigkeit dieses marktüblichen Verfahrens an sich, sondern die Frage, in welchem Maß im Bestellprozess nachvollziehbar und verständlich darüber informiert werden, dass und in welchem Umfang personenbezogene Daten im Rahmen von Bonitätsprüfungen an Wirtschaftsauskunfteien übermittelt werden.

Der betroffene Online-Versandhandelsmarktplatz hatte bereits verschiedene Hinweise und Informationen zur Bonitätsprüfung in den Bestellprozess und die Datenschutzerklärungen integriert. Aus Sicht des HmbBfDI bestand jedoch noch Optimierungsbedarf, insbesondere im Hinblick auf die Auffindbarkeit, Verständlichkeit und Eindeutigkeit der bereitgestellten Informationen. So waren Hinweise auf Bonitätsprüfungen teilweise nur an weniger prominenter Stelle zu finden, und

die Darstellung der betroffenen Zahlungsarten erfolgte nicht immer konsistent und einheitlich. Auch die möglichen Auswirkungen einer Bonitätsanfrage auf den Bonitätsscore wurden nicht ausreichend transparent erläutert.

Vor diesem Hintergrund wandte sich der HmbBfDI an das Unternehmen, um konkrete Verbesserung der Informationslage für die Nutzenden anzuregen und deren Umsetzung einzufordern. Ziel war es, dass die Kundschaft bereits vor Abschluss einer Bestellung klar und verständlich darüber informiert wird, ob und in welchem Umfang eine Bonitätsprüfung stattfindet, welche Daten dabei an Dritte übermittelt werden und welche möglichen Folgen dies haben kann.

Das Unternehmen setzte daraufhin mehrere Verbesserungsmaßnahmen um. Hinweise auf Bonitätsprüfungen wurden im Bestellprozess – insbesondere bei der Auswahl der Zahlungsarten – deutlicher hervorgehoben und verständlicher formuliert. Zudem wurden die Angaben zu den betroffenen Zahlungsarten vereinheitlicht und die Datenschutzerklärungen entsprechend angepasst. Auch die potentiellen Auswirkungen einer Bonitätsanfrage auf den Bonitätsscore werden nun transparenter dargestellt.

Der HmbBfDI begrüßt diese Maßnahmen als datenschutzfreundlichen Fortschritt, der zu spürbaren Verbesserungen im Bestellprozess führt. Die erhöhte Transparenz trägt zudem dazu bei, Missverständnisse und Unsicherheiten im Zusammenhang mit Datenverarbeitungen bei Bonitätsprüfungen zu reduzieren. Die deutlichen Hinweise im Bestellprozess zeigen exemplarisch, wie Datenschutzgrundsätze – insbesondere der Transparenzgrundsatz gemäß Art. 5 Abs. 1 lit. a DSGVO – in der Praxis umgesetzt werden können. Der HmbBfDI wird sich auch künftig für eine transparente und datenschutzkonforme Gestaltung digitaler Geschäftsprozesse einsetzen.

22. Neue Speicherfristen für Kundendaten

Mit dem Vierten Bürokratieentlastungsgesetz sind Speicherfristen aus der Abgabenordnung und dem Handelsgesetzbuch teilweise verkürzt worden. Daher sind bei der jährlichen Routinelöschung im Unternehmen Anfang 2025 mehr Daten als üblich zu bereinigen gewesen. Der HmbBfDI hat die Änderung zum Anlass genommen, zu einem digitalen Frühjahrsputz aufzurufen.

Wenn digitale Dokumente und Papierakten personenbezogene Daten enthalten, dürfen sie nach der DSGVO nur so lange aufbewahrt werden, wie es erforderlich ist. Mindestens einmal im Jahr ist es deshalb Zeit, sich einen Überblick zu verschaffen, was noch gespeichert ist und ob diese Daten oder Akten länger benötigt werden. Professionelle Datenverarbeiter erledigen dies automatisiert. Wo keine automatischen Routinen etabliert sind, muss händisch gelöscht werden.

Für viele Dokumente gibt es gesetzlich festgelegte Mindestspeicherfristen. Diese ergeben sich zumeist aus § 147 der Abgabenordnung (AO) und § 257 des Handelsgesetzbuchs (HGB) mit einem abgestuften System aus sechs, acht und zehn Jahren. Detaillierte Überblicke darüber, was wie lange vorzuhalten ist, hat unter anderem die Hamburgische Handelskammer veröffentlicht. Je nach Datenart und Geschäftszweig kommen teilweise spezielle Fristen hinzu. So haben beispielsweise Arztpraxen die berufsrechtliche Zehn-Jahres-Frist aus § 630f des Bürgerlichen Gesetzbuchs (BGB) oder auch die 30-Jahres-Frist der Strahlenschutzverordnung (StrlSchVO) zu beachten. Ein anderes Beispiel für besondere Fristen trifft Arbeitgeber, die unter anderem Aufzeichnungen zur geleisteten Arbeitszeit, zum Jugendschutz und zum Mutterschutz zwei Jahre lang aufbewahren müssen.

Wenn die Speicherfristen abgelaufen sind, müssen die Daten in der Regel unverzüglich gelöscht werden. Das Datenschutzrecht verlangt

jedoch keine sofortige Löschung in der Silvesternacht – je nach Komplexität des Systems kann der Prozess einige Wochen bis Monate dauern. Wichtig ist, dass er zum Jahresbeginn direkt eingeläutet wird. Bis zum Frühlingsbeginn sollte die jährliche Löschung abgeschlossen sein.

Im Jahr 2025 war beim digitalen Frühjahrsputz besondere Aufmerksamkeit geboten. Der Bundesgesetzgeber hat einige Aufbewahrungsfristen verkürzt, sodass auch die betroffenen Daten früher gelöscht werden müssen. Mit dem Vierten Bürokratieentlastungsgesetz sind die AO und das HGB angepasst worden. Die in der Praxis wichtigste Fallgruppe der Belege zu Buchungen muss jetzt acht Jahre anstelle der bisherigen zehn aufbewahrt und danach gelöscht werden. Für andere Dokumentenarten wie zum Beispiel Handelsbücher und Jahresabschlüsse bleibt es bei der Frist von zehn Jahren. Diese Gesetzesänderungen hatten zur Folge, dass im Frühjahr 2025 deutlich mehr Datenfelder bereinigt und die Löschkonzepte angepasst werden mussten. Für die Bereiche der Kredit- und Versicherungswirtschaft hat der zwischenzeitlich infolge der Bundestagswahl neu formierte Gesetzgeber diese Änderungen im Dezember 2025 teilweise wieder rückgängig gemacht. Diese im Gesetz zur Modernisierung und Digitalisierung der Schwarzarbeitsbekämpfung genannten Branchen müssen ihre Löschkonzepte damit nun ein zweites Mal innerhalb kurzer Zeit anpassen.

Auch personenbezogene Daten, für die es keine gesetzliche Aufbewahrungsfrist gibt, müssen gelöscht werden, wenn sie nicht mehr benötigt werden. Hier sind Unternehmen verpflichtet, sich einen Überblick zu verschaffen, wie lange diese Daten typischerweise Verwendung finden. In einem Löschkonzept sind dann eigenständige Löschfristen zu entwickeln, zu dokumentieren und intern umzusetzen. Die Länge der Fristen kann dabei, je nach Datenart und Geschäftszweig, stark variieren. Hilfestellung bei der internen Entscheidung geben in der Regel die jeweiligen Branchenverbände. Es kann auch sinnvoll sein, sich an zivilrechtlichen Verjährungsfristen zu orientieren. Für die Löschung datenschutzrechtlicher Dokumentationen zum Beispiel zur Beantwortung eines Auskunftsantrags bietet es sich an, sich an der dreijährigen Verjährungsfrist für Ordnungswidrigkeiten zu orientieren.

Dem HmbBfDI ist vor allem wichtig, dass Unternehmen sich ein nachvollziehbares Löschkonzept gegeben haben und die daran anschließende Löschung auch tatsächlich funktioniert. Wie lange die im Konzept verankerten Fristen sind, kann das jeweilige Unternehmen am besten einschätzen. Die Aufsichtsbehörde stellt dabei keine Zeitspannen in Frage, die auf unternehmerischer Erfahrung basierend plausibel begründet werden, solange sie nicht exzessiv ausgedehnt werden.

Die konzeptionelle und faktische Umsetzung des Löschgebots ist ein Schwerpunktthema des HmbBfDI. Bei Routinekontrollen der Datenhaltung in Unternehmen wird regelhaft nach Aufbewahrungsfristen und Löschprozessen gefragt. Im Rahmen einer strukturierten Stichprobenaktion hat der HmbBfDI beispielsweise die entsprechende Praxis bei Dienstleistern des Forderungsmanagements überprüft. In dem Zusammenhang hat er Ende 2024 gegen ein Unternehmen ein Bußgeld in Höhe von 900.000 Euro wegen unzureichender Datenlöschung verhängt (vgl. 33. TB 2024, Kap. V 1). In einem weiteren Fall der Branche hat er im Jahr 2025 ein weiteres Bußgeld im fünfstelligen Bereich verhängt. Das Thema Datenlöschung ist auch europaweit in den Fokus gerückt als Jahresthema des Coordinated Enforcement Framework der Mitglieder des Europäischen Datenschutzausschusses.

23. Handreichung zur Prüfung des berechtigten Interesses

Der HmbBfDI hat eine praxisnahe Handreichung zur Prüfung und Dokumentation des berechtigten Interesses nach Art. 6 Abs. 1 lit. f) DSGVO veröffentlicht. Die Handreichung soll Verantwortlichen und Datenschutzbeauftragten eine strukturierte Orientierung bieten und die Transparenz sowie Nachvollziehbarkeit der datenschutzrechtlichen Entscheidungsprozesse stärken.

Das „berechtigte Interesse" ist eine der sechs Rechtsgrundlagen, die die DSGVO für die Verarbeitung personenbezogener Daten vorsieht.

Gerade weil der Gesetzgeber diesen Erlaubnistatbestand offen formuliert hat, ergeben sich in der Praxis häufig Unsicherheiten und Abgrenzungsfragen. Verantwortliche stehen regelmäßig vor der Herausforderung, zu beurteilen, ob ein berechtigtes Interesse tatsächlich und rechtssicher vorliegt, wie die erforderliche Interessenabwägung vorzunehmen ist und wie die Entscheidung nachvollziehbar dokumentiert werden kann.

Checklisten und Handreichungen die die Anwendung des berechtigten Interesses praxisnah und schematisch aufbereiten, existieren bislang nur vereinzelt und überwiegend in englischer Sprache (Legitimate Interest Assessment / LIA).

Vor diesem Hintergrund hat der HmbBfDI eine Handreichung entwickelt, die sich an den aktuellen Empfehlungen des Europäischen Datenschutzausschusses (EDSA Guidelines 1 / 2024) orientiert. Ziel ist es, insbesondere Praktiker:innen eine systematische und nachvollziehbare Prüfung der Voraussetzungen des berechtigten Interesses zu ermöglichen. Die Handreichung ist als modularer Fragenkatalog konzipiert und unterstützt dabei, die wesentlichen Aspekte der Interessenabwägung zu erfassen und zu dokumentieren. Sie bietet eine praxisnahe Hilfestellung, ohne dabei den Anspruch auf Ersatz einer rechtlichen Beratung zu erheben.

Die Handreichung ist modular gestaltet und kann je nach Komplexität der jeweiligen Datenverarbeitung angepasst genutzt werden. Der HmbBfDI empfiehlt, die Interessenabwägung objektiv und unter Berücksichtigung der eigenen Interessen, der Interessen Dritter sowie der Rechte und Freiheiten der betroffenen Personen vorzunehmen. Sollten Zweifel bestehen oder die Interessen der Betroffenen möglicherweise überwiegen, ist es ratsam, die technischen und organisatorischen Maßnahmen zu überprüfen und sicherzustellen, dass die Grundsätze der DSGVO konsequent umgesetzt werden.

Mit der Bereitstellung dieser Handreichung möchte der HmbBfDI dazu beitragen, Unsicherheiten bei der Anwendung des berechtigten In-

teresses zu reduzieren und die datenschutzkonforme Verarbeitung personenbezogener Daten zu fördern. Sie dient als Hilfestellung zur Dokumentation der Interessenabwägung und eignet sich als Nachweis der Vornahme einer umfangreichen Prüfung des „berechtigten Interesses".

Die Handreichung des HmbBfDI ist auf der Website des HmbBfDI abrufbar (https://datenschutz-hamburg.de/news/hmbbfdi-veroeffentlicht-fragenkatalog-zur-interessenabwaegung-nach-dsgvo). Eine englischsprachige Fassung steht zur Verfügung.

24. „Fastlane" für Databreaches mit technischem Schwerpunkt

Seit dem Sommer 2024 werden Databreach-Fälle, deren Ursachen technischer Natur sind, direkt vom Referat Technischer Datenschutz (T) in einer Fastlane bearbeitet. Durch dieses Vorgehen sollen technische Sachverhalte schneller eingeschätzt werden können. So kann bei den verantwortlichen Stellen auf eine zeitnahe Abhilfe hingewirkt und eine schnellstmögliche Benachrichtigung der Betroffenen erreicht werden. Insgesamt sind die Databreach-Fälle weiter angestiegen.

Zu den Aufgaben des HmbBfDI gehört die Entgegennahme von Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO, auch Datenschutzvorfälle oder Databreaches genannt.

Neben der Prüfung auf Einhaltung der gesetzlichen Vorgaben – etwa die fristgerechte Meldung innerhalb von 72 Stunden nach Kenntnis vom Datenschutzvorfall – steht vor allem die Bewertung der Risiken für die betroffenen Personen im Vordergrund. Hierbei geht es auch um die Frage, ob ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht, aus der nach Art. 34 DSGVO die Pflicht zur Benachrichtigung über den Vorfall folgt.

In der Vergangenheit war eine Zunahme von Fällen zu beobachten, die einen technischen Schwerpunkt haben, also nicht durch menschliche Fehler wie etwa ein Fehlversand von E-Mails verursacht wurden. Hierzu zählen insbesondere Datenschutzvorfälle, die durch erfolgreiche Phishing- und Ransomware-Angriffe oder aber auch durch Softwarefehler verursacht werden. Bei diesen Fällen sind für die Risikobewertung tiefgehende technischen Kenntnisse erforderlich.

Aus diesem Grund wurde zur Bearbeitung von Databreaches mit technischem Schwerpunkt beim HmbBfDI eine Fastlane eingerichtet. Ziel dieser Verfahrensweise ist die beschleunigte Erstprüfung der technischen Sachverhalte, um die Risiken für die Betroffenen möglichst zeitnah beurteilen zu können. Die schnelle Bearbeitung der Fälle ermöglicht es häufig, die eigenen Untersuchungen durchführen zu können, bevor die Ursache des Datenschutzvorfalles durch den Verantwortlichen behoben werden konnte. So wird der HmbBfDI dazu befähigt, frühzeitig beratend die Verantwortlichen zu unterstützen. Ziel ist es darauf hinzuwirken, dass schnellstmöglich die Ursachen des Databreaches abgestellt und alle betroffenen Personen umfassend benachrichtigt werden, so dass diese auch eigene Schutzmaßnahmen ergreifen können.

Innerhalb der Fastlane für Datenschutzvorfälle mit technischem Schwerpunkt kommt es zur Umkehr der Federführung zwischen Jurist:in und Techniker:in. Bisher wurden alle Databreach-Fällen zunächst federführend durch ein:e Jurist:in bearbeitet, die dann ggf. Unterstützung bei den zuständigen Techniker:innen anfordern konnte. Seit diesem Jahr wird diese Verantwortung bei den Themenbereichen Hacking und Softwarefehler umgedreht. Während die verantwortlichen Techniker:innen die Federführung haben, werden sie in diesen Fällen von den für die jeweiligen Themenbereiche zuständigen Jurist:innen auf Anfrage unterstützt.

Falltypen
Meldungen aufgrund von Ransomeware-Angriffen gehören zu den typischen Fällen, die über die Fastlane direkt im Referat Technischer Datenschutz bearbeitet werden. Bei diesen können häufig Datenleaks im Darknet gefunden werden, die den verantwortlichen Stellen entweder noch nicht bekannt waren oder in der Meldung keine Erwähnung gefunden haben. Die Veröffentlichung dieser Datensätze erfolgt in der Regel durch die Ransomware-Gruppe, um nicht-zahlungswillige Erpressungsopfer weiter unter Druck zu setzen oder nach endgültiger Zahlungsverweigerung gegenüber zukünftigen Opfern mehr Glaubwürdigkeit hinsichtlich ihrer Drohungen zu erlangen. Dadurch werden nicht selten auch die Daten von Dritten wie Kund:innen oder Geschäftspartner:innen öffentlich.

Datenschutzvorfälle als Folge von Phishing-Attacken machen ebenfalls einen größeren Anteil innerhalb der Fastlane aus. Dabei ist zu beobachten, dass auch Zweifaktorauthentifizierung (2FA) überwunden wird. Der Beratung der verantwortlichen Stellen hinsichtlich Phishing-resistenter Authentifizierung durch einen Universal Second Factor (U2F) bzw. Standards aus dem FIDO2 Konsortium (PassKeys) kommt hierbei eine wichtige Bedeutung zu.

Bei durch Softwarefehlern ausgelösten Databreaches muss häufig zunächst festgestellt werden, in wessen Systemen der Fehler aufgetreten ist. Insbesondere wenn die fehlerhafte Software nicht bei der für die Datenverarbeitung verantwortlichen Stelle direkt entwickelt und/oder eingesetzt wird, sondern beispielsweise bei einem Auftragsverarbeiter, bedarf die Aufklärung des Sachverhaltes eines tiefen Verständnisses von Software- und Schnittstellenarchitekturen. Die Auftragsverarbeiter halten sich gegenüber den verantwortlichen Stellen nicht selten bedeckt, was die Details der Softwarefehler betrifft. Hier können die technischen Referent:innen dazu beitragen, der verantwortlichen Stelle bei der Analyse der Ursachen zu helfen und ihre Ansprüche auf datenschutzkonforme Abhilfe gegenüber den Auftragsverarbeitern durchzusetzen. Teilweise können auch weitere Kunden der Auftragsverarbeiter identifiziert werden, die von dem gleichen Softwarefehler

betroffen waren und bisher entweder keine Kenntnis von einem daraus resultierenden Datenschutzvorfall erlangt haben oder diesen nicht gemeldet haben.

> Fallschilderung Softwarefehler:

Zu den bemerkenswerten Einzelfällen aus der Fastlane gehört der Databreach bei einem Dienstleister in der Gastronomie. Das Unternehmen bietet eine Software as a Service zur Bestellungsabwicklung für Restaurants an. Diese wird momentan von mehreren hundert Restaurants eingesetzt.

Der Fall wurde durch einen Hinweis vor fast einem Jahr eröffnet und beschäftigt den HmbBfDI bis heute. Es begann mit einer kleinen Sicherheitslücke, die das Auslesen von Rechnungen anderer Personen ermöglichte. Hierfür war lediglich das Hochzählen einer Nummer ausreichend. Solche Sicherheitslücken werden als „Insecure Direct Object Reference" (IDOR) bezeichnet. Diese weit verbreitete Art von Fehler ist leicht zu finden und zu beheben. Um solche Lücken zu verhindern, muss ein geeignetes Rechte- und Rollenkonzept vorliegen. Ob eine Person auf andere Objekte zugreifen kann, muss bei jedem Zugriff überprüft werden. Zusätzlich kann hier helfen, keine einfachen Nummern zu verwenden, die schlicht hochgezählt werden können kann. Für Referenzen sollte hier z. B. auf UUIDs zurückgegriffen werden.

Bei der weiteren Analyse haben sich schnell zusätzliche Sicherheitslücken gezeigt. Nach kurzer Zeit war es gelungen, über Cross-Site-Scripting (XSS) an Anmeldedaten von anderen Benutzer:innen einschließlich dem Admin-Account zu gelangen. Zusätzlich fanden sich vergessene und öffentlich zugängliche Backups von Programmcode und Datenbankinhalten. In diesen befanden sich dann hartkodierte Zugangsdaten für weitere Systeme wie unter anderem Datenbankserver.

Auch die angeblich behobene IDOR war nach wie vor präsent. Es wurden nur die Rechnungen gelöscht, auf die wir zugegriffen hatten. Diese IDOR ist an mancher Stelle immer noch zugänglich. Bei den weiteren aufgefundenen Lücken handelt es sich um „SQL Injections", fehlende Authentifizierung bei Admin-Dashboards,

Fehlernachrichten, die zu viele Informationen preisgeben, und Remote Code Execution (RCE). All diese Fehler haben immer zu einem kompletten Verlust der Daten führen können.
Erschwerend kommt hinzu, dass der Verantwortliche erst geantwortet hat, nachdem wir eine Zwangsanordnung versendet hatten. Unsere Aufgabe als Aufsichtsbehörde bestand erst einmal darin, den Verantwortlichen auf den nicht datenschutzkonformen Zustand hinzuweisen und darauf hinzuwirken, dass dieser hergestellt wird. Dies wurde über mehrere Runden von Meldungen getan. Zum Zeitpunkt des Beitrags war dieser Zustand immer noch nicht hergestellt, weswegen wir uns auch in 2026 mit diesem Fall befassen werden.
Für uns als Behörde war herausfordernd, diese Lücken immer wieder belegen zu müssen. Eine dafür unterstützende Infrastruktur soll deshalb im Jahr 2026 aufgebaut werden.
Als Behörde wollen wir uns hier auch für die Hinweise von Sicherheitsforscher:innen bedanken. Diese haben einen großen Beitrag geleistet, dieses Fehlverhalten aufzudecken.

> Fallschilderung Ransomware:
Als Beispiel für Ransomeware-Fälle kann der Fall bei einem weiteren Dienstleister dienen. Dieser meldete uns im Januar 2025 einen Ransomeware-Angriff. Zuerst betraf dies nur die Büroinfrastruktur der Firma. Nachdem der Zustand der Infrastruktur wieder hergestellt wurde, kam es aber zu einem weiteren Befall. Es stellte sich heraus, dass sich die Ransomeware-Gruppe bereits seit dem Sommer 2024 in ihrem Netzwerk aufgehalten hat. Dies ist eine typische Vorgehensweise. Oft agieren Ransomware-Gruppen in drei Phasen:
In der ersten werden einfache Ziele im Internet gesucht. In diesem Fall handelt es sich um die Gruppe Lynx, welche ein Ransomware-As-A-Service benutzt – also eine Gruppe mit weniger technischem Sachverstand, die eingekaufte Lücken und Techniken nutzt. Aktuell werden Firewalls von verbreiteten Herstellern angegriffen, da diese häufig eklatante Lücken aufweisen. Eine andere Methodik ist es, Zugangsdaten von erfolgreichen Phishingversu-

chen einzukaufen. Nach dem Einstieg durch die Firewall finden die Angreifer:innen häufig ein offenes Netzwerk vor, in dem keine weiteren Sicherheitsmaßnahmen überwunden werden müssen. Sie können sich frei im Netz von Server zu Server und von Client zu Client bewegen.

In der ersten Phase wird meist nur dafür gesorgt, den erneuten Zugang zu sichern, indem eine Backdoor platziert wird. Anschließend ziehen sich die Angreifer:innen zunächst wieder aus dem Netzwerk zurück. Dieser erste Schritt läuft in der Regel komplett automatisiert ab. In diesem konkreten Fall haben wir nicht bestimmen können, ob eine Sicherheitslücke ausgenutzt wurde oder einfach Zugangsdaten mit administrativen Rechten aus dem Darknet gekauft wurden.

Erst in der zweiten Phase prüfen die Ransomeware-Gruppen, welche Ziele erfolgreich infiltriert wurden. Anhand der IP-Adresse und des Netzwerks, zu dem die Gruppe nun Zugang hat, wird überprüft, ob sich ein weiteres Vorgehen lohnt – also das Unternehmen für die manuelle dritte Phase ausgewählt wird. Im vorliegenden Fall wäre auch denkbar, dass der Zugang weiterverkauft wurde, da die kompromittierten Informationen auch für andere, staatliche Akteure interessant sein können.

Erst in der dritten Phase erfolgt der eigentliche Ransomeware-Angriff – also die Verschlüsslung sowie die Exfiltration der Daten. Durch das Ausleiten der Daten wird ein weiteres Druckmittel aufgebaut mit dem Hinweis auf die mögliche Veröffentlichung.

In diesem Fall, hat die Gruppe die Daten verschlüsselt und einen großen Teil aus dem Firmennetzwerk exportiert. Aufgrund fehlender Sicherheitssoftware war es möglich, ungehindert im Netzwerk in andere Rechner einzudringen. Lediglich ein Server wurde mittels Sophos Endpoint Protection überwacht. Diese wurde allerdings sofort deaktiviert, so dass keine weiteren Alarme ausgelöst wurden. Nach dem aufgefallen war, dass ein Administrator ungewöhnliche Zugriffe anfordert, flog die Anwesenheit der Ransomware-Gang auf. Nachdem diese bemerkt wurde, beschleunigten die Angreifer:innen ihr Vorgehen und gingen dazu über, die virtuellen Maschinen der Büroinfrastruktur mittels einer Sicherheitslücke

ebenfalls zu verschlüsseln, womit die gesamte Serverinfrastruktur nicht mehr verfügbar war. Durch diesen „Escape" ist es Ihnen auch möglich gewesen, in bestimmte andere Netzwerke, also das Produktivsystem, einzudringen.
Für uns als Behörde stellte sich die Frage, wie es zur ersten Infektion gekommen ist. Dies hat man aufgrund fehlender Protokollierung aus dem fraglichen Zeitraum nicht mehr aufklären können. Daraufhin wurden die Mitarbeitenden benachrichtigt und die Datenschutzbehörden der anderen EU-Länder informiert, in denen weitere Produktivsysteme laufen. Ein Bußgeld konnte aufgrund des in §42 Nr. 4 BDSG benanntem Verwertungsverbots nicht verhängt werden.
Aus diesem und ähnlichen Ransomware-Fällen kann für Unternehmen einiges gelernt werden. Sie sollten eine „Security in Depth" Strategie verfolgen. Eine Firewall alleine reicht seit langem nicht mehr aus. Bei der Wahl der Firewall sollte auch darauf geachtet werden, wie sich der Hersteller gegenüber Sicherheitsforschenden verhält und mit welcher Frequenz sie von Sicherheitslücken betroffen sind. Eine Netzwerktrennung innerhalb der eigenen Infrastruktur ist immer noch ein unerlässliches Mittel. Administrator:innen und Personen, die an der Entwicklung von Software beteiligt sind, müssen davon ausgehen, besonders lohnenswerte Ziele für Angriffe zu sein. Diese Personen müssen also mit besonders gut geschützten Accounts arbeiten.

Insgesamt wurden im Berichtsjahr 356 Fälle bearbeitet, die Folgen von Hacking-Attacken waren. Davon entfallen jeweils ca. 100 auf Phishing und Ransomeware-Angriffe, 75 auf die Kompromittierung bestehender Accounts, 9 auf das Ausnutzen von Schwachstellen in öffentlich zugänglichen Anwendungen, 5 Supply-Chain-Kompromittierungen und 2 Fälle von erfolgreichem Bruteforcing. In den übrigen Fällen lagen andere Ursachen zugrunde oder der initiale Angriffsvektor konnte nicht ermittelt werden. Hinzu kamen 45 gemeldete Datenschutzvorfälle, die durch Hard- und Softwarefehler verursacht wurden.

Wie in den Jahren zuvor, sehen wir einen Anstieg von Cyberkriminalität, die insbesondere Firmen mit schwacher technischer Ausstattung zum Ziel haben. Wir rechnen aufgrund der globalen Lage auch im Jahr 2026 mit einem erhöhten Aufkommen von Ransomware-Angriffen und Phishing. Der Fastlane-Prozess ist ein erster Schritt, um mit dem erhöhten Aufkommen besser umgehen zu können.

25. IT-Labor

Um die Einhaltung des Datenschutzes verlässlich und professionell prüfen zu können, baut der HmbBfDI eine virtuelle Serverinfrastruktur für technische Prüfungen auf.

Der HmbBfDI führt eine Vielzahl technischer Prüfungen durch. Um diese zukünftig noch effizienter und professioneller zu gestalten, wurde mit dem IT-Labor eine virtuelle Netzwerk- und Infrastruktur aufgebaut, die speziell auf die Anforderungen der Prüfprozesse zugeschnitten ist.

Das IT-Labor bietet eine neue Prüfplattform, mit der vernetzte virtuelle Maschinen und Container bereitgestellt und verwaltet werden können. In dieser Prüfumgebung ist die Durchführung vielfältiger technischer Prüfszenarien möglich. Dazu gehören unter anderem die Analyse von Webseiten hinsichtlich Datenschutz und IT-Sicherheit, die Überprüfung von Smartphone-Applikationen auf datenschutzkonforme Verarbeitung personenbezogener Daten sowie die Analyse von Werbe-E-Mails auf potenzielles Benutzer:innentracking. Für jedes dieser Szenarien stehen spezifische Prüfwerkzeuge und Testumgebungen bereit, sodass der initiale Aufwand für ein konkretes Prüfvorhaben deutlich reduziert wird.

Um den steigenden Anforderungen und neuen Prüfmethoden gerecht zu werden, ist die Infrastruktur modular aufgebaut und kann flexibel um zusätzliche Bausteine erweitert werden. Ein besonderer Vorteil der

Modularität liegt in der individuellen Konfigurierbarkeit der Prüfungsumgebungen, die sich kontinuierlich an neue technische Entwicklungen anpassen lassen. Für jede Prüfung werden gezielt die benötigten Ressourcen und Einstellungen bereitgestellt – sei es für die Analyse komplexer Fachverfahren, die Überprüfung von Schnittstellen oder die Bewertung neuer Softwarelösungen. So lassen sich unterschiedliche technische Anforderungen und Prüfziele optimal abbilden und gleichzeitig sinken die Hürden für den Einsatz von Werkzeugen mit hoher Komplexität und Ressourcenbedarf.

Ein zentrales Element der Infrastruktur ist der Auswerteserver, auf dem die Ergebnisse der technischen Prüfungen zusammengeführt und analysiert werden können. Dieser Server dient als zentrale Plattform für die Auswertung, Dokumentation und Nachverfolgung der Prüfergebnisse. Die Nachvollziehbarkeit und Wiederherstellbarkeit der Prüfumgebung stellen einen weiteren Vorteil der virtuellen Prüfumgebung dar, da die Umstände der Prüfung jederzeit vollständig rekonstruierbar sind.

Die gesamte Infrastruktur basiert wesentlich auf quelloffener Software wie Proxmox, Website Evidence Collector und PiRogue Toolsuite. Dies ist eine wichtige Voraussetzung dafür, das IT-Labor mit leistbarem Aufwand zu betreiben, die Prüfwerkzeuge an die spezifischen Anforderungen des HmbBfDI anpassen zu können und in diesem Bereich digital souverän zu agieren. Der HmbBfDI steht dazu teilweise mit den Softwarehersteller:innen im Austausch.

Die Infrastruktur ist so abgesichert, dass ausschließlich autorisierte Mitarbeitende des HmbBfDI Zugang zu den jeweiligen Prüfungsumgebungen erhalten. Durch eine klare Vergabe von Zugriffsrechten und die konsequente Trennung der einzelnen Prüfungsumgebungen ist sichergestellt, dass die Daten und Prüfergebnisse jederzeit geschützt bleiben.

26. Vereinheitlichung von Prüfstandards

Der HmbBfDI strebt gemeinsam mit dem Senat an, Prüfstandards für digitale Projekte zu vereinheitlichen. Damit sollen die in der DSGVO genannten Grundsätze wie Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz im Hinblick auf die fortschreitende Digitalisierung und unter Berücksichtigung föderaler Grundsätze weiterhin hinreichend sichergestellt werden durch die verantwortlichen Stellen und gleichzeitig Effizienz bei digitalen Anwendungen gewährleistet werden.

Die Senatskanzlei und der HmbBfDI erarbeiten gemeinsam einen Prüfstandard mit der Zielgruppe öffentlicher Stellen in Hamburg. Der Datenschutz wird dabei als Teil einer Lösung betrachtet und nicht als Hindernis bei der Umsetzung von Projekten, wie beispielweise der Nutzung durch neue KI-Modelle bis hin zu automatisierten Verarbeitungsvorgängen sowie einer Zentralisierung von Verwaltungsaufgaben. Ausgangspunkt ist dabei die Richtlinie zur Beteiligung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, die für bestimmte Fälle eine Beteiligung des HmbBfDI bei der Einführung neuer IT-Verfahren vorsieht. Die Richtlinie ist für den HmbBfDI ein wichtiger Baustein in der Einbindung in die Entwicklung der digitalen Infrastruktur der öffentlichen Verwaltung. Da die Richtlinie keine konkreten Vorgaben zum Verfahrensablauf, wie z. B. dem konkreten Zeitpunkt der Einbindung des HmbBfDI enthält, ist auch vor diesem Hintergrund eine Konkretisierung durch ergänzende Prüfstandards sinnvoll.

Ein Hamburgischer Prüfstandard soll das sog. „Einer für alle"-Prinzip mitdenken, nach dem nach Vorstellung des HmbBfDI nicht nur auf der Verwaltungsebene, sondern auch auf der Seite der Aufsichtsbehörden Mehrfachprüfungen gleichartiger Digitalisierungsprojekte nicht nur im OZG-Kontext vermieden werden könnten. Die zu erarbeitenden Prüfstandards sollen die Basis für die Akzeptanz einer in Hamburg zu

bundeslandübergreifenden zur Verfügung gestellten Verfahren geben, damit diese Verfahren in anderen Bundesländer nicht erneut geprüft werden müssen. Dieser Gedanke stellt aus Sicht des HmbBfDI einen wichtigen Baustein dar für eine souveräne datenschutzkonforme Digitalisierung im Rahmen einer demokratisch legitimierten und zudem getragenen Entscheidung durch die Exekutive und die unabhängigen Aufsichtsbehörden. Bei dieser Aufgabe widmet sich der HmbBfDI insbesondere der Frage, was die Hamburger Verwaltung braucht, um den Datenschutz von Anfang an mitzudenken. Öffentliche Stellen verfügen bereits über viele Erfahrungen mit der Einführung von digitalen Projekten. Von diesen Erfahrungen ausgehend ist es entscheidend, die Projektmanager:innen selbst in den Prozess der Erstellung eines Prüfstandards miteinzubeziehen. Die Projektphasen orientieren sich demzufolge an dem Handbuch der FHH zum Projektmanagement, einsehbar unter dem Link: https://epub.sub.uni-hamburg.de/epub/voll-texte/2021/122930/.

Einzelne Projektphasen sind:
- Phase 1: Projektinitiierung (Vorprojektphase)
- Phase 2: Projektplanung
- Phase 3: Projektdurchführung und Controlling
- Phase 4: Projektabschluss
- Phase 5: Sonderfall – Vorabkonsultation (Art. 36 DSGVO).

Diesen Phasen werden datenschutzrechtliche Mindestanforderungen im Einzelnen zugeordnet. Der Prüfstandard umfasst eine formelle und materielle datenschutzrechtliche Prüfung. Der HmbBfDI sieht in dieser Zusammenführung der Prüfungsabfolge durch die frühzeitige Einbindung der Aufsichtsbehörde und der Stakeholder einen Mehrwert für alle an dem Digitalisierungsprojekt Beteiligten und einen sachgerechten Ansatz zur Konkretisierung der Beteiligungsrichtlinie Der Abstimmungsprozess ist bereits weit fortgeschritten und es wird ein abschließendes Ergebnis für das laufende Jahr 2026 angestrebt.

27. „Einer prüft für alle“ in der Arbeit der Datenschutzaufsichtsbehörden

Der „Einer für Alle“ (efa) Gedanke aus dem OZG kann entscheidende Impulse für die Gestaltung der Arbeit der Aufsichtsbehörden miteinander geben und bundesweit Rechtssicherheit stärken.

Das Jahr 2025 stand für die Datenschutzaufsichtsbehörden im Zeichen der Stärkung der Zusammenarbeit innerhalb der Datenschutzkonferenz. Man suchte nach Lösungsmöglichkeiten, auch um nicht unerschöpflich erweiterbare Kapazitäten vor dem Hintergrund steigender Beschwerdezahlen zu schonen. Die Übertragung des efa-Prinzips auf die Arbeit der Aufsichtsbehörden kann dafür ein guter Lösungsansatz sein.

Das efa-Prinzip steht im OZG-Kontext dafür, dass eine Stelle einen Onlinedienst konstruiert und anbietet, den andere Stellen dann unkompliziert übernehmen und nachnutzen können. Übertragen auf die Arbeit der Datenschutzaufsichtsbehörden kann das bedeuten, dass bei bundeslandübergreifenden Verfahren die Aufsichtsbehörde des Bundeslandes, in dem ein digitaler Dienst angeboten wird, die datenschutzrechtliche Prüfung vornimmt und das Prüfergebnis von den Aufsichtsbehörden der Bundesländer, in denen der jeweilige Dienst oder das Verfahren nachgenutzt wird, übernommen werden kann. Es prüft dann einer für alle.

Die Umsetzung dieser Lösung kann dabei auf verschiedene Weise vorgenommen werden: zum einen im Rahmen der Neuregelung der Zuständigkeiten im BDSG, zum anderen in der Abstimmung einheitlicher Prüfstandards, um verantwortlichen Stellen zur Förderung der Rechtssicherheit einheitliche Vorgaben machen zu können. Die Abstimmung einheitlicher Prüfstandards ermöglicht dann ggf. in einem zweiten Schritt durch eine mittelbare Selbstbindung, Prüfungsergebnisse aus anderen Bundesländern anzuerkennen. Entscheidend für diesen Me-

chanismus ist gerade die Abstimmung vereinheitlichter Prüfkriterien, um die Akzeptanz der Entscheidungen einzelner Aufsichtsbehörden gegenüber anderen Aufsichtsbehörden fördern zu können. Mit einer ähnlichen Wirkungsrichtung ist der HmbBfDI auch auf Hamburger Ebene in den Dialog mit der SK zu einem Verwaltungsstandard in datenschutzrechtlicher Hinsicht eingetreten, vgl. dazu vorstehend den Bericht in Kap. III 29.

In diese Richtung hat die DSK im Bereich der OZG-Onlinedienste durch die Verabschiedung eines Standardisierten Prüfprozesses zu datenschutzrechtlichen Anforderungen bei Efa-Onlinediensten nach dem Onlinezugangsgesetzes (OZG) einen wichtigen ersten Schritt getan. Der Prüfprozess ist unter https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Standardisierter_Pruefprozess_OZG.pdf abrufbar.

Der standardisierte Prüfprozess der DSK bietet eine strukturierte Handlungsanleitung zur datenschutzrechtlichen Begleitung länderübergreifender efA-Onlinedienste gemäß Onlinezugangsgesetz (OZG). Er richtet sich vor allem an betreibende Behörden, die für die Einhaltung der DSGVO und weiterer Spezialnormen verantwortlich sind, sowie an weitere beteiligte Stellen.

Der Prozess gliedert sich in fünf Phasen: Initialisierung (Klärung von Verantwortlichkeiten und Beteiligten), Definition (Erfassung der verarbeiteten Daten, Rechtsgrundlagen und Betroffenenrechte), Planung und Durchführung (Umsetzung von Datenschutz durch Technikgestaltung, Risikobewertung und ggf. Datenschutz-Folgenabschätzung) sowie Abschluss (Etablierung eines Datenschutzmanagements).

Besonderes Augenmerk liegt auf der frühzeitigen Risiko-Vorprüfung und der strukturierten DSFA, die von der Modellierung der Verarbeitung bis zur Wirksamkeitsprüfung der Maßnahmen reicht. Ergänzend enthält der Prüfprozess eine Standardstruktur für Datenschutzkonzepte mit integrierter DSFA sowie umfangreiche Hilfestellungen wie Projektmanagementhandbücher und „Muss-Listen“ für risikoreiche Verarbeitungsvorgänge. Insgesamt gewährleistet der

Prüfprozess eine systematische und nachvollziehbare Umsetzung der datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten im Rahmen des OZG.

Dieser Prüfstandard kann nun als Grundlage dazu dienen, Prüfstandards auch für andere Bereiche zu entwickeln und abzustimmen, beispielweise für bundeslandübergreifend zur Verfügung gestellte digitale Fachverfahren, die nicht unter das OZG fallen oder Dienste aus der Deutschen Verwaltungs-Cloud. Nicht zuletzt steht dieser Standard auch Pate für die weitere Ausarbeitung von Prüfstandards in Hamburg, zu denen vorstehend in Kap. III 26 berichtet wird.

28. Zugang zu Forschungsdaten nach Digital Services Act

Seit dem 29. Oktober 2025 erhalten Forschende im Rahmen des Digital Services Act (DSA) Zugang zu nicht-öffentlichen Plattformdaten, um systemische Risiken zu untersuchen. Hamburg wurde von der Datenschutzkonferenz (DSK) beauftragt, federführend eine Schnittstelle zum Digital Services Coordinator bei der Bundesnetzagentur einzurichten und Prüfprozesse zu etablieren, die im föderalen System die schnelle und fachkundige Bewertung von Anträgen ermöglichen.

Die Datenschutzkonferenz hat gemeinsam mit der Bundesnetzagentur als Digital Services Coordinator einen Prozess entwickelt, der sicherstellt, dass Anträge auf Zugang zu Forschungsdaten geordnet und effizient von zuständigen Datenschutzaufsichtsbehörden bearbeitet werden. Der HmbBfDI übernimmt dabei eine zentrale Rolle und betreibt eine Clearingstelle, die als Schnittstelle zwischen den Datenschutzaufsichtsbehörden und der Bundesnetzagentur fungiert. Diese Clearingstelle nimmt die Anträge entgegen und leitet sie an die jeweils zuständigen Datenschutzbehörden weiter, die für die fachliche Prüfung und Entscheidung verantwortlich sind. Parallel dazu gibt es eine Schnittstellen-Dialoggruppe, in der strategische Themen rund um

den Digital Services Act und den Datenschutz diskutiert werden. Der HmbBfDI ist in dieser Gruppe zusammen mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie dem jeweiligen Vorsitz der DSK – in 2025 der Berliner Beauftragen für Datenschutz und Informationsfreiheit – dauerhaft vertreten und übernimmt eine federführende Rolle im föderalen Austausch.

Um die Prüfungen nach Art. 40 DSA zu unterstützen, wurde eine Checkliste für Forschende veröffentlicht, die die wichtigsten Anforderungen und Prüfkriterien für den Zugang zu Forschungsdaten zusammenfasst. Diese Checkliste hilft u.a. dabei zu beurteilen, ob die beantragten personenbezogenen Daten für die wissenschaftliche Fragestellung notwendig sind, ob die Anforderungen an die Datenminimierung eingehalten werden und ob personenbezogene Daten angemessen anonymisiert oder pseudonymisiert sind. Außerdem werden Anforderungen an die technische und organisatorische Umsetzung des Datenschutzes gestellt, etwa zur sicheren Übermittlung und Speicherung der Daten. Ziel ist es, den Prüfprozess transparent und nachvollziehbar zu gestalten, den Schutz der Nutzendendaten sicherzustellen und gleichzeitig die Forschung weitgehend zu ermöglichen.

Seit dem Start der Regelungen sind die ersten Anträge auf Zugang zu nicht-öffentlichen Plattformdaten eingegangen und an die jeweils zuständigen Datenschutzaufsichtsbehörden weitergereicht worden. Für das Jahr 2026 wird erwartet, dass die Anzahl der Anträge steigt und die Clearingstelle ihre Rolle als zentrale Koordinationsstelle weiter ausbaut.

Unter dem neuen Vorsitz der Datenschutzkonferenz im Jahr 2026 setzt die Schnittstellen-Dialoggruppe ihre Arbeit fort und behandelt weiterhin wichtige Themen zu Fragen der Plattformregulierung. Die Etablierung dieses effizienten Prüfprozesses im föderalen System ist ein Beitrag zur Förderung der Transparenz großer Online-Plattformen und zur Sicherstellung des Datenschutzes im digitalen Raum.

29. Data Act

Der europäische Data Act ist seit September 2025 von Unternehmen anzuwenden, die vernetzte Geräte herstellen oder damit handeln. Soweit mit ihnen personenbezogene Daten generiert werden, obliegt den Datenschutzbehörden die Aufsicht über die Einhaltung des neuen Rechtsakts. Der HmbBfDI hat umfassend für das Thema sensibilisiert und nimmt sich Beschwerden und Beratungsanfragen nach dem Data Act an.

Das Ziel des Data Act besteht darin, bisherige Datenmonopole bei vernetzten Geräten zu überwinden. Er soll dafür sorgen, dass auch andere Marktteilnehmende Zugang zu den bei der Nutzung entstehenden Daten erhalten und davon profitieren können. Unternehmen und Privatpersonen, die vernetzte Geräte nutzen, sollen künftig ebenfalls Zugriff auf die darin erzeugten Daten bekommen. Im Mittelpunkt steht dabei das sogenannte Internet der Dinge („Internet of Things"), zu dem unter anderem vernetzte Maschinen, Fahrzeuge, Haushaltsgeräte, Fernseher sowie Medizin- und Fitnessgeräte zählen. Bisher ist es häufig so, dass diese Produkte fortlaufend Nutzungsdaten und beispielsweise Informationen zum Verschleiß einzelner Komponenten an die Hersteller übermitteln. Fahrzeughersteller erhalten auf diesem Weg wertvolle Rückmeldungen zur Nutzung ihrer Fahrzeuge, von denen auch Werkstätten oder Ersatzteilhersteller profitieren könnten – bislang jedoch meist ohne freien Zugang zu diesen Daten. Gleiches gilt für die Nutzenden selbst. Der Data Act soll sowohl Privatpersonen als auch Geschäftskunden, die ein internetfähiges Produkt erworben haben, ermöglichen, selbst zu entscheiden, wem sie die bei der Nutzung anfallenden Daten zugänglich machen. Diese neuen Möglichkeiten erlauben es den Nutzenden zunächst, ihr eigenes Nutzungsverhalten zu analysieren und ggf. zu verbessern. Über Lizenzvereinbarungen können sie zudem beispielsweise Werkstätten oder Ersatzteilherstellern die Auswertung der Gerätedaten gestatten. Der Data Act regelt dabei auch die faire Ausgestaltung solcher Verträge.

Das Herzstück des Data Act ist der Datenzugang. In den Anwendungsbereich des Rechtsakts fallende Gerätedaten hat der Hersteller auf Antrag Dritten bereitzustellen. Dabei gibt es zwei wesentliche Ausschlussgründe, wegen derer der Zugang verweigert werden kann: Der Anspruch besteht nicht, wenn die Herausgabe entweder Geschäftsgeheimnisse oder den Datenschutz verletzen würde. Art. 5 Abs. 1 DA legt dabei fest, dass die DSGVO unberührt von den Bestimmungen des Data Act vorrangig gilt. Beide Rechtsakte sind europäische Verordnungen auf gleicher Ebene, aber sie sind mit einer Kollisionsregel zu Gunsten des Datenschutzes versehen. In der Praxis bedeutet dies, dass kein Datenzugang gewährt werden darf, der als unzulässige Übermittlung personenbezogener Daten nach der DSGVO einzustufen wäre. Der Zugang zu personenbezogenen Daten bedarf einer Rechtsgrundlage nach Art. 6 DSGVO, der Data Act selbst enthält solche Rechtsgrundlagen nicht. Daher bestehen in der Praxis Zugangsansprüche vor allem unter der Voraussetzung, dass eine datenschutzrechtliche Einwilligung der Betroffenen oder eine vertragliche Vereinbarung vorliegt; ggf. kann die Offenlegung auch aufgrund eines überwiegenden berechtigten Interesses nach Art. 6 Abs. 1 lit. f DSGVO zulässig sein.

Zu den Rechten und Pflichten aus dem Data Act, dem Zusammenspiel mit dem Datenschutzrecht und der aufsichtsbehördlichen Durchsetzung hat der HmbBfDI im April 2025 eine ausführliche Handreichung veröffentlicht. Sie trägt den Titel „Der Data Act als Herausforderung für den Datenschutz“.

Dreht sich eine Fallgestaltung um personenbezogene Daten, ist die jeweils zuständige Datenschutzbehörde gemäß Art. 37 Abs. 3 DA auch die Aufsichtsbehörde zur Durchsetzung des Data Act. Die Rechte auf Datenzugang, auf transparente Information sowie auf Wechsel des Cloud-Anbieters kann der HmbBfDI ggf. mit Anordnungen durchsetzen. Dem HmbBfDI stehen gemäß Art. 37 Abs. 3 Satz 2 DA alle Mittel aus Kapitel VI und VII der DSGVO zur Verfügung, um Fällen nach dem Data Act nachzugehen. Auch Bußgelder kann er für Verstöße gegen den Data Act verhängen.

Jede natürliche und juristische Person kann nun Beschwerde beim HmbBfDI einlegen, wenn sie Grund zur Annahme hat, dass ein Hamburger Unternehmen ihre Rechte aus dem Data Act in Bezug auf personenbezogene Daten verletzt. Die Beschwerden können formlos an das Funktionspostfach dataact@datenschutz.hamburg.de gerichtet werden. Alternativ können die Postanschrift der Behörde oder das allgemeine Beschwerdeformular verwendet werden. Jeder Beschwerde wird federführend in dem Referat nachgegangen, das auch die datenschutzrechtliche Aufsicht über die jeweilige verantwortliche Stelle hat. Damit wird der Zielrichtung des Art. 37 Abs. 3 Data Act gefolgt, Datenverwendungen nach der Datenschutz-Grundverordnung und nach dem Data Act einheitlich zu beurteilen. Das Fachreferat führt seine Ermittlungen in enger Abstimmung mit dem Fachbereich für Informationsfreiheit, um die Expertise zu Geschäftsgeheimnissen als Hinderungsgrund für einen Informationszugang einzubeziehen. Im Berichtszeitraum sind auf diesem Wege vor allem Beratungsanfragen eingegangen, die der HmbBfDI beantwortet hat.

Die Zuständigkeit des HmbBfDI als Data-Act-Aufsicht ist auf Fälle mit personenbezogenen Daten beschränkt. Für alle übrigen Konstellationen muss der Bundesgesetzgeber eine oder mehrere Aufsichtsbehörden für Deutschland benennen. Ein Gesetzesentwurf der Bundesregierung sieht die Bundesnetzagentur für diese Aufgabe vor. Darüber hinaus ist nach dem Entwurf beabsichtigt, die Bundesnetzagentur auch für Fallgestaltungen in Bezug auf den Schutz personenbezogener Daten bei nichtöffentlichen Stellen einzusetzen. In der Konstellation soll die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit der Bundesnetzagentur inhaltliche Einschätzungen zuliefern. Die in Art. 37 Abs. 3 Data Act vorgesehene und derzeit gelebte Zuständigkeit der jeweiligen Landesdatenschutzbehörde wird durch den Entwurf negiert. Seitens des Bundesrats bestehen Bedenken, inwieweit es sinnvoll und zulässig ist, eine Doppelaufsicht für die Datenhaltung in Unternehmen zu schaffen. Neben der Bundesnetzagentur und der Bundesdatenschutzbeauftragten auf der einen Seite bleiben schließlich weiterhin die Landesdatenschutzbeauftragten für alle übrigen Verarbeitungen personenbezogener Daten zuständig.

Dauerhaft zuständig bleiben die Landesdatenschutzbehörden auch nach dem Gesetzesentwurf für die Aufsicht über öffentliche Stellen in Bezug auf personenbezogene Daten. Relevant ist dies vor allem für zwei Fallgruppen. Zum einen bleibt der HmbBfDI die Aufsichtsbehörde nach dem Data Act für öffentliche Stellen, die als Hersteller oder Verbreiter vernetzter Produkte auftreten. Denkbar ist dies beispielsweise in der Gesundheitsforschung des UKE. Zum anderen fallen Notfallzugriffe von Behörden nach Art. 14 DA in seine Aufsicht.

Falls der Gesetzesentwurf in der Form verabschiedet wird, gibt der HmbBfDI alle offenen Verfahren nach dem Data Act in Bezug auf nichtöffentliche Stellen ab dem Zeitpunkt des Geltungsbeginns des Durchführungsgesetzes an die Bundesnetzagentur ab. Soweit Fragestellungen des reinen Datenschutzrechts enthalten sind, bleibt der entsprechende Teil des Falles beim HmbBfDI. Vorstellbar ist eine solche Trennung beispielsweise, wenn Bürger:innen die Herausgabe von Informationen verlangen und dabei offenlassen, ob es sich um einen Auskunftsantrag nach Art. 15 DSGVO oder einen Zugangsantrag nach dem Data Act handelt.

Gemäß Art. 37 Abs. 3 Satz 2 DA i.V.m. Art. 59 DSGVO hat der HmbBfDI einen Tätigkeitsbericht über die Erfüllung seiner Aufgaben nach dem Data Act zu erstellen. Der vorliegende Tätigkeitsbericht Datenschutz beinhaltet mit den vorstehenden Ausführungen zugleich den Tätigkeitsbericht nach dem Data Act.

30. Intelligenter Föderalismus statt Zentralisierung: Reform der Datenschutzaufsicht in der bundespolitischen Debatte

Nach der Bundestagswahl hat eine bundespolitische Diskussion um eine Reform der Datenschutzaufsicht begonnen. Der HmbBfDI setzt sich für einen intelligenten Föderalismus ein und sieht darin den besseren Ansatz zur Unterstützung der digitalen Transformation in Deutschland als in einer Zentralisierung.

Bereits im Vorwort zum letzten Tätigkeitsbericht wurde auf die zunehmende Zentralisierung von Aufsichtsstrukturen bei der Umsetzung der europäischen Digitalrechtsakte hingewiesen. Konkret diskutiert wird nun die Frage, ob und wie die Datenschutzaufsicht in Deutschland effizienter und einheitlicher gestaltet werden kann. Der HmbBfDI hat sich frühzeitig in diese Debatte eingebracht und einen eigenen Drei-Punkte-Plan vorgestellt, der auf eine intelligente Vernetzung der bestehenden föderalen Strukturen abzielt. Konkret schlug der HmbBfDI vor,

- bei länderübergreifenden Sachverhalten die zentrale Zuständigkeit einer Aufsichtsbehörde bei länderübergreifenden Forschungsprojekten und Unternehmensgruppen zu schaffen (one-stop-shop),
- das Einer-prüft-für-Alle-Prinzip (EfA) gesetzlich zu verankern, wodurch Prüfungen eines IT-Systems durch eine Landesdatenschutzbehörde für andere Behörden grundsätzlich verbindlich sind
- und die Datenschutzkonferenz als gemeinsames Entscheidungsgremium mit verbindlichen Mehrheitsentscheidungen zu institutionalisieren.

Im Frühjahr 2025 waren die Koalitionsverhandlungen auf Bundesebene von Vorschlägen zur Bündelung von Kompetenzen bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)

geprägt. Diese Vorschläge stützen sich auf die Initiative „Handlungsfähiger Staat“, die eine stärkere Zentralisierung und Vereinheitlichung der Datenschutzaufsicht vorgeschlagen hatte. Als Reaktion hierauf haben die Datenschutzaufsichtsbehörden der Länder den Drei-Punkte-Plan aufgegriffen, weiterentwickelt und sich zu eigen gemacht.

Die politische Debatte hat sich im Berichtsjahr weiter zugespitzt. Bund und Länder haben sich mit einem Staatsmodernisierungs-Beschluss vom 4. Dezember 2025 auf eine abgestimmte Reform der Datenschutzaufsicht bis Ende 2027 geeinigt. Der Beschluss listet ergebnisoffen zahlreiche Maßnahmen auf – darunter auch viele Vorschläge der Datenschutzaufsichtsbehörden der Länder: „Hierzu können insbesondere die Bündelung von Kompetenzen bei der BfDI oder Aufsichtsbehörden der Länder (beispielsweise durch Zuständigkeitskonzentration und/oder One-Stop-Shop-Regelungen), eine bessere Einbindung der DSK und/oder die Einführung eines Kohärenzverfahrens unter Nutzung der Möglichkeiten des Art. 87 Abs. 3 Grundgesetz auf Bundesebene oder im Wege von Staatsverträgen zwischen den Ländern gehören.“

Der HmbBfDI hält den Ansatz des intelligenten Föderalismus weiterhin für den schneller und einfacher umsetzbaren Weg, um den Datenschutz in Deutschland zu stärken und die digitale Transformation zu unterstützen. Die vorgeschlagenen Maßnahmen können aus Sicht des HmbBfDI effektiv Bürokratie reduzieren, Rechtssicherheit schaffen und die Interessen von Bürger:innen und Unternehmen gleichermaßen berücksichtigen.

KI UND DATENSCHUTZ IV.

KI und Datenschutz

1. EDSA-Stellungnahme zu KI-Modellen

Die Stellungnahme 28 / 2024 des Europäischen Datenschutzausschusses (EDSA) hat europaweit Leitplanken für den datenschutzgerechten Umgang mit KI-Modellen gesetzt. Der HmbBfDI wendet die Vorgaben des EDSA nun praxisgerecht an.

Die datenschutzrechtliche Bewertung von Künstlicher Intelligenz (KI) und insbesondere von großen Sprachmodellen (Large Language Models, LLMs) ist seit der Einführung generativer KI-Systeme ein zentrales Thema für die Datenschutzaufsicht. Ausgangspunkt der Debatte war u.a. die Unsicherheit, ob und in welchem Umfang KI-Modelle selbst personenbezogene Daten enthalten und damit der DSGVO unterfallen. Der HmbBfDI hat sich frühzeitig mit dieser Frage auseinandergesetzt und im Sommer 2024 mit den sogenannten „Hamburger Thesen" einen Impuls für die fachliche Diskussion gesetzt. Diese Thesen betonten die Unterscheidung zwischen dem KI-Modell als technischem „Motor" und dem umfassenderen KI-System als „Fahrzeug", das diesen Motor nutzt und mit der Außenwelt interagiert. Die datenschutzrechtlichen Überlegungen zur Risikobegrenzung hatten sich dabei vor allem auf die Systemebene konzentriert: Denn Risiken für Betroffene entstehen primär durch die Verarbeitung im KI-System, nicht durch die bloße Existenz eines KI-Modells.

Mit der Stellungnahme 28 / 2024 des Europäischen Datenschutzausschusses vom 17. Dezember 2024 liegt nun erstmals eine europäische Positionierung zur KI-bezogenen Verarbeitung personenbezogener Daten vor. Die Stellungnahme entstand auf Initiative der irischen Datenschutzaufsichtsbehörde in Fortführung der durch die Hamburger Thesen begonnenen Debatte. Sie wurde in intensiven Abstimmungsrunden unter Beteiligung deutscher Behörden, darunter auch dem HmbBfDI, erarbeitet und ersetzt damit den Impuls der Hamburger Thesen.

Das Papier des EDSA adressiert zentrale Fragen: Unter welchen Umständen sind KI-Modelle als anonym zu bewerten? Wie kann das berechtigte Interesse an der Entwicklung und Nutzung von KI-Modellen datenschutzrechtlich begründet werden? Und wie wirken sich datenschutzrechtliche Mängel beim Training eines KI-Modells auf dessen spätere Nutzung aus?

Der EDSA unterscheidet hinsichtlich letzterer Frage drei Szenarien, die für die Bewertung des Einsatzes von KI-Modellen relevant sind:

1. Ein Verantwortlicher trainiert ein KI-Modell unter Verstoß gegen datenschutzrechtliche Vorgaben und nutzt dieses Modell anschließend selbst.
2. Ein Verantwortlicher nutzt ein KI-Modell, das von einem Dritten unter Verstoß gegen datenschutzrechtliche Vorgaben trainiert wurde.
3. Ein Verantwortlicher trainiert ein KI-Modell rechtswidrig, anonymisiert dieses jedoch im Anschluss und setzt es dann ein.

In den ersten beiden Szenarien fordert der EDSA eine Interessenabwägung, bei der insbesondere die vom Verantwortlichen ergriffenen risikomindernden (mitigierenden) Maßnahmen zu berücksichtigen sind. Im dritten Szenario – der Anonymisierung des Modells – findet die DSGVO nach Auffassung des EDSA keine Anwendung, sofern die Anonymität des Modells auch während des Einsatzes fortbesteht. Die Anonymitätsbehauptung muss also nicht nur für den Zeitpunkt der Modellentwicklung, sondern auch für die gesamte Einsatzphase aufrechterhalten werden.

Unabhängig von der konkreten Konstellation läuft die datenschutzrechtliche Bewertung letztlich auf einen ähnlichen Maßstab hinaus: Für alle KI-Modelle, die mit personenbezogenen Daten trainiert wurden, sind angemessene technische und organisatorische Maßnahmen zu ergreifen, um das Risiko einer rechtswidrigen Extraktion personenbezogener Daten aus dem KI-System zu begrenzen. Die Anforderungen an diese risikomindernden Maßnahmen sind in allen drei Szenarien

ähnlich, da die Gefahr einer unzulässigen Datenextraktion im Betrieb des KI-Systems besteht – unabhängig davon, ob das Modell selbst oder ein Dritter das Training durchgeführt hat oder ob eine Anonymisierung behauptet wird.

Bemerkenswert ist die Forderung des EDSA, dass Verantwortliche nachweisen müssen, sich mit der Rechtmäßigkeit des eingesetzten KI-Modells auseinandergesetzt zu haben. Im Bereich großer Sprachmodelle ist dieser Nachweis praktisch kaum zu erbringen, da die Trainingsdaten in der Regel aus frei verfügbaren Internetquellen stammen und eine vollständige Kontrolle oder Dokumentation nicht möglich ist. Dennoch verlangt der EDSA, dass Verantwortliche die Herkunft und die rechtlichen Rahmenbedingungen des Modells prüfen und dokumentieren – insbesondere, ob eine behördliche oder gerichtliche Feststellung zur Rechtswidrigkeit des Trainings vorliegt.

Die EDSA-Stellungnahme 28 / 2024 bietet einen Rahmen für die datenschutzrechtliche Bewertung von KI-Modellen und hebt die Bedeutung systemseitiger Schutzmaßnahmen hervor. Für die Aufsichtspraxis des HmbBfDI bedeutet dies, dass sich die Kontrolle auf die im KI-System implementierten Mechanismen zur Risikobegrenzung konzentriert. Die Herausforderung bleibt, die technische Komplexität und die mangelnde Transparenz bei der Entwicklung großer Sprachmodelle angemessen zu berücksichtigen. Der HmbBfDI wird die weitere Entwicklung aufmerksam begleiten und die eigenen Prüfmaßstäbe fortlaufend anpassen, um sowohl die Rechte der Bürgerinnen und Bürger zu schützen als auch die verantwortungsvolle Nutzung innovativer Technologien zu ermöglichen.

2. LLMoin

Die Prüfung des KI-Systems LLMoin durch den HmbBfDI wurde im Oktober 2025 abgeschlossen. Die Ergebnisse sind im Sinne des „Einer prüft für Alle" (EfA-Prinzip) auch für die Datenschutzaufsichtsbehörden anderer Bundesländer verfügbar, die LLMoin einsetzen möchten.

Die datenschutzrechtliche Prüfung von LLMoin durch den HmbBfDI begann im Jahr 2023 mit der Begleitung eines Pilotprojekts, bei dem die Verarbeitung von personenbezogenen Daten zunächst ausgeschlossen war. Ziel war es, die Einsatzmöglichkeiten von KI-gestützten Sprachmodellen in der öffentlichen Verwaltung zu erproben, ohne dabei datenschutzrechtliche Risiken einzugehen. Nach einer ersten Evaluationsphase wurde das System weiterentwickelt und ab 2024 für die Verarbeitung von personenbezogenen Daten mit normalem Schutzbedarf geöffnet. Die Prüfung des HmbBfDI begleitete diese Entwicklung eng und passte die Anforderungen an die jeweils neuen Nutzungsszenarien an.

Im Mittelpunkt der Prüfung standen die technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes. Dazu zählen insbesondere die Implementierung von Filtern zur Stärkung der Betroffenenrechte, die Ausgestaltung eines datenschutzfreundlichen Systemprompts sowie die Beschränkung der zentralen Protokollierung durch die Senatskanzlei. Die Handlungsanweisungen, welche u.a. die Verarbeitung sensibler Daten wie solche nach Art. 9 und 10 DSGVO sowie von Daten Minderjähriger ausschließen, wurden mehrfach überarbeitet. Die Verarbeitung bleibt auf Daten mit normalem Schutzbedarf beschränkt, was durch die verbindlichen Handlungsanweisungen und Schulungen sichergestellt wird.

Ein weiterer wichtiger Aspekt der Prüfung war die Berücksichtigung der aktuellen Entwicklungen im Europäischen Datenschutzausschuss

(EDSA). Dessen Stellungnahme 28 / 2024, welche in Kap. IV 1 besprochen wird, wurde dabei als Maßstab herangezogen, insbesondere hinsichtlich der Frage, wie sich ein möglicherweise rechtswidriges Training von KI-Modellen auf deren spätere Nutzung auswirkt. Der HmbBfDI prüfte, ob die eingesetzten technischen und organisatorischen Maßnahmen – wie Filter und Systemprompts – geeignet sind, das Risiko einer unzulässigen Extraktion personenbezogener Daten aus dem Sprachmodell angemessen zu begrenzen. Die Prüfung ergab, dass die getroffenen Maßnahmen im Kontext der internen Nutzung und des daraus folgenden begrenzten Nutzer:innenkreises als ausreichend bewertet werden können.

Die Sicherstellung der Betroffenenrechte wurde durch die Einführung eines Intent-Routings und einer Denylist umgesetzt, die es ermöglichen, Widersprüche nach Art. 21 DSGVO sowie Berichtigungs- und Löschungsrechte auf Systemebene umzusetzen. Die zeitlich begrenzte Speicherung von Prompts und Ausgaben durch die Senatskanzlei erfolgt aufgrund nachdrücklicher Empfehlung des HmbBfDI nunmehr ausschließlich im Falle technischer Fehler oder bei konkreter Einwilligung.

Im Ergebnis kommt der HmbBfDI zu dem Schluss, dass LLMoin ein datenschutzfreundlich konzipiertes KI-System ist, dessen Risiken durch eine Kombination aus technischen und organisatorischen Maßnahmen ausreichend gemindert werden. Die vom HmbBfDI vorgebrachte Kritik hinsichtlich des aktuellen Systemprompts und der Erfüllung von Informationspflichten gegenüber Bürger:innen wird nach Kenntnis des HmbBfDI bereits durch Maßnahmen der Senatskanzlei adressiert. Insgesamt bestehen daher keine durchgreifenden Bedenken gegen den produktiven Einsatz von LLMoin in der öffentlichen Verwaltung.

Die Prüfung von LLMoin erfolgte auch mit Blick auf das „Einer prüft für Alle"-Prinzip, das vorsieht, dass die Ergebnisse und Bewertungen des HmbBfDI auch anderen Bundesländern zur Verfügung gestellt werden, die LLMoin ebenfalls nutzen möchten, wodurch dort keine erneute grundlegende Prüfung durch die Datenschutzaufsichtsbe-

hörden erforderlich ist. Damit leistet der HmbBfDI auch einen Beitrag zur Harmonisierung und Standardisierung der datenschutzrechtlichen Bewertung von KI-Systemen in der öffentlichen Verwaltung über die Landesgrenzen hinaus.

3. Einführung LLMoin beim HmbBfDI

Im November 2025 begann der HmbBfDI mit der stufenweisen Einführung des KI-Systems LLMoin in der eigenen Dienststelle. Die Entscheidung zur Nutzung von Künstlicher Intelligenz (KI) wurde auch durch einen drastischen Anstieg der Eingabezahlen im Jahr 2025 ausgelöst, dem nur begrenzt mit personeller Aufstockung begegnet werden konnte. Die ersten Erfahrungen mit LLMoin sind überwiegend positiv und zeigen, dass KI einen wertvollen Beitrag zur Bewältigung des Arbeitsaufkommens leisten kann, ohne dabei datenschutzrechtliche Grundsätze zu kompromittieren.

Im Zeitraum von 2023 bis 2025 hat der HmbBfDI das KI-System LLMoin einer umfassenden datenschutzrechtlichen Prüfung unterzogen. Die Ergebnisse dieser Prüfung werden in Kap. IV 2 dargestellt und bilden die Grundlage für die Entscheidung, LLMoin auch in der eigenen Dienststelle einzusetzen. Unmittelbar nach Abschluss der Prüfung im Oktober 2025 wurde die Einführung von LLMoin als unterstützendes Werkzeug für die tägliche Arbeit des HmbBfDI angegangen.

Die Einführung von LLMoin erfolgt in zwei Phasen. In der ersten Erprobungsphase, die im November 2025 begann, ist die Nutzung und Abfrage von personenbezogenen Daten im Prompt noch ausdrücklich untersagt. Grundlage hierfür sind die lokalen Handlungsanweisungen des HmbBfDI, die ergänzend zu den globalen Vorgaben der Senatskanzlei gelten. Beispiele für Nutzungsszenarien in dieser Phase sind etwa die Unterstützung beim Verfassen oder bei der Zusammenfassung von Fachtexten oder die Formulierung von Stellungnahmen so-

wie Übersetzungen. Auch ohne die Verarbeitung personenbezogener Daten zeigt sich, dass LLMoin die Effizienz und in Teilen auch Qualität der Text- und Informationsverarbeitung steigern kann.

Die Resonanz innerhalb der Dienststelle auf die Einführung von LLMoin ist überwiegend positiv. Die Beschäftigten schätzen insbesondere die Möglichkeit, auf ein datenschutzkonform betriebenes KI-System zurückgreifen zu können, das die Nutzung dienstlicher Dokumente ermöglicht und gleichzeitig die Entstehung von sogenannter Schatten-KI – also nicht autorisierten oder privat genutzten KI-Anwendungen – verhindert. Die ersten Ergebnisse der Erprobungsphase bestätigen, dass LLMoin einen echten Mehrwert für die tägliche Arbeit bietet und die Bearbeitung von Routineaufgaben deutlich erleichtert. Die freiwillige Nutzung des Systems und die Möglichkeit, sich durch interne Schulungen und E-Learning-Module weiterzubilden, tragen zur hohen Akzeptanz bei.

Mit Blick auf die zweite Umsetzungsphase ist vorgesehen, die Nutzung von LLMoin auch für die Verarbeitung von personenbezogenen Daten zu öffnen. Dies würde insbesondere die Bearbeitung von Beschwerden erleichtern, in denen personenbezogene Informationen verarbeitet werden müssen. Die rechtlichen Voraussetzungen für diese erweiterte Nutzung werden derzeit sorgfältig geprüft. Ein zentrales Element dieser Prüfung ist die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO, um die mit der KI-Nutzung verbundenen Risiken zu identifizieren und angemessen zu bewerten. Erst nach Abschluss dieser Prüfung und der Festlegung geeigneter Schutzmaßnahmen kann die zweite Phase der Einführung beginnen.

Besonders hervorzuheben ist, dass LLMoin ausschließlich als Sprachtool eingesetzt wird und keine automatisierten Entscheidungen trifft oder Entscheidungsvorschläge generiert. Die globalen und lokalen Handlungsanweisungen des HmbBfDI untersagen ausdrücklich die Nutzung von LLMoin zur Entscheidungsfindung im Sinne des Art. 22 DSGVO. Vielmehr dient das System als unterstützendes

Werkzeug zur Formulierung und Prüfung von Texten, zur Recherche in bereitgestellten Dokumenten und zur Steigerung der Effizienz im Arbeitsalltag.

4. IVBeo2 der Polizei Hamburg: Weiterentwicklung der Videoüberwachung durch KI-Training

Die geplante Weiterentwicklung der „Intelligenten Videobeobachtung" (IVBeo) der Polizei Hamburg am Hansaplatz und Hachmannplatz durch Training der eingesetzten künstlichen Intelligenz mit eigenen Videosequenzen (IVBeo2) wirft komplexe datenschutzrechtliche Fragen auf. Der HmbBfDI hat das Vorhaben intensiv geprüft und begleitet, um die Einhaltung der gesetzlichen Vorgaben und den Schutz der Rechte der betroffenen Bürger:innen sicherzustellen.

Die Videobeobachtung öffentlicher Räume durch die Polizei Hamburg stellt einen erheblichen Eingriff in das Recht auf Schutz personenbezogener Daten dar, insbesondere für Bürger:innen, die sich ohne konkreten Anlass im überwachten Bereich aufhalten. Der HmbBfDI sieht derartige Maßnahmen grundsätzlich kritisch und prüft sie stets unter Berücksichtigung der engen gesetzlichen Voraussetzungen, wie sie insbesondere im Hamburgischen Gesetz über die Datenverarbeitung der Polizei (PolDVG) geregelt sind. Die Einhaltung dieser Vorgaben wird bei allen Videoüberwachungsvorhaben der Polizei Hamburg durch den HmbBfDI kontrolliert.

Seit 2019 beobachtet die Polizei Hamburg den Hansaplatz und seit 2024 den Hachmannplatz zu bestimmten Zeiten mittels Videotechnik. Beide gefahrenabwehrrechtlichen Maßnahmen waren jeweils bereits Gegenstand einer umfangreichen Prüfung des HmbBfDI (vgl. 29. Tätigkeitsbericht 2020, Kap. III 2 und 33. Tätigkeitsbericht 2024, Kap. II 2).

Das Projekt IVBeo wurde als Erweiterung der seit 2019 bestehenden Videoüberwachung am Hansaplatz im Jahr 2023 und am Hachmannplatz im Jahr 2025 eingeführt. Die eingesetzte Software, die auf künstlicher Intelligenz basiert, unterstützt Polizeibeamt:innen bei der Beobachtung, indem sie automatisiert Bewegungsmuster erkennt, die mit Gefährdungen assoziiert sind, und die Beamt:innen am Monitor auf relevante Szenen aufmerksam macht. Die abschließende Bewertung und die Einleitung polizeilicher Maßnahmen erfolgen weiterhin durch Menschen. Ursprünglich ist IVBeo mit Videodaten aus Mannheim trainiert worden. Der HmbBfDI begleitete auch diesen Pilotversuch im Jahr 2023 und hatte zunächst keine datenschutzrechtlichen Bedenken (vgl. 32. Tätigkeitsbericht 2023, Kap. III 1). Die Polizei Hamburg stellte im Rahmen der Projektevaluation allerdings fest, dass zahlreiche Detektionen des Systems nicht nachvollziehbar waren, da die Beamt:innen keine Gefahrensituationen erkennen konnten. Es gab also zu viele falsche Alarmmeldungen. Diese erhöhte Zahl nicht-polizeilich relevanter Hinweise wurde auf die eingeschränkte Testumgebung und die stichpunktartige Auswertung im Projekt IVBeo zurückgeführt.

Die Polizei Hamburg verfolgt daher mit dem Anschlussprojekt IVBeo2 nun das Ziel, die eingesetzte KI-Software durch Training und Testung mit eigenen Hamburger Videosequenzen vom Hansaplatz und Hachmannplatz weiterzuentwickeln und so eine Anpassung an die spezifischen örtlichen Gegebenheiten zu erreichen.

Durch den am 15. Januar 2025 angenommenen Änderungsantrag (Bü.-Drs. 22/17442) wird nun das Trainieren und Testen von IT-Systemen erfreulicherweise auch erstmalig und ausdrücklich in § 37a PolDVG auf ein rechtliches Fundament gestellt. (vgl. 33. Tätigkeitsbericht 2024 Kap. III 1.1).

Die Effektivität der Videobeobachtung soll durch das auf den nun vorhandenen § 37a PolDVG gestützte Trainieren mit Hamburger Daten erhöht werden. Zu diesem Zweck werden relevante Szenen – etwa besondere Wetterphänomene, Lichtverhältnisse oder Fehldetektionen – aus der laufenden Videobeobachtung manuell ausgewählt und von

der Polizei gespeichert. Diese Videosequenzen werden anschließend an das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) übermittelt, das die KI-Software entwickelt und betreibt.

Die Begleitung des Projekts durch den HmbBfDI war zunächst dadurch erschwert, dass die Polizei Hamburg die erforderlichen Unterlagen erst nach wiederholter Nachfrage und mit erheblicher zeitlicher Verzögerung zur Verfügung gestellt hat (vgl. 33. Tätigkeitsbericht 2024, Kap. IV 9). Dadurch erhielt der HmbBfDI erst im August 2025 umfassende Informationen und Dokumente von der Polizei Hamburg und dem IOSB zu dem geplanten Vorhaben. Im Anschluss beantwortete die Polizei Hamburg allerdings alle ergänzenden Nachfragen des HmbBfDI zeitnah. Die Prüfung des HmbBfDI konzentrierte sich insbesondere auf die Themen Sicherheit, Zugriff, Speicherung, Diskriminierungspotential und Löschung.

Nach sorgfältiger Auswertung der vorgelegten Unterlagen und der ergänzenden Auskünfte sieht der HmbBfDI keine durchgreifenden datenschutzrechtlichen Bedenken gegen das Training der KI-Modelle mit den Videoaufnahmen von Hansaplatz und Hachmannplatz. Die getroffenen technischen und organisatorischen Maßnahmen gewährleisten einen hohen Schutz der personenbezogenen Daten und eine den gesetzlichen Anforderungen genügende transparente Information der betroffenen Bürger:innen. Das vorgenommene Data Labeling (auch Data Tagging), mit dem unterschiedliche Datenpunkte der Videoaufnahmen mit Informationen gekennzeichnet werden, damit Machine-Learning-Algorithmen deren Bedeutung besser verstehen können, ließ für den HmbBfDI kein Diskriminierungspotenzial erkennen. Die Polizei Hamburg legte dar, dass die Ausgestaltung des Prozesses zur Identifikation, Speicherung und Löschung der Videosequenzen zudem detailliert dokumentiert und protokolliert wird. Das IOSB verarbeitet die Daten zudem in einem gesicherten Netzwerk, auf das ausschließlich wenige, genau festgelegte und sicherheitsüberprüfte Mitarbeiter:innen des IOSB Zugriff haben. Die Polizei Hamburg hat keinen Zugriff auf die beim IOSB gespeicherten und verarbeiteten Daten. Im Hinblick auf die beim IOSB gespeicherten Videosequenzen wurde dem HmbBfDI

nachvollziehbar dargelegt, dass die Trainingsdaten bis zum Ende des Projekts (voraussichtlich August 2026) aufbewahrt werden müssen, um die Software schrittweise an die Hamburger Verhältnisse anpassen zu können. Die Polizei Hamburg hat dem HmbBfDI zudem zugesichert, dass die betroffenen Personen vor Ort durch QR-Codes auf die mit dem Projekt verbundenen Datenschutzinformationen hingewiesen werden und sich so direkt informieren können.

Ein wichtiger Aspekt der datenschutzrechtlichen Bewertung betraf schließlich die Frage, ob aus den trainierten KI-Modellen Rückschlüsse auf die verwendeten Trainingsdaten gezogen werden können. Nach Auskunft des Fraunhofer IOSB speichern die bei IVBeo eingesetzten KI-Modelle lediglich abstrahierte Parameter, die die statistischen Zusammenhänge zwischen Eingabe- und Ausgabedaten beschreiben. Es werden keine Klarbilder oder sonstige personenbezogene Daten im Modell selbst gespeichert. Diese dienen ausschließlich als Trainingseingaben. Da die personenbezogenen Daten aus Hamburg nur einen sehr kleinen Teil der gesamten Trainingsdaten ausmachen, sei eine direkte Rückgewinnung oder Rekonstruktion spezifischer Trainingsdaten aus IVBeo praktisch ausgeschlossen. Eine Ableitung individueller Bewegungsprofile oder sonstiger personenbezogener Daten sei nach aktuellem Stand der Technik nicht möglich.

Nach letztem Kenntnisstand erfolgte am 8. Januar 2026 die erste Übergabe von Videosequenzen an das IOSB. Seit diesem Termin ist es dem IOSB möglich, das Training mit Hamburger Daten zu starten.

Die fortlaufende Überprüfung der Einhaltung der datenschutzrechtlichen Vorgaben bleibt ein zentrales Anliegen des HmbBfDI, um den Schutz der Rechte der Bürger:innen auch bei innovativen polizeilichen Maßnahmen sicherzustellen.

5. KI an Schulen

Der Einsatz von Künstlicher Intelligenz (KI) in Schulen bietet vielfältige Chancen, wirft jedoch auch erhebliche datenschutzrechtliche Fragen auf. Der HmbBfDI beleuchtet die Risiken und gibt Hinweise für einen verantwortungsvollen Umgang mit personenbezogenen Daten im schulischen Kontext.

Der Einsatz von KI im Schulbereich hat in den vergangenen Jahren deutlich zugenommen. Digitale Lernplattformen und intelligente Assistenzdienste versprechen eine individuelle Förderung von Schüler:innen und eine Entlastung der Lehrkräfte. Zahlreiche private Anbieter haben entsprechende Lösungen entwickelt und bieten diese Schulen und Schulträgern an. Diese Systeme verarbeiten dabei aber große Mengen personenbezogener Daten, darunter u.U. Leistungsdaten, Verhaltensanalysen und Kommunikationsinhalte.

Vor dem Einsatz von KI-Systemen im Bildungsbereich sind in den meisten Fällen eine umfassende Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen und die Risiken für die Rechte und Freiheiten der Betroffenen sorgfältig zu bewerten. Die Verarbeitung personenbezogener Daten von Schüler:innen, Lehrkräften und Eltern sollte auf Basis einer gesetzlichen Ermächtigung erfolgen. Gerade bei Minderjährigen ist der Einsatz von KI besonders sensibel zu behandeln, da sie häufig nicht die volle Tragweite der Datenverarbeitung überblicken können. Die Schule als verantwortliche Stelle muss sicherstellen, dass die Betroffenen transparent über die Zwecke, den Umfang und die Risiken der Datenverarbeitung informiert werden.

Ein weiteres zentrales Problemfeld ist die Zweckbindung der Datenverarbeitung. KI-Systeme sind häufig darauf ausgelegt, große Datenmengen zu analysieren und daraus Muster zu erkennen, die über den ursprünglichen Zweck hinausgehen können. Dies birgt die Gefahr, dass

Daten für andere Zwecke als die pädagogische Unterstützung verwendet werden, etwa zur Leistungsüberwachung oder, soweit vertraglich nicht ohnehin ausgeschlossen, zum Training der Modelle der LLM-Anbieter. Der HmbBfDI weist darauf hin, dass eine solche Zweckänderung nur unter bestimmten Voraussetzungen zulässig ist und stets einer sorgfältigen Prüfung bedarf.

Auch die Datenminimierung ist ein wesentliches Prinzip. KI-Anwendungen sollten nur die Daten verarbeiten, die für die jeweilige Funktion unbedingt erforderlich sind. In der Praxis zeigt sich jedoch, dass viele Systeme weit mehr Informationen erfassen, als tatsächlich benötigt werden. Der HmbBfDI empfiehlt, bereits bei der Auswahl und Implementierung von KI-Lösungen auf datensparsame Technologien zu setzen und regelmäßig zu überprüfen, ob die erhobenen Daten noch erforderlich sind.

Ein weiteres kritisches Thema ist die Transparenz der eingesetzten KI-Systeme. Häufig ist die Funktionsweise für Nutzer:innen und Verantwortliche schwer nachvollziehbar. Automatisierte Entscheidungsfindungen sollten im Schulbereich ohnehin keinen Einsatz finden, ansonsten unterlägen auch die entsprechenden Entscheidungslogiken Transparenzgrundsätzen. Dies erschwert die Kontrolle der Datenverarbeitung und die Wahrnehmung der Betroffenenrechte. Schulen sollten daher bei der Einführung von KI-Systemen auf eine möglichst hohe Nachvollziehbarkeit und Erklärbarkeit achten und die Betroffenen umfassend informieren.

Nicht zuletzt ist die Sicherheit der Daten ein zentrales Anliegen. KI-Systeme sind häufig mit externen Servern oder Cloud-Diensten verbunden, was zusätzliche Risiken für die Integrität und Vertraulichkeit der Daten mit sich bringt. Es empfiehlt sich daher, die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO regelmäßig zu überprüfen und insbesondere bei der Auswahl von Dienstleistern auf hohe Datenschutzstandards zu achten.

Die vorstehenden Grundsätze sind im Schulbereich sorgfältig auf das jeweils konkret eingesetzte KI-System anzuwenden. Denn im Schulbereich kommen ganz unterschiedliche KI-Systeme zum Einsatz, was von adaptiven Lernsystemen bis hin zu allgemeinen Lerntools mit KI-Funktionen zur Erfassung von Lernständen zur gezielten Leistungsverbesserung reichen kann. Der Funktionsumfang ist dann entscheidend für die konkreten Risiken für die Rechte und Freiheiten der Schüler: innen und den Umfang der deshalb zu ergreifenden technischen und organisatorischen Maßnahmen und die für eine Prüfung anzusetzenden Rechtmäßigkeitsanforderungen.

Zusammenfassend sieht der HmbBfDI im Einsatz von Künstlicher Intelligenz im Schulbereich sowohl Chancen als auch Risiken für die informationelle Selbstbestimmung der Betroffenen. Die Einhaltung der datenschutzrechtlichen Vorgaben ist eine Grundvoraussetzung für die Akzeptanz und den erfolgreichen Einsatz dieser Technologie. Schulen und Schulträger sind aufgefordert, die Rechte und Interessen der Betroffenen zu wahren und den Datenschutz von Anfang an in die Entwicklung und Nutzung von KI-Systemen zu integrieren.

6. ARGO-CL und KI im Gesundheitsbereich

Das Universitätsklinikum Hamburg-Eppendorf (UKE) hat mit ARGO-Clinical Letters (CL) ein KI-Modell entwickeln lassen und setzt dieses ein, um Epikrisen-Vorschläge für Arztbriefe zu generieren. ARGO-CL sammelt Befunde aus einer Patientenakte und kann daraus „mit nur einem Klick" entsprechende Entwürfe erstellen. Trainiert wurde das Modell mit mehreren Millionen pseudonymisierter Patientenakten des UKE.

Der HmbBfDI hat sich zunächst mit der Frage befasst, ob die Entwicklung des klinischen Large Language Models (LLM) ARGO-CL wissenschaftliche Forschung darstellt und deshalb rechtmäßig auf der Grundlage von Normen erfolgen konnte, die eine Verarbeitung

von Behandlungsdaten zu wissenschaftlichen Forschungszwecken erlauben (vgl. 33. TB 2024, Kap. IV 7). Dieselbe Frage stellt sich für das Nachtraining des Modells (Fine-Tuning).

Im Ergebnis kann für ARGO-CL in beiden Fällen die privilegierte Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken angenommen werden. Das UKE beziehungsweise die mit Entwicklung und Training des LLM befasste UKE-Tochtergesellschaft IDM gGmbH (IDM) hat auf Nachfrage zum Forschungskonzept und insbesondere zu der Anforderung an einen Erkenntnisgewinn ergänzend vorgetragen. Die formulierten und im Zusammenhang mit der Entwicklung und dem Fine-Tuning von ARGO-CL bearbeiteten Fragen ließen erkennen, dass es darum ging und geht, ein LLM für ein spezifisches Anwendungsgebiet – die Erstellung von standardisierten Arztbriefen, die den Anforderungen des deutschen Gesundheitssystems genügen – neu zu entwickeln. Außerdem wird die Performance des eingesetzten LLM untersucht und bewertet, unter anderem hinsichtlich der Risiken, die aus der Auswahl, Menge und Reihenfolge der bei der Erstellung von Epikrisen-Vorschlägen für Arztbriefe durch ARGO-CL verarbeiteten Informationen resultieren. Auch Abweichungen werden betrachtet, die sich im Verhältnis zur Erstellung von Epikrisen-Entwürfen durch behandelnde Ärzt:innen ergeben können. Die Möglichkeit der Berufung auf wissenschaftliche Forschung unterliegt in zeitlicher Hinsicht aber einer Beschränkung, und zwar wenn das KI-Modell zu einem bestimmten Zeitpunkt als ausreichend trainiert betrachtet wird und kein Nachtraining mehr erforderlich ist.

Auch zu den Anstrengungen, die seitens IDM unternommen wurden, um die zu Trainingszwecken eingesetzten Daten von Patient:innen im Vorfeld zu pseudonymisieren, wurden im Berichtsjahr zusätzliche Informationen zur Verfügung gestellt. Hier wird sich mit Blick auf die Stellungnahme 28 / 2024 des Europäischen Datenschutzausschusses zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen die abschließende Klärung der Frage anschließen, welche systemseitigen Maßnahmen – zum Schutz der Rechte und Freiheiten von Betroffenen – getroffen

worden sind, um das Risiko der Extraktion personenbezogener Daten aus ARGO-CL zu minimieren. Solche Maßnahmen wären nur dann nicht erforderlich, wenn sich das Modell letztendlich als anonym erweisen sollte – trotz der zum Training verwendeten, pseudonymisierten und damit weiterhin personenbeziehbaren Daten und trotz etwaiger personenbezogener Daten, die bereits im Zusammenhang mit der Entwicklung des zugrunde gelegten LLM vom bereitstellenden Unternehmen genutzt worden waren.

Neben ARGO-CL hat der HmbBfDI im Jahr 2025 Hinweise zum Einsatz weiterer KI-Anwendungen durch leistungserbringende Institutionen in Hamburg erhalten. So gibt es zum Beispiel Arztpraxen, in denen Telefonanrufe nicht mehr persönlich, sondern mittels KI-Telefonassistenten entgegengenommen werden. Anliegen wie Terminanfragen können gegebenenfalls unmittelbar selbst von der KI bearbeitet werden, bei anders gelagerten Anfragen, z. B. zu einer Diagnose oder einem Rezept, würde zur behandelnden Person durchgestellt werden müssen. Dafür müsste die KI die Anrufe aber grundsätzlich erst einmal entsprechend klassifizieren können.

Der Einsatz solcher KI-Telefonassistenten muss nicht zwangsläufig datenschutzrechtlich problematisch sein. In jedem Fall erfordert dieser aber eine transparente Information der betroffenen, anrufenden Personen durch die datenschutzrechtlich verantwortliche Stelle. Regelmäßig ist das die Praxis, die die KI einsetzt und dazu einen Auftragsverarbeitungsvertrag mit dem Anbieter abschließt, Art. 28 Abs. 3 DSGVO. Als Auftragsverarbeiter darf dieser die Daten der anrufenden Personen nicht ohne Weiteres zu eigenen Zwecken, z. B. zum Training der eigenen KI, einsetzen. Weiterhin wäre zum Beispiel auch darauf zu achten, dass sämtliche Personen, die bei dem Dienstleister mit den Daten der Anrufer:innen umgehen, im gleichen Umfang wie die Mitarbeitenden der Arztpraxis der Schweigepflicht unterliegen. Überdies haben in aller Regel die Praxisbetreiber vor Einsatz dieser Systeme eine Abschätzung der Risiken für die Betroffenen in Form einer Datenschutz-Folgeabschätzung vorzunehmen.

7. Ray-Ban Meta KI-Brille

Der HmbBfDI prüft seit Sommer 2025 die Ray-Ban Meta KI-Brille umfassend auf ihre datenschutzrechtlichen Implikationen. Ziel ist es, die Funktionsweise, die Erkennbarkeit von Aufnahmen sowie letztlich die Einhaltung der datenschutzrechtlichen Vorgaben zu bewerten. Die Untersuchung ist noch nicht abgeschlossen; ein Prüfbericht wird für 2026 erwartet.

Die Markteinführung der Ray-Ban Meta KI-Brille hat eine breite öffentliche und mediale Aufmerksamkeit hervorgerufen. Die Brille vereint klassische Funktionen einer smarten Brille – wie Foto- und Videoaufnahmen – mit KI-gestützten Features, darunter Meta AI und Echtzeit-Übersetzungen. Angesichts der damit verbundenen datenschutzrechtlichen Herausforderungen hat der HmbBfDI frühzeitig eine eigene Prüfung initiiert. Anlass waren neben der Berichterstattung auch Informationen der irischen Datenschutzaufsichtsbehörde DPC, die als federführende Behörde für Meta in Europa agiert. Ziel der Untersuchung ist die datenschutzrechtliche Bewertung der Ray-Ban Meta AI Glasses aus Sicht der Nutzenden in Deutschland mit Fokus auf KI-basierter Funktionalität sowie des rechtmäßigen Einsatzes speziell in sozialen Netzwerken sowie der Verwendung der anfallenden Daten zum KI-Training bei Meta.

Um einen unabhängigen und praxisnahen Eindruck zu gewinnen, hat der HmbBfDI zwei Exemplare der Brille beschafft und eine mehrstufige technische und rechtliche Analyse begonnen. Die Prüfung erfolgte sowohl im IT-Labor des HmbBfDI (siehe Kap. III 28) als auch in realen Anwendungsszenarien. Ein besonderer Fokus lag auf der Frage, inwieweit die Brille im Alltag durch ihre Nutzer:innen datenschutzkonform eingesetzt werden kann und ob die Rechte von Nutzer:innen und Dritten gewahrt bleiben.

Im ersten Schritt wurden die Grundfunktionen der Brille getestet. Die integrierte Kamera und die Mikrofone ermöglichen es, Fotos sowie Videos samt Tonaufnahmen zu erstellen. Dabei wurde insbesondere untersucht, ob für Außenstehende erkennbar ist, dass eine Aufnahme stattfindet. Die Brille verfügt über eine LED-Leuchte, die bei aktiver Aufnahme aktiviert werden soll. Die Sichtbarkeit dieser LED wurde in verschiedenen Situationen geprüft, um festzustellen, ob sie tatsächlich einen wirksamen Hinweis für Dritte darstellt. Gerade im öffentlichen Raum ist es essenziell, dass Personen, die aufgenommen werden, dies auch wahrnehmen können.

Ein weiterer Schwerpunkt der Prüfung lag auf den KI-Funktionen der Brille. Die Ray-Ban Meta KI-Brille bietet unter anderem die Möglichkeit, per Sprachbefehl Fotos und Videos aufzunehmen, Übersetzungen in Echtzeit zu erhalten und mit Meta AI zu interagieren. Der HmbBfDI hat geprüft, ob die vom Europäischen Datenschutzausschuss (EDSA) vorgegebenen Voraussetzungen zum Einsatz von KI-Modellen (Stellungnahme 28 / 2024) umgesetzt wurden. Zudem steht der HmbBfDI in einem direkten Austausch auch mit der federführenden Aufsichtsbehörde in Irland (IDPC) und hat ihr bereits einen umfassenden Fragekatalog vorgelegt.

Um die technische Funktionsweise der Brille besser zu verstehen, wurde eine der Brillen durch IT-Forensiker:innen geöffnet und die einzelnen Bauteile analysiert. Zudem wurden die bei der Nutzung entstehenden Datenströme untersucht. Dabei zeigte sich, dass ein Großteil der übertragenen Daten verschlüsselt ist, sodass eine weitergehende Analyse der konkreten Inhalte nur eingeschränkt möglich war. Dennoch konnten wertvolle Erkenntnisse über die Art und den Umfang der Datenübertragung gewonnen werden.

Besondere Aufmerksamkeit galt den Tonaufnahmen, durch die sowohl Geräusche und Gespräche der Nutzer:innen der Brille als auch von Dritten im Umfeld erfasst werden können. Der HmbBfDI hat geprüft, inwieweit die Erfassung von Gesprächen für die Betroffenen erkennbar ist und ob die Brille die Anforderungen an die Einwilligung und die Wahrung der Persönlichkeitsrechte erfüllt.

Die Prüfung der Ray-Ban Meta KI-Brille ist noch nicht abgeschlossen. Der HmbBfDI hat im Sommer 2025 mit der Untersuchung begonnen und rechnet im Jahr 2026 mit einem Abschluss. Die Ergebnisse werden in einem gesonderten Prüfbericht veröffentlicht, der sowohl technische als auch rechtliche Aspekte umfassend beleuchten wird. Ziel ist es, die Rechte der Bürgerinnen und Bürger zu schützen, die Nutzenden zu sensibilisieren und einen verantwortungsvollen Umgang mit innovativen Technologien zu fördern. Des Weiteren wird der finale Prüfbericht auch der federführenden Aufsichtsbehörde in Irland (IDPC) vorgelegt, die etwaige Maßnahmen ergreifen oder Empfehlungen abgeben kann, wenn sich noch Nachbesserungsbedarf aus datenschutzrechtlicher Sicht auf Seiten von Meta ergeben sollte. Die fortlaufende Überprüfung bleibt angesichts regelmäßiger Produktupdates und Anpassungen der Datenschutzpolitik von Meta unerlässlich.

8. Orientierungshilfe der DSK zu generativen KI-Systemen mit RAG-Methode

Im Oktober 2025 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine umfassende Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit Retrieval Augmented Generation (RAG)-Methode. Sie bietet Verantwortlichen, die den Einsatz solcher Systeme planen oder bereits umsetzen, eine Grundlage für deren datenschutzkonforme Gestaltung und Bewertung.

Die zunehmende Verbreitung generativer KI-Systeme, insbesondere solcher, die ein Large Language Model (LLM) mit der Retrieval Augmented Generation (RAG)-Methode kombinieren, stellt Verantwortliche vor neue datenschutzrechtliche Herausforderungen. Die RAG-Methode ermöglicht es, ein LLM gezielt mit aktuellen oder organisationsspezifischen Informationen aus einer separaten Datenbasis zu versorgen. Hierzu werden relevante Textabschnitte aus Referenzdokumenten

mittels eines Embedding-Modells in einen Vektorraum überführt und in einer Vektordatenbank gespeichert. Bei einer Anfrage werden die semantisch passenden Abschnitte durch einen Retriever identifiziert und dem LLM als Kontext zur Generierung einer Antwort bereitgestellt. Diese technische Architektur bietet Vorteile hinsichtlich der Richtigkeit und Nachvollziehbarkeit der Ausgaben, wirft aber auch spezifische datenschutzrechtliche Fragen auf.

Die Orientierungshilfe der DSK analysiert die Auswirkungen der RAG-Methode auf die Einhaltung der Grundsätze der Datenschutz-Grundverordnung (DSGVO), insbesondere im Hinblick auf Richtigkeit, Transparenz, Integrität, Zweckbindung, Datenminimierung und die Wahrung der Betroffenenrechte. Ein zentrales Ergebnis ist, dass die RAG-Methode die Möglichkeit eröffnet, die generierten Antworten eines KI-Systems an überprüfbaren und aktuellen Informationen auszurichten. Fehlerhafte oder veraltete Daten in den Referenzdokumenten können gezielt aktualisiert oder gelöscht werden, was im Zusammenhang mit personenbezogenen Daten die Umsetzung des Grundsatzes der Richtigkeit nach Art. 5 Abs. 1 Buchst. d DSGVO erleichtert. Allerdings bleibt die datenschutzrechtliche Bewertung des zugrundeliegenden LLM unberührt: Ein auf unklarer Rechtsgrundlage trainiertes LLM bleibt auch im RAG-System problematisch, sodass die Anforderungen an die Rechtmäßigkeit des Trainings nicht entfallen. Vgl. hierzu auch Kap. I 1.

Die Orientierungshilfe hebt hervor, dass die Nachvollziehbarkeit der generierten Antworten durch die Dokumentation der genutzten Referenzdokumente verbessert werden kann. Nutzer:innen können erkennen, auf welche konkreten Informationen bzw. Dokumente sich die KI-Ausgabe stützt. Die Transparenz hinsichtlich der Funktionsweise des LLM selbst bleibt jedoch eingeschränkt, da die internen Prozesse der Sprachmodelle und die Bedeutung der erzeugten Embeddings für Außenstehende schwer nachvollziehbar sind. Verantwortliche sind daher angehalten, die Auswahl und Qualität der Referenzdokumente sorgfältig zu prüfen und die entsprechenden Informationspflichten gegenüber den Betroffenen zu erfüllen.

Die Orientierungshilfe betont zudem die Vorteile der RAG-Methode für die Integrität und Vertraulichkeit der verarbeiteten Daten. Da personenbezogene Daten in der Vektordatenbank und den Referenzdokumenten gespeichert werden und nicht dauerhaft im LLM verbleiben, können bewährte technische und organisatorische Maßnahmen wie Mandantentrennung und Rechte- und Rollenkonzepte angewendet werden, insbesondere bei sensiblen Daten nach Art. 9 und 10 DSGVO. Die Möglichkeit, ein RAG-System on-premise zu betreiben, reduziert zudem das Risiko einer Übertragung personenbezogener Daten an externe Betreiber großer Sprachmodelle.

Ein weiterer Schwerpunkt der Orientierungshilfe liegt auf der Zweckbindung und Datenminimierung. Die gezielte Bereitstellung von Referenzdokumenten für das RAG-System ermöglicht eine strikte Begrenzung der Verarbeitung auf den jeweiligen Verarbeitungszweck. Die Datenminimierung wird dadurch unterstützt, dass nur die für die jeweilige Anwendung erforderlichen Dokumente in die Vektordatenbank aufgenommen werden. Die gezielte Löschung von personenbezogenen Daten kann technisch durch das Entfernen von Einträgen in der Datenbank und den Referenzdokumenten umgesetzt werden. Soweit sich die Rechte auf die Referenzdokumente und die Vektordatenbank beziehen, ist die Umsetzung der Betroffenenrechte in RAG-Systemen grundsätzlich möglich. Dabei ist allerdings zu beachten, dass durch die RAG-Komponenten (Referenzdokumente, Embedding-Modell) eine zusätzliche Verarbeitung (Speicherung) personenbezogener Daten erfolgt, die ihrerseits datenschutzrechtliche Pflichten nach sich zieht.

Der HmbBfDI hat an der Erarbeitung dieses Papiers mitgewirkt und unterstützt die darin formulierten Empfehlungen ausdrücklich. Er wird die Entwicklung in diesem Bereich weiter begleiten und steht für Beratungen und Rückfragen zur Verfügung.

9. The Bridge Blueprint: Ein Brückenschlag zwischen Datenschutz und KI-Regulierung

Das Diskussionspapier „The Bridge Blueprint" behandelt die Schnittstellen zwischen Datenschutz und KI-Regulierung in Europa. Der Anspruch ist, einen Weg aufzuzeigen, der die Anwendung beider Regelwerke in der Praxis harmonisiert. Im Rahmen einer öffentlichen Konsultation sind zahlreiche Rückmeldungen eingegangen, die Impulse für die Weiterentwicklung des Ansatzes liefern. Dabei ist der ganzheitliche Ansatz auf große Zustimmung gestoßen.

Die europäische Debatte um Künstliche Intelligenz (KI) und Datenschutz ist von Unsicherheiten und komplexen Überschneidungen verschiedener Rechtsakte geprägt. Insbesondere das Zusammenspiel der DSGVO mit der KI-Verordnung (KI-VO) wirft vielfältige Fragen auf. Vor diesem Hintergrund hat die Europäische Kommission ein sog. Omnibus-Paket mit Rechtsänderungen vorgelegt, das auch Reformen der DSGVO mit Blick auf KI-spezifische Anforderungen vorsieht. Die dazu kontrovers geführte Reformdebatte macht aber deutlich, dass die Herausforderungen im Zusammenspiel von Datenschutz und KI-Regulierung nicht allein durch Gesetzesänderungen gelöst werden können.

Das Diskussionspapier „The Bridge Blueprint" (https://datenschutz-hamburg.de/news/eine-bruecke-zwischen-dsgvo-und-ki-vo-das-diskussionspapier-the-bridge-blueprint) hat diese Problematik aufgegriffen und verdeutlicht, dass ein ganzheitlicher, verbindender Ansatz notwendig ist, um die Schnittstellen zwischen der DSGVO und sektorspezifischen Regelungen wie der KI-Verordnung zu gestalten.

Die DSGVO gilt zwar grundsätzlich unberührt von anderer Digitalregulierung. Dieser Grundsatz schließt jedoch eine Auslegung nicht aus, die andere Digitalrechtsakte mit in den Blick nimmt.

Gerade beim Einsatz von KI-Systemen treten Risiken für die Rechte und Freiheiten der Betroffenen besonders deutlich zutage. Das Brückenpapier nimmt diese Herausforderung auf und zeigt anhand ausgewählter Problemfelder – von den Datenschutzgrundsätzen, Rechtsgrundlagen und besonderen Kategorien personenbezogener Daten bis hin zu automatisierten Entscheidungen –, dass die KI-Verordnung die praktische Anwendung der DSGVO prägt. Dabei wird die DSGVO als verbindendes Brückenrecht verstanden, das Datenschutzprinzipien mit den technischen und regulatorischen Anforderungen der KI-VO zusammenführt. Ziel ist es, die Anwendung beider Regelwerke zu harmonisieren und so Rechtssicherheit für den Betrieb von KI-Systemen zu schaffen.

10. Umsetzung der KI-VO

Die Mitgliedstaaten haben zur Durchführung der europäischen KI-Verordnung (KI-VO) die Aufgabe, zuständige Marktüberwachungsbehörden zu benennen. Der Entwurf des Bundesgesetzgebers legt die Aufsicht pauschal in die Hände der Bundesnetzagentur, ohne dabei spezifische Anforderungen des Unionsrechts und des deutschen Föderalismus zu berücksichtigen. Die Folge könnte sein, dass beispielsweise der Einsatz von LLMoin in der Hamburgischen Verwaltung von einer Bundesbehörde kontrolliert wird.

Im Jahr 2026 entscheidet sich die politische Kontroverse, wer in Deutschland die Marktüberwachung über die Einhaltung der Pflichten aus der KI-VO beim Einsatz von KI-Systemen übernimmt. In Bezug auf die meisten nichtöffentlichen Stellen ist es wahrscheinlich, dass die Bundesnetzagentur dafür ausgewählt wird. Der Entwurf des Bundesgesetzgebers sieht es entsprechend vor. Nach dessen Vorschlag soll die Zuständigkeit auch pauschal den öffentlichen Bereich des Bundes und der Länder betreffen. Gegen Letzteres regt sich zu Recht Widerspruch aus dem Bundesrat.

So ist es ist im Hinblick auf die Hochrisiko-Sektoren der Bildung und grundlegender öffentlicher Dienstleistungen zweifelhaft, inwiefern eine Übertragung der Marktüberwachung an eine Bundesbehörde verfassungsrechtlich zulässig wäre. Da Bildung, Ausbildung und Wissenschaft sowie die Daseinsvorsorge regelmäßig Ländersache sind, steht die vorgesehene Zuständigkeit einer zentralen Bundesbehörde im Konflikt zur Eigenstaatlichkeit der Länder und der Zuständigkeitsordnung des Grundgesetzes. Die Verwaltung obliegt grundsätzlich den Ländern. Die Länder führen die Bundesgesetze als eigene Angelegenheit aus, eine Bundesbehörde kann lediglich im spezifisch geregelten Fall zuständig sein. Nach Art. 87 Abs. 3 Satz 1 GG können für Angelegenheiten, für die dem Bund die Gesetzgebung zusteht, selbständige Bundesoberbehörden errichtet werden. Die Begründung zum Gesetzentwurf nennt als Grundlage für die Gesetzgebungskompetenz des Bundes das Recht der Wirtschaft gemäß Art. 74 Nr. 11 GG. Die oben genannten Bereiche unterfallen aber der ausschließlichen Gesetzgebungs- und Verwaltungskompetenz der Länder. Soweit die Länderstellen KI-Systeme für einen Markt entwickeln, unterfallen sie auch dem Recht der Wirtschaft. Soweit aber Schulbehörden, Polizei- oder Verwaltungsbehörden der Länder Hochrisiko-KI-Systeme als Anbieter für eigene Zweck entwickeln oder als Betreiber anwenden und an keinem Marktgeschehen teilnehmen, unterfällt diese Tätigkeit nicht mehr dem Recht der Wirtschaft, sondern allein dem jeweiligen Landesrecht.

In spezifischen öffentlich-rechtlichen Bereichen benennt die KI-VO dabei sogar explizit die Datenschutzbehörden als Marktaufsicht. Gleichwohl schlägt der Bundesgesetzgeber auch dort eine Zuständigkeit der Bundesnetzagentur vor. Die KI-VO weist die Zuständigkeit für die Marktüberwachung über die in Anhang III Nr. 1 genannten Hochrisiko-KI-Systeme, sofern diese für Strafverfolgungszwecke, Grenzmanagement, Justiz und Demokratie eingesetzt werden, sowie über die nach Anhang III Nummern 6, 7 und 8 genannten Hochrisiko-KI-Systeme nach Art. 74 Absatz 8 KI-VO den Datenschutzaufsichtsbehörden bzw. jenen Behörden zu, die nach den Bedingungen der DSGVO oder JI-Richtlinie benannt wurden. Es handelt sich hier um ein Ergebnis der

Trilog-Verhandlungen: Privilegien beim KI-Einsatz durch Strafverfolgungsbehörden wurden nur unter der Bedingung akzeptiert, dass die für die Durchsetzung der JI-Richtlinie bereits zuständigen Behörden die Marktüberwachung wahrnehmen. In Deutschland sind dies die Datenschutzaufsichtsbehörden, die damit in allen von Art. 74 Abs. 8 KI-VO aufgezeigten Varianten die zu benennenden Behörden sind. In der nationalen Umsetzung besteht folglich gem. Art. 74 Abs. 8 KI-VO kein Spielraum im Sinne einer Öffnungsklausel.

Der Blick in die weiteren Mitgliedstaaten zeigt ein klares Bild. Die meisten Mitgliedstaaten weisen ihren Datenschutzbehörden eine zentrale Rolle bei der Aufsicht über die KI-VO zu. Nur Staaten mit neu gegründeten zentralen KI-Behörden weichen teilweise davon ab, binden die Datenschutzbehörden jedoch entweder beratend, durch Repräsentation in der KI-Behörde oder durch Sonderkompetenzen ein. Allein der deutsche Entwurf sieht trotz dezentraler Struktur einen bewussten Ausschluss der Datenschutzbehörden vor. Der deutsche Entwurf weicht von der sich europaweit etablierenden Grundstruktur ab mit der Begründung, dass die Datenschutzbehörden „primär grundrechtsschützend" seien. Dieser Ansatz ist in doppelter Hinsicht falsch. Zum einen setzen sich die Datenschutzbehörden nicht einseitig für das Recht auf informationelle Selbstbestimmung ein. Bereits die Kompetenzen des HmbBfDI für Informationsfreiheit sowie für Zugangsansprüche nach dem Data Act (siehe Kap. III 32) verdeutlichen den Auftrag der Behörde, ein ausgewogenes Verhältnis aus Datennutzung und Datenschutz zu gewährleisten. Zum anderen enthält Art. 74 Abs. 8 KI-VO in Verbindung mit Art. 43 Abs. 1 UAbs. 3 KI-VO ein grundrechtsschützendes Element zu Gunsten der durch den KI-Einsatz betroffenen Personen. Die unionsrechtliche Zuständigkeitsregelung bezweckt gerade eine institutionelle Verschränkung von Produktsicherheit und Grundrechtsschutz. Eine Aufsichtsbehörde zu benennen, die auch die Einzelinteressen Betroffener in den Blick nimmt, ist in den punktuellen, grundrechtssensiblen Bereichen des Art. 74 Abs. 8 KI-VO gerade der erkennbare Wille des Unionsgesetzgebers.

Der HmbBfDI steht der Verwaltung ohnehin als Ansprechpartner für Auslegungs- und Umsetzungsfragen im Hinblick auf die KI-VO zur Verfügung, solange keiner anderen Stelle diese Aufgabe durch Gesetz zugewiesen ist. Zudem erfordert die tägliche Datenschutzaufsicht die Berücksichtigung auch der Wertungen und Bestimmungen der KI-VO (siehe Kap. IV 9). Würde die Marktaufsicht in diesem Bereich an eine andere Bundesbehörde gegeben werden, müssten sich die Senatsbehörden die Verarbeitung personenbezogener Daten im KI-Kontext künftig mit zwei Aufsichtsbehörden abstimmen.

BUSSGELDER, ANORDNUNGEN, GERICHTSVERFAHREN V.

Bussgelder, Anordnungen, Gerichtsverfahren

1. Meldungen personenbezogener Daten an das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) – Rechtmäßigkeit und Interessenabwägung

Das Hinweis- und Informationssystem der Versicherungswirtschaft ist ein wichtiges Instrument für die Aufdeckung von betrügerischen Aktivitäten. Gleichzeitig hat eine Eintragung einen stigmatisierenden Charakter für die Betroffenen. Bei der Frage, ob Einmeldungen zurecht erfolgen oder nicht, sind daher die Belange und Interessen beider Beteiligter zu berücksichtigen und sorgfältig gegeneinander abzuwägen.

Im Berichtsjahr wurde der HmbBfDI mit einer Beschwerde befasst, in der eine Versicherungsnehmerin das Einschreiten gegen die Einmeldung ihrer personenbezogenen Daten in das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) begehrte. Hintergrund war ein Schadenfall, den die Betroffene ihrer Tierhalterhaftpflichtversicherung gemeldet hatte. Nach Prüfung durch einen Gutachter wurde der Schaden jedoch nicht als durch das Tier verursacht, sondern als sogenannter Thermikschaden eingestuft, also ein Schaden, der durch Temperaturunterschiede entstanden ist. Die Versicherung lehnte daraufhin die Regulierung ab und meldete den Vorgang unter Angabe der persönlichen Daten der Versicherungsnehmerin an das HIS. Die Betroffene wurde über die Einmeldung informiert und wandte sich nach erfolgloser Korrespondenz mit der Versicherung an den HmbBfDI.

Das HIS dient dem Informationsaustausch zwischen Versicherungsunternehmen und unterstützt diese bei der Risikobeurteilung, der Aufklärung von Versicherungsfällen und der Bekämpfung von Versicherungsmissbrauch. Die Einmeldung von personenbezogenen Daten erfolgt insbesondere dann, wenn im Zusammenhang mit einem Schadenfall Auffälligkeiten festgestellt werden, die auf ein erhöhtes Risiko oder einen möglichen Betrug zum Nachteil der Versicherung hindeuten

könnten. Die Versicherungsnehmerin sah sich durch die Einmeldung zu Unrecht in den Verdacht des Versicherungsbetrugs gestellt und machte geltend, sie habe nach bestem Wissen und Gewissen gehandelt. Sie forderte die Löschung ihrer personenbezogenen Daten aus dem HIS.

Der HmbBfDI prüfte die Einmeldung der personenbezogenen Daten eines hamburgischen Versicherers in das HIS unter Berücksichtigung der datenschutzrechtlichen Vorgaben. Maßgeblich für die Zulässigkeit der Datenverarbeitung ist Art. 6 Abs. 1 lit. f) DSGVO, wonach eine Verarbeitung rechtmäßig ist, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Im Rahmen dieser Interessenabwägung ist zu berücksichtigen, dass Versicherungsunternehmen auf zutreffende Angaben der Versicherungsnehmer angewiesen sind, da sie regelmäßig keine eigene Kenntnis vom Schadenshergang haben. Die Einmeldung in das HIS dient dazu, auffällige Sachverhalte zu dokumentieren und anderen Versicherern Hinweise auf mögliche Unregelmäßigkeiten zu geben.

Im vorliegenden Fall war entscheidend, dass die Versicherungsnehmerin ihre Annahme zum Schadenshergang als Tatsache dargestellt hatte, obwohl sie den tatsächlichen Ablauf nicht sicher beobachten konnte und die als Annahme sich zudem nachträglich als unzutreffend herausstellte. Die Versicherung konnte daher von einer betrugsgeneigten Auffälligkeit ausgehen, ohne dass es auf eine nachgewiesene Betrugsabsicht ankam.

Die Prüfung durch den HmbBfDI ergab, dass die Einmeldung im Einklang mit den datenschutzrechtlichen Vorgaben stand. Das berechtigte Interesse der Versicherung an der Einmeldung und der Funktionsfähigkeit des HIS überwog im konkreten Fall die Interessen der betroffenen Person. Im Besonderen hatte die betroffene Person durch ihre Angaben selbst den Anlass für die Einmeldung gesetzt. Ein Anspruch auf Löschung der Daten bestand daher nicht. Auch ein Widerspruch gegen die Verarbeitung nach Art. 21 DSGVO war nicht erfolgreich,

da keine besonderen, über die allgemeinen Interessen hinausgehenden Gründe vorlagen. Die betroffene Person wandte sich nach der Entscheidung des HmbBfDI an das Verwaltungsgericht Hamburg, das die Entscheidung des HmbBfDI bestätigte und die Klage abwies (VG Hamburg, Urt. v. 30.09.2025 - 17 K 5439/23).

Der Fall verdeutlicht, dass die Einmeldung personenbezogener Daten in das HIS ein sensibles Instrument ist, das einer sorgfältigen datenschutzrechtlichen Prüfung bedarf. Die Interessen betroffener Personen sind im Einzelfall gegen das berechtigte Interesse der Versicherungsunternehmen an der Betrugsprävention abzuwägen. Die Einmeldung ist nur zulässig, wenn sie erforderlich ist und keine milderen Mittel zur Zweckerreichung bestehen. Betroffene Personen haben das Recht, die Berichtigung oder Löschung ihrer personenbezogenen Daten zu verlangen, wenn diese unzutreffend oder unrechtmäßig verarbeitet wurden. Der HmbBfDI wird auch künftig die Rechtmäßigkeit solcher Einmeldungen sorgfältig prüfen und steht betroffenen Personen als Ansprechpartner zur Verfügung, wenn hamburgische Versicherer Einmeldungen in das HIS vornehmen.

2. Bußgelder wegen unbefugten Zugriffs auf eine Patientenakte durch Beschäftigte eines Krankenhauses

Ein Zugriff auf Patient:innenakten ohne beruflichen Grund und ohne Einwilligung der betroffenen Personen ist ein schwerwiegender Verstoß gegen Vorschriften der DSGVO. Dies kann ein Bußgeld rechtfertigen.

Im Berichtszeitraum wurde der HmbBfDI über eine Datenpanne in einem Hamburger Krankenhaus informiert. Zwei medizinische Beschäftigte hatten die elektronische Patientenakte eines Kollegen aufgerufen und eingesehen, der dort behandelt wurde. Der Zugriff wurde im Krankenhausinformationssystem protokolliert.

Beide Beschäftigten waren nicht an der medizinischen Behandlung des Kollegen beteiligt. Sie hatten keinen beruflichen Anlass, die Gesundheitsdaten ihres Kollegen einzusehen. Ihr Handeln lag außerhalb ihrer dienstlichen Aufgaben und diente eigenen Zwecken. Beschäftigte, die außerhalb ihrer beruflichen Aufgaben und Befugnisse personenbezogene Daten für eigene Zwecke verarbeiten, gelten als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. In diesen Fällen tragen nicht die Arbeitgeber:innen, sondern die jeweils handelnden Mitarbeiter:innen selbst die datenschutzrechtliche Verantwortung und können Adressat:innen eines Bußgeldbescheids werden. Auf die berufsfremden Motive der Beschäftigten für die Einsichtnahme, wie etwa Neugier oder auch Empathie, kommt es insoweit nicht an.

Die Verarbeitung besonderer Kategorien personenbezogener Daten, wie Gesundheitsdaten, ist nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Ausnahmen, etwa eine Verarbeitung aufgrund einer Einwilligung oder zur Durchführung einer medizinischen Behandlung, sind in Art. 9 Abs. 2 DSGVO geregelt. Diese lagen hier nicht vor. Die technische Möglichkeit, im Krankenhausinformationssystem auf eine Akte zuzugreifen, entbindet die Nutzenden nicht von der Pflicht, personenbezogene Daten nur im Rahmen der ihnen übertragenen Aufgaben zu verarbeiten.

Der HmbBfDI verhängte gegen beide Beschäftigte ein Bußgeld, auch um die Bedeutung des Schutzes personenbezogener Daten im Gesundheitswesen zu unterstreichen. Ein Beschäftigter akzeptierte das Bußgeld, die andere Beschäftigte legte Einspruch ein. Sie räumte den Zugriff zwar ein, argumentierte aber, dass der Krankenhausalltag vielfältige Konstellationen bereithalte, die eine Einsichtnahme auch ohne systemseitige Erfassung als Behandlerin rechtfertigen könnten. Der HmbBfDI bewertete diese Argumentation als zu allgemein und nicht nachvollziehbar. Das Verfahren wurde an das Amtsgericht Hamburg abgegeben. Das Gericht stellte das Verfahren nach zwei Verhandlungstagen wegen nicht gebotener Ahndung gem. § 47 Abs. 2 OWiG ein. Nach Auffassung der Vorsitzenden sei nicht nachgewiesen geworden, dass die Beschäftigte nicht an der Behandlung des Kollegen beteiligt

gewesen sei und ein Versuch, den Sachverhalt durch die Befragung weiterer Zeugen aufzuklären, sei aus Sicht des Gerichts unverhältnismäßig.

Der HmbBfDI kann die Entscheidung des Gerichts nicht nachvollziehen. Der rechtswidrige Zugriff wurde protokolliert und durch eine Datenpannen-Meldung des Krankenhauses bekannt. Es war die eigene und zutreffende Wertung des Krankenhauses als Arbeitgeberin, dass der Zugriff der Beschäftigten auf die Patientenakte ihres Kollegen rechtswidrig erfolgt war. Der HmbBfDI wird in vergleichbaren Fällen auch künftig prüfen, ob die Verhängung eines Bußgelds gegen Beschäftigte eines Krankenhauses geboten ist. Patient:innen müssen darauf vertrauen können, dass ihre Gesundheitsdaten nur mit Rechtsgrundlage verarbeitet werden. Dies gilt auch für Beschäftigte, die als Patient:innen behandelt werden. Unbefugte Zugriffe auf Patient:innenakten gefährden dieses Vertrauen.

3. Bußgeld wegen unzureichender Transparenz bei einer automatisierten Entscheidung über Kreditkartenanträge

Kommt ein Unternehmen bei rein automatisierten Entscheidungen über Kreditkartenanträge seinen datenschutzrechtlichen Informations- und Auskunftspflichten gegenüber Antragstellenden nicht nach, kann dies zu einer spürbaren Sanktion führen. Betroffene Personen müssen die Gründe und Kriterien nachvollziehen können, die zu einer ablehnenden Entscheidung ihres Kreditkartenantrags geführt haben. Dies gilt insbesondere bei Entscheidungen, die ausschließlich auf Algorithmen eines Unternehmens basieren.

Der HmbBfDI hat im Berichtszeitraum ein Bußgeld im mittleren sechsstelligen Bereich gegen ein Unternehmen aus der Finanzwirtschaft verhängt, da es die Informations- und Auskunftspflichten bei auto-

matisierten Entscheidungen in mehreren Fällen nicht ausreichend erfüllt hatte.

Automatisierte Entscheidungen, die auf Basis von Algorithmen und ohne menschliches Eingreifen getroffen werden, sind in der Kreditwirtschaft längst Alltag. Gerade im Finanzsektor ist die Nachvollziehbarkeit automatisierter Entscheidungen von besonderer Bedeutung, da die Ablehnung eines Kreditkartenantrags erhebliche Auswirkungen für die betroffenen Personen haben kann. Ohne Kreditkarte ist die gesellschaftliche Teilhabe oft eingeschränkt, zum Beispiel sind Buchungen von Mietwagen oder Hotels in vielen Fällen ohne Kreditkarte nicht möglich. Die DSGVO sieht daher vor, dass automatisierte Entscheidungen nur unter den engen Voraussetzungen von Art. 22 DSGVO zulässig sind und Verantwortliche weitergehende Informationspflichten gemäß den Artt. 12 Abs. 1, 13 Abs. 2 lit. f), 14 Abs. 2 lit. g) DSGVO erfüllen müssen. Betroffene Personen haben zudem das Recht, auf Antrag gem. Artt. 12 Abs. 1, 15 Abs. 1 lit. h) DSGVO aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zu erhalten.

In den zugrunde liegenden Beschwerdefällen hatte das Unternehmen online gestellte Kreditkartenanträge mittels eines automatisierten Systems abgelehnt, ohne den Antragstellenden ausreichend zu erklären, warum ihre Anträge trotz guter Bonität nicht erfolgreich waren. Die Antworten des Unternehmens waren so allgemein gehalten, dass die betroffenen Personen die ablehnenden Entscheidungen nicht nachvollziehen konnten. Die DSGVO verlangt jedoch, dass bei der Erhebung der Daten verständlich erläutert wird, nach welchen Kriterien das System entscheidet und der betroffenen Person auf Antrag zusätzlich erklärt wird, welche Faktoren in ihrem konkreten Fall für die Entscheidung ausschlaggebend waren. Erst dadurch wird sie in die Lage versetzt, ihre weiteren Rechte gemäß Art. 22 Abs. 3 DSGVO geltend zu machen, wie die Überprüfung der Entscheidung durch einen Menschen, die Darlegung des eigenen Standpunkts und die Anfechtung der Entscheidung.

Dieses Bußgeldverfahren und auch die hierzu bereits ergangene Rechtsprechung des EuGH (Rechtssache C-634/21 – „Schufa“ und Rechtssache C-203/22 – „Dun & Bradstreet“) verdeutlichen, dass die Erklärbarkeit automatisierter Entscheidungen ein zentrales Datenschutzthema ist, das mit der fortschreitenden Digitalisierung weiter an Bedeutung gewinnt. Die Datenschutzaufsichtsbehörden nehmen das Transparenzgebot computergestützter Entscheidungen verstärkt in den Blick und schreiten konsequent ein, bevor sich unrechtmäßige Prozesse verfestigen. Für Unternehmen bedeutet dies, dass sie nicht nur die technischen und rechtlichen Anforderungen automatisierter Systeme erfüllen, sondern auch die Ressourcen für eine adressatengerechte Erklärung im Einzelfall vorhalten müssen. Nur so kann gewährleistet werden, dass der Mensch nicht zum Objekt undurchsichtiger IT-Systeme wird, sondern seine Rechte gegenüber der datenverarbeitenden Stelle wirksam wahrnehmen kann.

Im Verwaltungs- und Bußgeldverfahren hat das Unternehmen erhebliche Anstrengungen unternommen, um seine Prozesse zur Erfüllung der Rechte der betroffenen Personen zu verbessern und umfangreich mit dem HmbBfDI zusammengearbeitet. In Abstimmung mit dem HmbBfDI wurden Formulierungen für eine verständliche Erläuterung der Ablehnungen von Kreditkartenanträgen entwickelt, mit denen einerseits die Nachvollziehbarkeit der Entscheidungen für die Antragstellenden sichergestellt und andererseits legitime Geheimhaltungsinteressen des Unternehmens gewahrt werden. Diese Anstrengungen und die Kooperationsbereitschaft des Unternehmens wurden bei der Bemessung des Bußgeldes erheblich mildernd berücksichtigt. Der Bußgeldbescheid wurde von dem Unternehmen akzeptiert.

4. Bußgeld gegen Handelsunternehmen wegen unterlassener Negativauskunft bei Auskunfts-, Löschungs- und Werbewiderspruchsanträgen

Unternehmen müssen sicherstellen, dass sie auch dann fristgerecht und umfassend auf Auskunftsanträge, Löschungsanträge und Widersprüche gegen Direktwerbung betroffener Personen reagieren, wenn keine personenbezogenen Daten verarbeitet werden. Die Einhaltung dieser Pflicht ist ein zentraler Bestandteil der Rechtsdurchsetzung im Datenschutz. Unterbleibt dies, drohen empfindliche Bußgelder.

Der HmbBfDI hat im Berichtszeitraum ein Bußgeld gegen ein Handelsunternehmen im niedrigen sechsstelligen Bereich verhängt, weil dieses wiederholt und über einen längeren Zeitraum Anträge betroffener Personen auf Auskunft, Löschung und Widerspruch gegen Direktwerbung (Rechte der betroffenen Personen gem. Artt. 15, 17 und 21 DSGVO) nicht fristgerecht innerhalb eines Monats beantwortet hatte. Über die Gründe für die Verzögerung wurden die Antragsteller:innen nicht informiert. Die beantragten Informationen wurden regelmäßig erst nach Aufforderung durch den HmbBfDI im Verwaltungsverfahren zur Verfügung gestellt.

Die betroffenen Personen hatten zuvor postalische Werbung des Unternehmens erhalten, die durch beauftragte Dienstleistungsunternehmen versendet wurde. Die Namen und Adressen der Empfänger:innen waren dabei nicht beim Handelsunternehmen selbst gespeichert, sondern nur bei den beauftragten Dienstleistungsunternehmen.

Unternehmen sind grundsätzlich dazu verpflichtet, ihre internen Prozesse so auszugestalten und anzupassen, dass geltend gemachte Betroffenenrechte nach der DSGVO fristgerecht bearbeitet und beantwortet werden können. Das Nichtvorliegen von personenbezogenen Daten entbindet die Verantwortlichen nicht von der Pflicht, auf

entsprechende Anträge fristgerecht zu reagieren. Auch für den Fall, dass bei einem Unternehmen keine Daten der Antragssteller:innen verarbeitet werden, ist diesen auf ihre Anträge hin eine sogenannte Negativauskunft zu erteilen – also zu bestätigen, dass keine personenbezogenen Daten der Antragsteller:innen verarbeitet werden. Diese Verpflichtung dient der Transparenz und dem Schutz der Rechte der betroffenen Personen: Nur so kann sichergestellt werden, dass eine Auskunft, eine Löschung von personenbezogenen Daten oder die Umsetzung eines Werbewiderspruchs von den Verantwortlichen nicht einfach verweigert oder unterlassen wurde.

Die Erteilung einer Negativauskunft ist zudem von besonderer Bedeutung, damit die betroffenen Personen erfahren, bei wem ihre Daten tatsächlich verarbeitet werden. Nur wenn sie wissen, dass das angefragte Unternehmen keine Daten von ihnen verarbeitet, können sie gezielt bei anderen Stellen – etwa bei den Dienstleistungsunternehmen, die die Werbung versendet haben – ihre Rechte auf Auskunft, Löschung oder Widerspruch wahrnehmen. Die Negativauskunft trägt somit entscheidend dazu bei, Transparenz über Datenverarbeitungsketten herzustellen und die effektive Durchsetzung der Betroffenenrechte zu ermöglichen.

Das Handelsunternehmen hat die Verstöße gegenüber dem HmbBfDI eingeräumt, seine internen Prozesse bereits während des Bußgeldverfahrens deutlich verbessert und kooperativ mit der Aufsichtsbehörde zusammengearbeitet. Diese Umstände wurden bei der Bemessung des Bußgeldes mildernd berücksichtigt. Der Bußgeldbescheid wurde von dem Unternehmen akzeptiert.

GRENZÜBERSCHREITENDE THEMEN VI.

Grenzüberschreitende Themen

1. Datenschutzniveau in den USA

In den USA sind derzeit tiefgreifende Veränderungen der politischen Landschaft zu beobachten. Inwieweit die Vereinigten Staaten auf Dauer ein vertrauenswürdiges Empfängerland für personenbezogene Daten europäischer Bürger:innen sein werden, ist daher kaum absehbar. Derzeit sind Datentransfers dorthin weiter rechtlich möglich. Stellen, die US-Dienstleister einsetzen, ist jedoch zu raten, die Lage kontinuierlich zu beobachten und Alternativen in den Blick zu nehmen.

Für die USA besteht ein sogenannter Angemessenheitsbeschluss der EU-Kommission. Dies bedeutet, dass Datenübermittlungen in die USA möglich sind, sofern eine solche Weitergabe innerhalb der Europäischen Union auch zulässig wäre. Auf den Beschluss können sich alle Stellen berufen, die personenbezogene Daten an einen Empfänger in den Vereinigten Staaten transferieren, der sich bestimmten Garantien nach dem Data Privacy Framework unterworfen hat. Welche Unternehmen und Dienstleister dies sind, kann auf der Internetseite www.dataprivacyframework.gov abgefragt werden. Die EU-Kommission hat ihren Angemessenheitsbeschluss auf Grundlage der Executive Order 14086 erlassen. Das US-Gesetz aus dem Jahr 2022 verfolgt das Ziel, geheimdienstliche Auswertungen auf ein verhältnismäßiges Maß zu reduzieren und einen ausreichenden Rechtsschutz herzustellen. Die Einschränkungen der nachrichtendienstlichen Aktivitäten waren seinerzeit als Antwort auf die Schrems-II-Entscheidung des Europäischen Gerichtshofs aus dem Jahr 2020 eingeführt worden. Das Gericht hatte darin eine anlasslose staatliche Massenüberwachung in den Vereinigten Staaten erkannt.

Seit dem Regierungswechsel im Januar 2025 sind in den USA weitreichende politische Veränderungen zu beobachten. Die Lage ist auch in Bezug auf die Regulierung der Digitalwirtschaft und die Sicherheits-

strategie volatil, wobei kaum klare Zielrichtungen erkennbar sind. Die Executive Order 14086 ist weiterhin gültig (Stand: Dezember 2025). Damit unterliegen die US-Geheimdienste weiterhin den von der Vorgängerregierung eingeführten prozeduralen und inhaltlichen Beschränkungen in Bezug auf die Massenauswertung der Daten europäischer Bürger:innen. Auch ein Rechtsschutzmechanismus ist weiterhin zu gewährleisten. Ob an der Executive Order längerfristig festgehalten wird, ist jedoch unsicher. Sie beruht auf einer Einigung des vorherigen US-Präsidenten Biden mit der EU-Kommission. Eine Annullierung ist voraussetzungsfrei und ohne Umsetzungsfrist jederzeit durch den Nachfolger möglich. Der aktuelle US-Präsident hat direkt zu seinem Amtsantritt einen Großteil der Präsidialanordnungen seines Vorgängers aufgehoben. Alle Executive Orders, die die nationale Sicherheit betreffen, hat er hingegen zunächst unangetastet gelassen und angekündigt, sie einer 45-tägigen Überprüfung zu unterziehen. Auch nach Ablauf dieser Prüffrist wurde die Executive Order 14086 nicht aufgehoben. Im November 2025 hat der Präsident angekündigt, alle Rechtsakte aufzuheben, die sein Vorgänger mittels des sogenannten Autopen hat unterschreiben lassen. Ob die EO 14086 zu dieser Gruppe gehört und ob die Ankündigung tatsächlich umgesetzt werden wird, ist unklar.

Sollte die EO 14086 künftig annulliert werden, würde dies die Wirksamkeit des Angemessenheitsbeschlusses nicht unmittelbar berühren. Es handelt sich um einen einseitigen Rechtsakt der Europäischen Union. In regelmäßigen Abständen von zwei Jahren überprüft die EU-Kommission zu allen Angemessenheitsbeschlüssen, ob das darin festgestellte angemessene Datenschutzniveau im Zielland weiterhin besteht. Im Fall tiefgreifender Änderungen der Rechtslage in den USA ist anzunehmen, dass die EU-Kommission das Review vorziehen würde. Solange der Angemessenheitsbeschluss aber nicht zurückgenommen oder auf andere Weise annulliert wird, handelt es sich um verbindliches Recht, auf das sich datenexportierende Stellen gegenüber Datenschutzbehörden und Gerichten berufen können.

Bei der Überprüfung wird zu beachten sein, dass der in der EO 14086 etablierte Rechtsschutz derzeit bei realistischer Betrachtung nicht gewährleistet werden kann. Mit dem Regierungswechsel wurden die von der Demokratischen Partei nominierten Mitglieder des Privacy and Civil Liberties Oversight Board (PCLOB) ihres Amtes enthoben. Eine Nachbesetzung ist noch nicht erfolgt. Das Aufsichtsgremium über den Datenschutz bei den US-Geheimdiensten ist damit derzeit nicht beschlussfähig. Eine Absetzung von Personal in derartigen Gremien ist nach einem Regierungswechsel in den USA relativ üblich und bei einer zeitnahen Nachbesetzung auch unkritisch. Je länger die Vakanz andauert, desto problematischer ist aber der nicht gewährleistete Rechtsschutz für das Datenschutzniveau.

Der Angemessenheitsbeschluss kann auch durch den Europäischen Gerichtshof für ungültig erklärt werden. So erging es bereits den beiden Vorgängerregelungen zu den USA. Das Data Privacy Framework hat allerdings bereits einen ersten Härtetest vor Gericht bestanden. Das Europäische Gericht (EuG) hat am 03. September 2025 eine Nichtigkeitsklage des französischen Bürgerrechtlers Philippe Latombe abgewiesen. Das Gericht erster Instanz hat dabei ausdrücklich nicht die faktischen Entwicklungen des Jahres 2025 zum Gegenstand seiner Betrachtung gemacht, sondern ausschließlich die geltenden Rechtsakte beurteilt. Sein Ergebnis deckt sich mit der Einschätzung des HmbBfDI (vgl. 31. TB 2022, Kap. V 4): Nach der Papierlage hat das Datenschutzniveau in den USA große Fortschritte im Vergleich zu der vorherigen Situation gemacht. Die wesentlichen Kritikpunkte des EuGH aus den Schrems-Entscheidungen wurden aufgegriffen und mit tragfähigen rechtlichen Lösungen beantwortet. Entscheidend für den Bestand des Angemessenheitsbeschlusses muss jedoch sein, wie die rechtlichen Anforderungen in der praktischen Umsetzung gelebt werden. Das EuG spielt den Ball der Kommission zu und betont deren Aufgabe eines kontinuierlichen Monitorings. Der Kläger hat Rechtsmittel gegen das Urteil eingelegt. Daher steht demnächst eine erneute Überprüfung durch den EuGH an, die auch die Annullierung des Angemessenheitsbeschlusses zum Ergebnis haben kann.

Auch wenn Übermittlungen an Empfänger, die dem Data Privacy Framework unterliegen, derzeit rechtlich nicht zu beanstanden sind, müssen Datenexporteure die politischen Entwicklungen im Blick behalten. Eine Veränderung der Rechtslage kann jederzeit kurzfristig eintreten. Auch über die rechtlichen Anforderungen hinaus ist eine Strategie der digitalen Souveränität ratsam. Die US-Regierung hat Sanktionen gegen Beschäftigte der NGO Hate Aid verhängt, die von der Bundesnetzagentur als Trusted Flagger nach dem DSA ernannt ist. Dieser Vorfall verdeutlicht eine mittlerweile tiefe Kluft zwischen den Rechtsverständnissen der USA und der EU über den digitalen Raum. Vor diesem Hintergrund werden datenverarbeitende Stellen in der EU der Frage nicht ausweichen können, ob es mittelfristig tragfähig sein wird, Kund:innen- und Beschäftigtendaten sowie Geschäftsgeheimnisse Dienstleistern aus den USA anzuvertrauen.

2. Consent or Pay-Modelle

Der Europäische Datenschutzausschuss hat im April 2024 eine Stellungnahme zu „Consent or Pay"-Modellen großer Online-Plattformen veröffentlicht. Im Mai 2024 wurde zusätzlich ein Mandat für die Erarbeitung umfassender Leitlinien beschlossen, die künftig für alle Anbieter solcher Modelle gelten sollen.

Entsprechend dem Beschluss „Bewertung von Pur-Abo-Modellen auf Websites" der DSK von März 2023 hält der HmbBfDI „Pur-Abo"-Modelle, auch genannt „Consent or Pay"-Modelle, auf Webseiten und in Apps unter bestimmten Voraussetzungen für datenschutzrechtlich zulässig. Diese Modelle zeichnen sich dadurch aus, dass Nutzer:innen wählen, ob sie ein kostenfreies Angebot mit personalisierter Werbung und Tracking oder ein kostenpflichtiges Angebot ohne Tracking und Werbung nutzen möchten.

Entscheidend für die Zulässigkeit dieser Modelle ist, dass die Einwilligung in die Verarbeitung personenbezogener Daten freiwillig, informiert und eindeutig erfolgt, wie es insbesondere Art. 4 Nr. 11 und Art. 7 DSGVO vorsehen. Die Freiwilligkeit ist hier gegeben, wenn eine echte Wahlmöglichkeit zwischen gleichwertigen Alternativen besteht und das Entgelt für das werbefreie Angebot marktüblich und nicht offensichtlich unverhältnismäßig hoch ist. Zudem dürfen keine überragenden Macht- oder Verhandlungsungleichgewichte vorliegen, wie sie etwa im Verhältnis zwischen Bürger:innen und Behörden bestehen. Die Nutzer:innen müssen klar und verständlich über die Zwecke der Datenverarbeitung, die Möglichkeit des Widerrufs und weitere relevante Aspekte informiert werden. Zudem muss die Einwilligung „granular" gestaltet sein, Nutzer:innen müssen also die Möglichkeit haben, gesondert in verschiedene Zwecke der Datenverarbeitung einzuwilligen und einzelne Verarbeitungszwecke auch abzulehnen. Die Einwilligung darf sich also nicht pauschal auf mehrere unterschiedliche Zwecke erstrecken.

Im April 2024 veröffentlichte der Europäische Datenschutzausschuss (EDSA) die „Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms". Diese Stellungnahme bezieht sich ausschließlich auf große Online-Plattformen und deren Geschäftsmodelle, bei denen Nutzer:innen die Wahl zwischen einer kostenlosen Nutzung mit Einwilligung in die Verarbeitung personenbezogener Daten für verhaltensbasierte Werbung oder einer kostenpflichtigen, einwilligungsfreien Nutzung haben. Der EDSA stellte klar, dass solche „Consent or Pay"-Modelle in der Regel nicht den Anforderungen an eine freiwillige und informierte Einwilligung nach der DSGVO genügen, insbesondere wenn Nutzer:innen Nachteile erleiden, weil sie ohne die Erteilung einer Einwilligung vom Dienst ausgeschlossen werden, ohne dass ihnen eine gleichwertige Alternative angeboten wird.

Im Anschluss an die Veröffentlichung der Stellungnahme beschloss der EDSA auf seiner Plenarsitzung im Mai 2024 ein weiteres Mandat zur Erarbeitung von Leitlinien für „Consent or Pay"-Modelle. Ziel

dieser Leitlinien ist es, die Anforderungen an die Einwilligung und die Ausgestaltung entsprechender Abomodelle für alle Anbieter – unabhängig von deren Größe oder Marktstellung – zu konkretisieren und zu vereinheitlichen. Die Leitlinien sollen über die bisherigen Aussagen der Stellungnahme hinausgehen und auch Aspekte berücksichtigen, die für kleinere und regionale Anbieter relevant sind. Die Leitlinien des EDSA befinden sich noch in der Entwicklung. Mit ihrer Veröffentlichung ist im Jahr 2026 zu rechnen.

Der HmbBfDI sieht in der Entwicklung dieser Leitlinien die Chance, die bei Anbietern in seiner Zuständigkeit erprobten Abomodelle auf Grundlage des Beschlusses der DSK auf europäischer Ebene zu verankern. Die deutschen Aufsichtsbehörden setzen sich dafür ein, dass diese Grundsätze auch in den künftigen EDSA-Leitlinien Berücksichtigung finden.

3. Neue EU-Verordnung: Strengere Regeln für politische Werbung

Seit dem 10. Oktober 2025 gilt die EU-Verordnung (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung (TTPW-VO). Die Datenschutzbehörden sind für die Aufsicht über diejenigen Vorschriften der Verordnung zuständig, die Targeting- und Anzeigenschaltungsverfahren im Zusammenhang mit politischer Werbung im Internet betreffen.

Parteien und Politiker:innen nutzen zunehmend digitale Medien wie soziale Netzwerke und Online-Plattformen, um Wähler zu adressieren. Politische Botschaften lassen sich mithilfe dort eingesetzter Targeting- und Anzeigenschaltungsverfahren passgenau ausspielen, beispielsweise durch personalisierte Wahlkampagnen. Targetingverfahren sind nach der Legaldefinition in Art. 3 Nr. 11 TTPW-VO Verfahren, die eingesetzt werden, um, auf der Grundlage der Verarbeitung perso-

nenbezogener Daten, eine politische Anzeige nur an eine bestimmte Person oder Personengruppe zu richten oder diese auszuschließen. Anzeigenschaltungsverfahren sind nach der Legaldefinition in Art. 3 Nr. 12 TTPW-VO Optimierungsverfahren, die eingesetzt werden, um die Verbreitung, die Reichweite oder die Sichtbarkeit einer politischen Anzeige auf der Grundlage der automatisierten Verarbeitung personenbezogener Daten zu erhöhen, und die es ermöglichen, die politische Anzeige nur einer bestimmten Person oder Personengruppe zuzustellen.

Die TTPW-VO enthält in Art. 18 und 19 konkrete Vorgaben für das Targeting und die Anzeigenschaltung im Zusammenhang mit politischer Werbung im Internet. Art. 18 TTPW-VO bestimmt die Voraussetzungen für eine zulässige Verarbeitung personenbezogener Daten zu Zwecken des Targetings und der Anzeigenschaltung. Unter anderem ist Bedingung, dass die betroffene Person ihre ausdrückliche Einwilligung in die gesonderte Verarbeitung personenbezogener Daten für Zwecke der politischen Werbung erteilt hat (Art. 18 Abs. 1 lit. b) TTPW-VO). Art. 19 TTPW-VO enthält Informationspflichten, die die Verantwortlichen beim Einsatz von Targeting- oder Anzeigenschaltungsverfahren im Zusammenhang mit politischer Werbung im Internet gegenüber der betroffenen Person zu erfüllen haben.

Als unmittelbar geltendes Unionsrecht muss die TTPW-VO nicht in nationales Recht umgesetzt werden. Um den Vorgaben der Verordnung vollständig nachzukommen, sind von den einzelnen Mitgliedstaaten gleichwohl gesetzliche Durchführungsbestimmungen zu erlassen, die die TTPW-VO ergänzen. In Deutschland trägt das Politische-Werbung-Transparenz-Gesetz (PWTG) diesem Erfordernis Rechnung, das sich aktuell im Abstimmungsverfahren befindet. Das Gesetz wird insbesondere Regelungen zu den Zuständigkeiten der deutschen Behörden sowie zur nationalen Ausgestaltung der Ordnungswidrigkeitsbestimmungen treffen.

Die Zuständigkeiten der Datenschutzbehörden ergeben sich weitestgehend bereits unmittelbar aus der TTPW-VO: Den Datenschutzbehörden obliegt gemäß Art. 22 Abs. 1 S. 1 TTPW-VO die Aufsicht in Bezug auf Art. 18 und Art. 19 TTPW-VO. Ihnen stehen die Untersuchungs- und Abhilfebefugnisse gemäß Art. 58 DSGVO i.V.m. Art. 22 Abs. 1 S. 2 TTPW-VO zu; bei Verstößen gegen Art. 18 und Art. 19 TTPW-VO dürfen die Datenschutzbehörden gemäß Art. 25 Abs. 6 TTPW-VO Bußgelder verhängen.

In Art. 24 sieht die TTPW-VO ein eigenes Beschwerderecht vor, nach dem Personen oder Einrichtungen mögliche Verstöße gegen die Verordnung den Aufsichtsbehörden mitteilen können. Für Verantwortliche mit Sitz in Hamburg wie beispielsweise Politiker:innen, Werbedienstleistende oder Online-Plattformen ist der HmbBfDI zuständig und nimmt entsprechende Beschwerden entgegen.

Art. 22 Abs. 2 TTPW-VO bestimmt, dass der Europäische Datenschutzausschuss (EDSA) Leitlinien ausarbeitet, mit denen die Datenschutzbehörden bei der Bewertung der Frage unterstützt werden sollen, ob die Anforderungen der Verordnung eingehalten werden. Neben Vertretern der Datenschutzbehörden aus Polen, Frankreich, Italien und den Niederlanden ist der HmbBfDI an der Erarbeitung dieser Leitlinien beteiligt. Mit ihrer Veröffentlichung ist im Jahr 2026 zu rechnen.

Gezielte politische Werbung in Verbindung mit der Verarbeitung personenbezogener Daten war auch vor Inkrafttreten der TTPW-VO nur eingeschränkt zulässig. Wichtige Vorschriften, die auch weiterhin Bestand haben, finden sich in der DSGVO sowie im Digital Services Act (DSA). Mit der TTPW-VO hat der europäische Gesetzgeber weitere Schutzvorkehrungen im besonders sensiblen Bereich der politischen Werbung geschaffen, die den bestehenden Regelungen nun ergänzend hinzutreten.

4. Meta KI Training – Datenschutz im Eilverfahren vor dem OLG Köln

Im Jahr 2025 wurde der HmbBfDI in einem richtungsweisenden Eilverfahren vor dem Oberlandesgericht Köln als sachverständige Stelle nach § 12 Unterlassungsklagegesetz (UKlagG) angehört. Im Ergebnis wurden die vorgetragenen datenschutzrechtlichen Bedenken aber nicht berücksichtigt. Meta konnte im Mai 2025 sein KI-Training beginnen.

Im Frühjahr und Sommer 2025 standen die geplanten Datenverarbeitungen von Meta Platforms Ireland Limited (Meta) im Fokus der datenschutz- und verbraucherschutzrechtlichen Diskussionen. Meta hatte im April 2025 angekündigt, ab dem 27. Mai personenbezogene Daten volljähriger Nutzer:innen von Facebook und Instagram, die öffentlich eingestellt wurden, für das Training und die Verbesserung eigener Systeme künstlicher Intelligenz (KI) zu verwenden. Die Verarbeitung sollte insbesondere Profilbilder, Aktivitäten in öffentlichen Gruppen, Kommentare, Bewertungen und weitere öffentlich geteilte Inhalte umfassen und stützte sich auf das berechtigte Interesse nach Art. 6 Abs. 1 f DSGVO. Nutzenden wurde vorab eine Widerspruchsmöglichkeit eingeräumt.

Die Ankündigung löste europaweit erhebliche Bedenken hinsichtlich der Rechtmäßigkeit und der Auswirkungen auf die Grundrechte der Betroffenen aus. Vor Inkrafttreten der neuen Datenschutzrichtlinien von Meta informierte der HmbBfDI die Betroffenen in Deutschland ausführlich über ihre Möglichkeit, gegen diese Datenverarbeitung Widerspruch einzulegen. Zudem bereitete der HmbBfDI mit einem Anhörungsschreiben an Meta ein mögliches Dringlichkeitsverfahren gemäß Art. 66 Abs. 1 DSGVO vor, um die Situation zu prüfen. Zu diesem Zeitpunkt schienen der HmbBfDI und die zuständige irische Datenschutzaufsichtsbehörde (IDPC) zunächst einig, dass sogenannte „historische" Daten – also Nutzerbeiträge, die vor dem Start

des KI-Trainings oder zumindest vor der ersten Ankündigung eines solchen Trainings im Mai 2024 veröffentlicht wurden – nicht auf Grundlage eines berechtigten Interesses von Meta für das KI-Training verwendet werden dürfen, da die Nutzer dies nicht vorhersehen konnten. Die Vorhersehbarkeit der Zweckänderung ist ein wichtiger Aspekt bei der Abwägung der Interessen. Und kein Facebook-Nutzer konnte 2015 auch nur ahnen, dass seine Posts 10 Jahre später zum Training eines Open-Source-KI-Modells genutzt werden. Nach einigen kleineren Zugeständnissen von Meta bewertete jedoch die IDPC wenige Tage vor Trainingsbeginn überraschend das berechtigte Interesse als hier zulässige Rechtsgrundlage und gab Meta lediglich Empfehlungen hinsichtlich der möglichen Auswirkungen auf die Datenschutzrechte von Personen. Sie kündigte zudem eine umfassende Prüfung und einen Bericht zum KI-Training bei Meta zum Oktober 2025 an. Dieser Bericht liegt bisher nicht vor.

Quasi zeitgleich fand ein von der Verbraucherzentrale NRW eingeleitetes Unterlassungsklageverfahren vor dem OLG Köln statt, mit dem Ziel, durch einen Eilantrag auf Erlass einer einstweiligen Verfügung Meta die geplante Nutzung von öffentlich zugänglichen Nutzerdaten für das Training seiner KI-Modelle zu untersagen. In der mündlichen Verhandlung am 22. Mai 2025 erläuterte der HmbBfDI die Anforderungen an die datenschutzrechtliche Zulässigkeit des KI-Trainings mit personenbezogenen Daten. Er bestätigte, dass die Verarbeitung auf Grundlage eines berechtigten Interesses nach Art. 6 Abs. 1 Buchstabe f DSGVO grundsätzlich möglich sei, sofern die Interessen der Betroffenen durch wirksame Schutzmaßnahmen gewahrt werden. Der HmbBfDI betonte dabei die Bedeutung eines effektiven Widerspruchsrechts und einer transparenten Information der Nutzer:innen, jedoch schränkte er deren Wirksamkeit in Bezug auf bestimmte Datenkategorien (Art. 9 DSGVO) ein. Die Einschätzung des HmbBfDI wurde zwar im Urteil des Oberlandesgerichts Köln gewürdigt, allerdings folgte das Gericht nicht der Argumentation des HmbBfDI insbesondere in Bezug auf die historischen Daten, deren Verwendung zum KI-Training der HmbBfDI nicht von berechtigten Interessen umfasst sah. Stattdessen schloss sich das

Gericht der Einschätzung der IDPC an, die am Vortag der Verhandlung veröffentlicht worden war.

Nachdem das OLG Köln den Antrag rechtskräftig abgewiesen hatte (AZ 15 UKl 2/25 vom 23. Mai 2025) und die nach der DSGVO zuständige IDPC die Aufnahme des KI-Trainings durch Meta öffentlich für unproblematisch hielt, führte der HmbBfDI das Dringlichkeitsverfahren – nach Abstimmung mit den deutschen Aufsichtsbehörden - nicht weiter, vor allem mit Blick auf eine einheitliche Bewertung des Sachverhalts auf EU-Ebene.

Zudem wurde in diesem Verfahren erstmals die Anwendbarkeit des Gesetzes über digitale Märkte (Digital Markets Act – DMA) geprüft. Das Gericht hatte über die Frage zu entscheiden, ob das bloße Einbringen von de-identifizierten und zerlegten Daten aus verschiedenen Plattformdiensten in einen KI-Trainingsdatensatz als „Zusammenführung" im Sinne des Art. 5 Abs. 2 DMA zu bewerten ist. Dies hätte zur Folge, dass Meta als sogenannter Torwächter eine gezielte Verknüpfung der personenbezogenen Daten nur auf eine Einwilligung der Nutzer hätte stützen können. Das Gericht entschied, dass in diesem Fall keine gezielte Verknüpfung personenbezogener Daten derselben Person aus unterschiedlichen Diensten erfolge. Ob diese Einschätzung in einem Hauptsacheverfahren Bestand haben wird, bei dem beispielsweise eine Stellungnahme der EU-Kommission zur Auslegung des DMA eingeholt werden kann, bleibt abzuwarten.

Auch in einem weiteren Verfahren vor dem Oberlandesgericht Schleswig im August 2025 wurde der HmbBfDI angehört. Geklagt hatte eine niederländische Verbraucherschutzorganisation. Die Einbindung des HmbBfDI als sachverständige Stelle trug dazu bei, die komplexen datenschutzrechtlichen Fragestellungen für das Gericht und die Verfahrensbeteiligten nachvollziehbar darzustellen und die Interessen der Betroffenen angemessen zu berücksichtigen. Das Gericht wies letztendlich den Antrag auf einstweilige Verfügung vor allem mit der Begründung zurück, dass keine ausreichende Dringlichkeit für den Erlass einer sofortigen gerichtlichen Maßnahme vorlag, da das Training

bereits begonnen hatte, der Antrag also zu spät kam. Es ließ jedoch in der mündlichen Verhandlung deutlich erkennen, dass es die Einschätzung des OLG Köln in Bezug auf die Rechtsgrundlage nach der DSGVO nur bedingt teilt, was jedoch in einem Hauptsacheverfahren zu entscheiden wäre.

Insgesamt bleibt festzustellen, dass Eilverfahren nach dem Unterlassungsklagerecht nur bedingt geeignet sind, komplexe datenschutzrechtliche Sachverhalte zu klären, auch wenn die Einbeziehung des HmbBfDI durch die Gerichte in die Verfahren positiv zu bewerten ist. Zum einen können die datenschutzrechtlichen Fragen kaum vertieft erörtert werden, zum anderen überlagern andere Aspekte wie die Eilbedürftigkeit die materiellrechtlichen Aspekte. Im Ergebnis entstand dadurch eine Scheinlegitimität einer Datenverarbeitung, an deren Rechtsmäßigkeit jedenfalls in diesem Umfang unter Fachleuten erhebliche Zweifel bestehen.

Die Vertröstung auf spätere Erfolge in der Hauptverhandlung oder vor dem EuGH nutzen in diesem Fall wenig. Die Daten von Millionen Nutzer:innen sind unwiderruflich in das KI-Modell geflossen.

5. Cross-regulatory Interplay and Cooperation Expert Subgroup (CIC ESG)

Die europäische Datenschutzlandschaft ist zunehmend von einer engen Zusammenarbeit zwischen verschiedenen Regulierungsbereichen geprägt. Der HmbBfDI bringt sich aktiv in die Arbeit der relevanten Expertengruppen ein und gestaltet die Diskussionen zur Schnittstelle zwischen Datenschutz, Wettbewerbs- und Verbraucherschutzrecht und zur Regulierung von Künstlicher Intelligenz (KI) mit.

Im Berichtsjahr hat sich der HmbBfDI intensiv an den europäischen Abstimmungsprozessen beteiligt, die darauf abzielen, die Zusammen-

arbeit zwischen Datenschutzaufsichtsbehörden und anderen Regulierungsinstanzen zu stärken. Die neu etablierte Cross-regulatory Interplay and Cooperation Expert Subgroup (CIC ESG) des Europäischen Datenschutzausschusses (EDSA) widmet sich der Frage, wie Datenschutz, Wettbewerbsrecht und Verbraucherschutz im digitalen Raum besser verzahnt werden können. Ziel ist es, Überschneidungen und Synergien zwischen den verschiedenen Rechtsbereichen zu identifizieren und die Zusammenarbeit der jeweils zuständigen Behörden zu fördern. Der HmbBfDI nimmt dabei die Rolle der Ländervertretung für die Datenschutzkonferenz (DSK) wahr und bringt sich aktiv in die Erarbeitung von Leitlinien und Positionspapieren ein.

In der CIC ESG werden insbesondere Fragen der regulativen Überschneidungen und der aufsichtsbehördlichen Schnittstellen zwischen Datenschutz und Wettbewerbsrecht behandelt. Dabei steht die Subgroup in einem engen Kontakt zu der Europäischen Kommission und sucht aktiv nach Austauschformaten mit anderen Netzwerken, etwa mit dem Europäischen Wettbewerbsnetz (European Competition Network = ECN). Dabei bringt der HmbBfDI seine Erfahrungen aus der Praxis ein, etwa im Umgang mit marktmächtigen Plattformen und deren datengetriebenen Geschäftsmodellen, die er beispielsweise bei dem Verfahren des Bundeskartellamts gegen Meta (Az. B6-22-16) bereits sammeln und mit anderen Behörden teilen durfte. Die CIC ESG hat im Berichtsjahr zudem an der Entwicklung von Empfehlungen zur Zusammenarbeit zwischen Datenschutzaufsicht und Verbraucherbehörden gearbeitet, um einheitliche Standards für den Informationsaustausch und die gemeinsame Bearbeitung von Fällen zu schaffen.

Ein weiterer Schwerpunkt der europäischen Zusammenarbeit lag im Berichtsjahr auf der Arbeit der hochrangigen Gruppe (High Level Group, HLG) nach dem Gesetz über digitale Märkte (Digital Markets Act, DMA) sowie ihrer Subgroups. Die HLG berät die Europäische Kommission bei der Umsetzung und Durchsetzung des DMA, sorgt für eine einheitliche Regulierung mit anderen Gesetzen, gibt Expertise zu Marktuntersuchungen bei neuen Diensten (wie KI) und hilft, den

DMA zukunftssicher zu machen, indem sie eine konsistente Regulierungsstrategie fördert und Empfehlungen ausspricht. Geregelt ist sie in Art. 40 DMA und wird von der EU-Kommission geleitet. Sie setzt sich aus fünf Netzwerken zusammen, dem Gremium europäischer Regulierungsstellen für elektronische Kommunikation, dem EDSA, dem Europäischen Wettbewerbsnetz, dem Netzwerk für die Zusammenarbeit im Verbraucherschutz und der Gruppe europäischer Regulierungsstellen für audiovisuelle Mediendienste, die die EU-Kommission beraten und Fachexpertise bereitstellen. Der HmbBfDI ist über den EDSA auf mehreren Ebenen in die Arbeit der HLG und ihrer Subgroups eingebunden und hat sich im Berichtsjahr insbesondere an den Diskussionen zur Regulierung von Künstlicher Intelligenz beteiligt. Vorbereitend zu den Sitzungen der HLG sowie ihrer Subgroups wird regelmäßig die CIC ESG des EDSA einberufen. Dort werden zunächst eine gemeinsame Position des EDSA entwickelt und entsprechende Beiträge konsolidiert, die anschließend in die Sitzungen der Gremien durch nominierte Vertreter:innen getragen werden.

Im Rahmen der HLG wurde ein gemeinsames Papier zur Regulierung von KI verabschiedet (https://digital-markets-act.ec.europa.eu/fifth-meeting-digital-markets-act-high-level-group-2025-12-12_en), das die Schnittstellen zwischen Datenschutz, Wettbewerbsrecht, Verbraucher- und Medienrecht im Kontext von KI-Systemen analysiert. Das Dokument hebt hervor, dass KI-Technologien zunehmend in die Ökosysteme marktmächtiger Plattformen integriert werden und dadurch neue Herausforderungen für den Datenschutz und die Wettbewerbsaufsicht entstehen. Der HmbBfDI hat sich in die Diskussionen eingebracht und auf die Bedeutung einer kohärenten und abgestimmten Regulierung hingewiesen, um sowohl die Rechte der Nutzerinnen und Nutzer zu schützen als auch Innovationen zu ermöglichen. Das verabschiedete Papier betont die Notwendigkeit einer verstärkten Zusammenarbeit zwischen den zuständigen Behörden, um einheitliche Standards für Transparenz, Fairness und den Zugang zu Daten zu schaffen. Es werden konkrete Ansatzpunkte für die gemeinsame Bearbeitung von Fällen und den Informationsaustausch zwischen Datenschutz-, Wettbewerbs- und Verbraucherbehörden

vorgeschlagen. Der HmbBfDI unterstützt diese Entwicklung und setzt sich dafür ein, dass die Erfahrungen aus Hamburg in die europäischen Prozesse einfließen.

Insgesamt zeigt sich, dass die behördenübergreifende Zusammenarbeit auf europäischer Ebene weiter an Bedeutung gewinnt. Der HmbBfDI sieht darin einen wichtigen Beitrag zur Stärkung des Datenschutzes im digitalen Raum und zur Bewältigung der Herausforderungen, die sich aus der zunehmenden Verflechtung von Datenschutz, Wettbewerbs- und Verbraucherrecht ergeben. Die aktive Mitwirkung in den relevanten Expertengruppen und Gremien ermöglicht es dem HmbBfDI, die Interessen der Bürgerinnen und Bürger sowie der öffentlichen Verwaltung wirkungsvoll zu vertreten und die Entwicklung einheitlicher europäischer Standards voranzutreiben.

BERATUNGEN ÖFFENTLICHER STELLEN VII.

Beratungen öffentlicher Stellen

1. Elektronische Bußgeldakten in den Bezirksämtern

Der HmbBfDI berät und begleitet die Bezirksämter bei der Einführung eines Systems für die elektronische Aktenführung in Bußgeldsachen. Der Betrieb des Produktes OWi21 auf einem Einheitsmandanten schafft datenschutzrechtliche Herausforderungen, die sich aus dem Zusammenspiel der Vorschriften aus dem Gesetz über Ordnungswidrigkeiten (OWiG), der Strafprozessordnung (StPO) sowie der JI-Richtlinie ergeben.

Das Fachverfahren „OWi21“ ist eine Software, mit der ausschließlich Verfahren über Ordnungswidrigkeiten bearbeitet werden können. Zweck der Verarbeitung ist eine digitale und rechtskonforme Abwicklung von OWi-Fällen.

Hintergrund der beabsichtigten Einführung einer elektronischen Aktenführung ist eine gesetzliche Vorgabe. Durch das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 wurde zum 1. Januar 2026 zunächst die verbindliche elektronische Aktenführung geplant. Nach aktuellem Sachstand besteht jedoch nach dem Datum das Risiko, die Digitalisierung in den Verfahren nicht hinreichend gewährleisten zu können. Um mögliche negative Folgen für die Funktionsfähigkeit der Durchführung von Verfahren nach dem Ordnungswidrigkeitengesetz zu vermeiden, wurde in § 110a Absatz 1d OWiG die sogenannte „Opt-Out“-Regelung aufgenommen, die besagt, dass über den 1. Januar 2026 hinaus bis zum 1. Januar 2027 eine papiergebundene Aktenführung für Bußgeldverfahren möglich ist. Die Bezirksämter haben von der Opt-Out Regelung Gebraucht gemacht.

Ziel der Bezirksämter ist aber weiterhin die elektronische Aktenführung an den besonderen Bedarfen des Ordnungswidrigkeitenrechts entsprechend anzupassen und bei Einführung möglichst passgenau

umzusetzen. Dem HmbBfDI ist die Spannungslage zwischen Digitalisierungsdruck und rechtlichen Hürden bewusst, er möchte hier im Rahmen seiner beratenden Beteiligung Hilfestellungen geben.

Dabei stehen Fragen im Vordergrund, die sich aus der Wahl eines Einheitsmandanten für den Betrieb von OWi21 ergeben. Einheitsmandant heißt in diesem Zusammenhang, dass alle Bußgeldstellen der Hamburger Bezirksämter ihre Bußgeldverfahren aus unterschiedlichsten Rechtsbereichen auf einem Mandanten führen. Da es sich bei den jeweiligen Bußgeldstellen aber aus datenschutzrechtlicher Sicht um getrennt verantwortliche Stellen handelt, ist der Einheitsmandant in Bezug auf die Abgrenzung der einzelnen Bereiche der einzelnen Stellen durch entsprechend Trennung von Lese- und Zugriffsrechten auszugestalten. Der Schwerpunkt der Beratung liegt in der Frage, inwieweit diese Rechtetrennung dann durchbrochen werden kann, wenn z. B. bei Wiederholungstätern ein Wissens- und Datenaustausch im Rahmen des § 49b StPO vorgenommen wird, und wie dieser Austausch technisch im Mandanten umgesetzt werden kann. Das kann bei Wiederholungstätern relevant werden, weil mögliche Vortaten bei der Festlegung der Höhe einer Geldbuße unter bestimmten Umständen Berücksichtigung finden können.

Die diesbezüglichen Fragen sind Gegenstand des Beratungsprozesses, der sich im Berichtsjahr 2026 fortsetzen wird.

2. Videoüberwachung am Gebäude der Staatsanwaltschaft Hamburg

Der HmbBfDI hat die Videoüberwachung am Gebäude der Staatsanwaltschaft Hamburg überprüft. Dabei hat er darauf hingewirkt, dass die Überwachung auf einen vertretbaren Umfang begrenzt wird und für Passant:innen hinreichend erkennbar ist, dass sie einen überwachten Bereich betreten.

Die Staatsanwaltschaft Hamburg hat an ihrem neuen Hauptsitz in der Ludwig-Erhardt-Straße 11-17 („Michaelisquartier“) eine Videoüberwachung eingerichtet. Diese verfolgt den Zweck, die Ausübung des Hausrechts zu unterstützen. Übergriffe auf Beschäftigte, Sachbeschädigungen oder Sabotageakte sollen unmittelbar erkannt und dadurch entweder noch verhindert oder zumindest aufgeklärt werden können. Die Kameraüberwachung umfasst nicht nur bestimmte öffentlich zugängliche Bereiche im Inneren des Gebäudes, sondern erstreckt sich auch auf unmittelbar an die Gebäudefassade angrenzende Flächen wie etwa Teile des öffentlichen Gehwegs vor dem Gebäude. Es findet eine Echtzeit-Bildübertragung statt, wobei die Übertragungswege verschlüsselt sind. Darüber hinaus erfolgt eine Speicherung der Aufnahmen für einen eng begrenzten Zeitraum, um ggf. eine anlassbezogene Auswertung auch noch wenige Tage später zu ermöglichen.

Die Auflösung der Überwachungskameras lässt eine detailgenaue optische Wahrnehmung und damit eine Identifizierung einzelner Personen anhand ihres äußeren Erscheinungsbilds zu. Eine solche Verarbeitung von personenbezogenen Daten ist nach Art. 6 Abs. 1 DSGVO nur erlaubt, wenn sie von einer Rechtsgrundlage gedeckt ist. Für die Videoüberwachung durch öffentliche Stellen der Freien und Hansestadt Hamburg existiert eine besondere Rechtsgrundlage in § 9 HmbDSG. Gemäß § 9 Abs. 1 HmbDSG ist die Videobeobachtung nur zulässig, soweit und solange sie zur Wahrnehmung des Hausrechts oder der Aufgabenerfüllung erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der zulässige Umfang der Videoüberwachung war im Hinblick auf das Michaelisquartier alleine am Maßstab des Hausrechts zu bestimmen, weil eine Datenverarbeitung zum Zwecke der Strafverfolgung (= Aufgabenerfüllung der Staatsanwaltschaft) gem. § 2 Abs. 4 HmbDSG nicht auf das HmbDSG gestützt werden kann.

Die Staatsanwaltschaft trug zunächst vor, dass sie eine Videoüberwachung über die Grundstückgrenzen hinaus plane und weitere Flächen vor dem Gebäude erfasst werden sollen. Für das Hausrecht im Sinne von § 9 Abs. 1 Nr. 2 HmbDSG gilt jedoch prinzipiell, dass die Beob-

achtungsbefugnis des Hausrechtsinhabers an der Grundstücksgrenze endet. Lediglich ein geringfügiges Überschreiten ist nach allgemeiner Ansicht zulässig. Ausnahmsweise kann es unter Berücksichtigung der konkreten örtlichen Umstände erforderlich sein, die Videoüberwachung bis zur unmittelbaren Umgebung der Räumlichkeiten auszuweiten (vgl. Europäischer Datenschutzausschuss, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte vom 29.01.2020, Rn. 27). Voraussetzung dafür sind Szenarien, in denen die reine Überwachung des Grundstücks für einen wirksamen Schutz desselben nicht ausreicht, bspw. bei zu befürchtenden Graffiti-Attacken an der Außenfassade. Eine maßvolle Ausweitung der Überwachung über das Grundstück hinaus steht dabei ebenso unter der Voraussetzung, dass die schutzwürdigen Interessen von betroffenen Personen nicht gegenüber dem Interesse an der Videoüberwachung überwiegen.

Um die der Staatsanwaltschaft als verantwortlicher Stelle obliegende Interessenabwägung vollständig nachvollziehen zu können, hat der HmbBfDI u. a. im Rahmen eines Ortstermins am 18.06.2025 die örtlichen Gegebenheiten, die Kameraausrichtungen sowie auch die technische Ausgestaltung der Videoüberwachung eingesehen. Dabei zeigte sich, dass aus technischer Sicht keine Bedenken gegenüber der eingerichteten Überwachungsanlage bestehen, weil hohe Sicherheitsstandards implementiert wurden.

Im Rahmen der anschließenden rechtlichen Überprüfung der Interessenabwägung konnte – bezogen auf eine Ausdehnung der Videoüberwachung über das Grundstück hinaus auf den Arkadengang an der Vorderseite – kein Überwiegen schutzwürdiger Interessen von Betroffenen festgestellt werden. Auf Nachfrage wurden dem HmbBfDI von Seiten der Staatsanwaltschaft mehrere Fälle aus der jüngeren Vergangenheit geschildert, in denen sowohl die Beschäftigten als auch die vorherigen Standorte Bedrohungen und Angriffen ausgesetzt waren, die teils zu erheblichen Schäden führten. Dies zeigte, dass gegenüber der Behörde eine erhöhte Gewaltbereitschaft besteht, die deutlich über das allgemeine Lebensrisiko hinausgeht. Soweit die geschilderten Vorfälle Angriffe auf das Gebäude selbst betrafen, dürften diese

künftig gerade durch die gesamte Erfassung des Arkadenbereichs als Hauptzugang mittels Videoüberwachung schnell erkannt und wirkungsvoll dokumentiert werden können.

Demgegenüber war für den HmbBfDI keine besonders ausgeprägte Schutzbedürftigkeit von betroffenen Personen erkennbar, die hinausgeht über das gewöhnliche Interesse daran, nicht videoüberwacht zu werden. Der Arkadengang selbst weist keine Eingänge zu Wohnungen oder Geschäften auf. Er stellt ausschließlich einen Durchgangsweg dar, auf dessen Passieren lediglich diejenigen Personen zwingend angewiesen sind, die tatsächlich zur Staatsanwaltschaft Hamburg möchten. Zwar wird der Durchgang gegebenenfalls auch von Besuchern des nahegelegenen Michels als Verbindungsweg in Richtung St. Pauli oder von Gästen der seitlich im Michaelisquartier untergebrachten Gastronomie genutzt. Allerdings handelt es sich – nach Wahrnehmung des HmbBfDI – in aller Regel um eine überschaubare Anzahl an Personen und es besteht für diese auch die zumutbare Alternative des Fußwegs auf der anderen Straßenseite oder auf der Rückseite des Gebäudes, sofern der Videoüberwachung ausgewichen werden soll. Um diese Entscheidung vor Betreten des überwachten Bereichs treffen zu können, hat der HmbBfDI darauf hingewirkt, dass außen vor dem Arkadengang Hinweisschilder auf die dahinter stattfindende Videoüberwachung anzubringen waren.

Darüber hinaus war die ursprünglich von der Staatsanwaltschaft in den Blick gefasste, zusätzliche Ausdehnung der Videoüberwachung auf weitere Flächen vor dem Gebäude wegen der engen Verbindung des Hausrechts mit den Grundstücksgrenzen nicht mehr mit § 9 Abs. 1 Nr. 2 HmbDSG vereinbar. Für ein solches Vorhaben fehlte es somit an der notwendigen Rechtsgrundlage, sodass insoweit keine Kameraüberwachung eingerichtet werden durfte und auch nicht mehr eingerichtet werden soll.

3. Neue Datenübermittlungspflichten zwischen Justizkasse und Finanzbehörde

Die Justizkasse Hamburg verlangte in Vergütungsanträgen wegen einer neuen Regelung mehr persönliche Daten von den Antragsstellerinnen, um diese der Finanzbehörde mitteilen zu können. Dabei bestand das Risiko, dass private Adressen für Prozessbeteiligte einsehbar wurden. Nach Abstimmung mit der Finanzbehörde ist es nun zulässig, statt der Privatadresse eine Postfachadresse anzugeben, um die eigene Privatsphäre besser schützen zu können.

Den HmbBfDI haben im Jahr 2025 mehrere Beschwerden von Berufsbetreuer:innen und Sachverständigen erreicht, die sich darüber beklagten, dass die Justizkasse Hamburg seit Jahresbeginn verschiedene zusätzliche personenbezogene Angaben in jedem Vergütungsantrag von ihnen verlangte. Hintergrund der von der Justizkasse angeforderten umfangreicheren Daten war eine Änderung der Mitteilungsverordnung (MV). Diese von der Bundesregierung erlassene Rechtsverordnung legt fest, in welchen Fällen Mitteilungen an die Finanzbehörden durch andere Behörden zu erfolgen haben.

Seit dem 01. Januar 2025 müssen alle deutschen Behörden – und somit auch die Justizkasse – sämtliche Zahlungen an Berufsbetreuer:innen, Sachverständige, Dolmetscher:innen und Übersetzer:innen der Finanzbehörde melden (§ 2 Abs. 1 MV). Eine Ausnahme besteht nur dann, wenn die Zahlungen im Kalenderjahr voraussichtlich weniger als 3.000 Euro betragen (§ 7 Abs. 2 MV). Der genaue Umfang der zu meldenden Daten ergibt sich wiederum aus der Abgabenordnung (AO). Der zuständigen Finanzbehörde sind bei Zahlungen von der Justizkasse an natürliche Personen der Familienname, der Vorname, der Tag der Geburt, die Anschrift des bzw. der Steuerpflichtigen sowie die jeweilige Steueridentifikationsnummer mitzuteilen (§ 93c Abs. 1 Nr. 2 lit. c AO). Um dem effektiv nachkommen zu können, müssen diese Daten von der

Justizkasse erhoben werden. Werden Vergütungsanträge gestellt, ist es grundsätzlich zulässig, in diesem Rahmen auch die entsprechenden Daten abzufragen.

Aus der gewählten Vorgehensweise können sich allerdings datenschutzrechtliche Risiken für die genannten Berufsgruppen ergeben. Denn die Vergütungsanträge sind – jedenfalls dann, wenn Sie zur Akte genommen werden und nicht in ein gesondertes Vergütungsheft gelangen – von den Prozessparteien prinzipiell einsehbar. Dadurch bestand insbesondere die Gefahr der Offenlegung von Privatanschriften der oben genannten Berufsgruppen gegenüber Dritten, die diesen aufgrund des Prozessverlaufs möglicherweise nicht wohlgesonnen waren. Verhindern ließe sich dies, indem im Vergütungsantrag nicht die Privatanschrift genannt werden müsste, sondern vielmehr eine bloße Postfach-Adresse genügte. Wegen des Gesetzeswortlauts („die Anschrift des Steuerpflichtigen") war allerdings die steuerrechtliche Zulässigkeit dieser Lösung zunächst fraglich und bedurfte einer Abstimmung mit der Finanzbehörde.

Eine Anfrage des HmbBfDI bei dem Datenschutzbeauftragten der Amtsgerichte ergab, dass an diesen bereits vor einigen Monaten die Frage herangetragen worden war, ob eine Postfachadresse ausreichen könnte. Dieser hatte sich zur Klärung zuerst an die Justizkasse und im weiteren Verlauf auch an die Finanzbehörde gewandt. Auf Nachfrage des HmbBfDI bei der Finanzbehörde stellte sich heraus, dass die Prüfung der Fragestellung dort längst abgeschlossen war, jedoch versehentlich eine Rückmeldung gegenüber Justizkasse und Amtsgerichten unterblieben war. Bei der Prüfung war die Finanzbehörde zu dem Ergebnis gelangt, dass steuerrechtlich die Nennung einer Postfachadresse gegenüber den Finanzbehörden ausreichend sei. Nach Rücksprache des HmbBfDI mit dem Datenschutzbeauftragten der Amtsgerichte und der Justizkasse Hamburg wird die Alternative nun bei den Vergütungsanträgen angeboten. Die Beschwerdeführenden wurden vom HmbBfDI darüber in Kenntnis gesetzt.

4. Bildungsverlaufregister

Die geplante Einführung einer bundesweiten Bildungsverlaufsstatistik (BVStat) wirft erhebliche datenschutzrechtliche und grundrechtliche Fragen auf. Der HmbBfDI sieht in der aktuellen Diskussion große Herausforderungen für den Schutz der Privatsphäre und betont die Notwendigkeit einer kritischen Auseinandersetzung mit den Risiken und Voraussetzungen eines solchen Vorhabens.

Den HmbBfDI beschäftigte im Rahmen seiner Mitarbeit in den DSK-Arbeitskreisen „Schulen und Bildungseinrichtungen" und „Statistik" eine Anfrage der Kultusministerkonferenz (KMK), die ein bundesweites Bildungsverlaufregister schaffen möchte. Zweck einer entsprechenden Bildungsverlaufsstatistik ist, die Bildungsbiografien von Menschen in Deutschland über verschiedene Lebensphasen hinweg zu erfassen und zusammenzuführen. Die BVStat soll Daten von der frühkindlichen Bildung über die Schulzeit und in einer späteren Berufsausbildung bis hin zur Weiterbildung bündeln, um die Bildungssteuerung zu verbessern und politische Entscheidungen zu unterstützen.

Aus Sicht des HmbBfDI ist dieses Vorhaben mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Auch wenn die Daten pseudonymisiert oder anonymisiert werden sollen, besteht die Gefahr, dass einzelne Personen dennoch identifizierbar sind. Dies kann zu einer erheblichen Beeinträchtigung der Grundrechte führen. Je mehr auf die Bildung bzw. den Bildungsverlauf der einzelnen Bürger:innen bezogene Daten innerhalb des Registers verarbeitet würden, desto größer wäre die Gefahr, dass unzulässige (Teil-)Profile der Bürger:innen erstellt würden, und desto schwerer würde der Eingriff wiegen.

Die Debatte um die Einführung einer bundesweiten Bildungsverlaufsstatistik ist nicht neu. Seit mehr als zwanzig Jahren wird darüber kontrovers diskutiert. Befürworter:innen betonen die Vorteile einer

effizienteren Bildungssteuerung und einer besseren Vergleichbarkeit von Bildungsdaten. Kritische Stimmen, weisen jedoch darauf hin, dass die Risiken für die betroffenen Schüler:innen und deren Familien oft unterschätzt werden. Neben dem Schutz der Privatsphäre stehen auch die Gefahr von Stigmatisierung und die Ausweitung bürokratischer Kontrollmechanismen im Raum.

Bei der BVStat handelt es sich um ein Vorhaben hoher Komplexität, das höchste fachliche und datenschutzrechtliche Anforderungen erfüllen muss. Besonders die Anforderungen an Zweckbindung, Pseudonymisierung und Datensparsamkeit sind hoch. Die bildungs(statistischen) Fachgremien haben daher bei der Konzeption einer BVStat frühzeitig Vertreter der deutschen Datenschutzaufsichtsbehörden einbezogen.

Für eine erfolgreiche und rechtssichere Einführung eines Bildungsverlaufsregisters sind aus Sicht des HmbBfDI zahlreiche Voraussetzungen zu erfüllen, die derzeit noch nicht ausreichend gegeben sind. Aus datenschutzrechtlicher Sicht stellt eine BVStat einen substanziellen Eingriff in die informationelle Selbstbestimmung dar, insbesondere, da es sich bei den betroffenen Personen um Kinder und Jugendliche handelt. Es besteht somit eine hohe Darlegungslast, aus welchen Gründen eine BVStat von überragendem Allgemeininteresse ist, der vorgesehene Umfang der Datenerhebung erforderlich ist und die intendierten Ziele und Zwecke nicht durch andere Instrumente erreicht werden können. Aus Sicht des HmbBfDI fehlt es derzeit diesbezüglich an einer hinreichenden Konkretisierung der mit der Neuanlage des vorgesehenen Bildungsverlaufsregisters verfolgten Zwecke und Nutzungsmöglichkeiten sowie des Inhalts und Umfangs der dazu vorgesehenen Datenverarbeitungen sowie des Ortes der Datenhaltung, insbesondere in Anbetracht der auf Länderebene teilweise bereits bestehenden Datenbestände.

Der bzw. die Gesetzgeber sollten im Rahmen einer sorgfältigen Verhältnismäßigkeitsprüfung die Risiken eines Bildungsverlaufsregisters ermitteln und abwägen. Bei der beabsichtigten Nutzung dieser Daten müssen auch der Aspekt der Minderjährigkeit der Betroffenen und die

Gefahr der lebenslangen Stigmatisierung mitberücksichtigt werden, die aus der dauerhaften Nachvollziehbarkeit ihrer Schullaufbahn bzw. Bildungshistorie resultieren kann. Der HmbBfDI erkennt an, dass eine solche Statistik Chancen für eine verbesserte Bildungssteuerung bieten kann. Damit diese Potenziale verantwortungsvoll genutzt werden können, ist es aus Sicht des HmbBfDI jedoch unerlässlich, die datenschutzrechtlichen Anforderungen und die berechtigten Interessen der Betroffenen in den Mittelpunkt zu stellen. Eine enge Zusammenarbeit aller beteiligten Akteur:innen ist eine wichtige Voraussetzungen, um tragfähige Lösungen zu entwickeln.

Der HmbBfDI wird diesen Prozess konstruktiv begleiten und sich für einen Ausgleich zwischen den angestrebten Verbesserungen und dem Schutz der Privatsphäre einzusetzen.

5. User-Help-Desk – Anfertigung nicht geschwärzter Screenshots mit sensiblen Inhalten

Screenshots mit personenbezogenen Daten, die in Supportfällen gefertigt werden und ungeschwärzt beim Dienstleister des Supports als Auftragsverarbeiter gespeichert werden, führen zumindest dann nicht zu einem nach Art. 33 DSGVO meldepflichtigen Risiko, wenn die Speicherung in einem zugriffsgeschützten Bereich erfolgt, auf den nur besonders zu Verschwiegenheit verpflichtete Mitarbeitende Zugriff haben und eine Schwärzung zeitnah nachgeholt wird.

Den HmbBfDI haben gelegentlich Data Breach-Meldungen unterschiedlicher Fachbehörden erreicht, in denen ein Verarbeitungsvorgang im Zusammenhang mit dem User-Help-Desk geschildert wurde. Alle Vorfälle verliefen in diesem Zusammenhang gleich. Unterschiedliche Fachbehörden wenden sich im Falle technischer Probleme an den User-Help-Desk (UHD) bei Dataport. Im Rahmen der Ticketaufnahme und Fehlerbehebung fertigen die bearbeitenden UHD-Agenten auch

Screenshots an, die personenbezogene Daten aus den jeweiligen Anwendungen der Fachbehörden enthalten können. Die Mitarbeiter:innen des UHD werden angehalten die personenbezogenen Daten in diesem Prozess zu schwärzen. Ein Hinweisfenster erscheint, das sie bei Anfertigung an die Schwärzungen erinnert. Dennoch kommt es gelegentlich dazu, dass die Schwärzungen vergessen werden und eine Weiterleitung an die nächste Abteilung innerhalb Dataports erfolgt, Dataport die nicht erforderlichen Daten also weiterverarbeitet. Für gewöhnlich werden diese problematischen Tickets nach der Identifizierung an das Sicherheitsmanagement bei Dataport weitergeleitet und in einen geschützten Mandanten übertragen, in dem nur eine geringe Anzahl an Personen aus dem Sicherheitsmanagement Zugriff hat. Aber auch dort werden die Tickets nach spätestens zwei Tagen geschwärzt. Zudem wird sodann ein bereinigtes Ersatzticket eröffnet. Dataport ist Auftragsverarbeiter der Bezirksämter – womit eine weisungsgebundene Datenverarbeitung erfolgt – und meldet gem. Art. 33 Abs. 2 DSGVO den Vorfall an die verantwortliche Stelle. Schließlich erfolgt eine Data Breach-Meldung nach Art. 33 DSGVO über die zuständige Fachamtsleitung. Die Mitarbeiter:innen bei Dataport und im UHD sind nach § 34 HmbSÜGG sicherheitsüberprüft und zur Verschwiegenheit verpflichtet.

Die meldenden Fachämter baten um Aufklärung, ob diese Vorfälle auch künftig noch im Rahmen des Art. 33 DSGVO an den HmbBfDI zu melden sind. Der HmbBfDI wies darauf hin, dass eine Meldung nach Art. 33 DSGVO in den geschilderten Fällen nicht durchgeführt werden muss. Wichtig in diesem Zusammenhang ist jedoch, dass der zu bewertende Vorfall nicht von dem konkret geschilderten Sachverhalt abweicht und weitere Umstände hinzutreten, die ein Risiko für die Betroffenen nahelegen. Dies wäre etwa dann der Fall, wenn die Daten an einen Empfänger außerhalb Dataports gelangten oder wenn das nicht geschwärzte Dokument für lange Zeit außerhalb des geschützten Mandanten aufbewahrt (also übersehen oder vergessen) würde.

Die wesentlichen Umstände, die den HmbBfDI zu der Bewertung bewegten, waren, dass die weitere Verarbeitung der Informationen über die bestehenden Schweigepflichten der Mitarbeiter:innen geschützt

wird. Es ist nicht davon auszugehen, dass die Informationen an Dritte weitergeleitet oder anderen offengelegt werden, da dies mit einem Verstoß gegen die Schweigepflicht der Mitarbeiter:innen verbunden wäre. Zudem ist bereits ein Vorgehen implementiert, bei dem das Dokument bereinigt und das ursprüngliche Dokument in einen geschützten Mandaten überführt wird. Das Verfahren sieht grundsätzlich auch vor, dass jedenfalls die Mitarbeiter:innen des UHD personenbezogene Daten einsehen können, denn ein Zugriff auf den Vorgang ist erforderlich, um die Fehleridentifizierung überhaupt vorzunehmen zu können. Zwar werden die isolierten Daten für einen gewissen Zeitraum „ungeschwärzt" aufbewahrt. Dies findet allerdings in einem geschützten Umfeld statt und eine Schwärzung wird hier nachgeholt.

6. Parkraumregister

Bedürfnisse intensiver Verkehrsplanung setzen eine breite Datengrundlage voraus und sind ein gutes Beispiel dafür, inwieweit Wertungen aus dem Fachrecht maßgeblich auch für die datenschutzrechtliche Bewertung sind.

Der HmbBfDI wurde an der Schaffung eines Parkraumregisters beratend hinzugezogen, das im Rahmen des Koalitionsvertrags in der Entwicklung eines umfassenden Masterplans Parken für die Stadt Hamburg vorgesehen ist. Ziel dieses Masterplans ist es, eine systematische und vollständige Erfassung der vorhandenen Stellplätze im öffentlichen sowie im privaten Raum Hamburgs zu realisieren.

Im Fokus der zur Beratung stehenden Projektphase steht die erstmalige Erfassung privater Stellplätze. Diese Aufgabe wird vom Landesbetrieb Geoinformation und Vermessung (LGV) übernommen. Die Erhebung basiert auf bereits rechtmäßig erhobenen und vorhandenen Datenbeständen, wie beispielsweise Orthofotos, Katasterdaten aus dem Amtlichen Liegenschaftskatasterinformationssystem (ALKIS)

sowie Befahrungsfotos. Durch die Kombination dieser Datenquellen wird eine möglichst genaue und vollständige Erfassung der Stellplätze gewährleistet.

Erfasst und digitalisiert werden dabei verschiedene Arten von Stellplätzen: oberirdische Parkflächen, überdachte Parkplätze, Parkdecks sowie Tiefgaragen. Die Erfassung erfolgt mittels moderner GIS-Technologie (Geographische Informationssysteme), die eine punktgenaue Erfassung der Stellplätze gemäß dem Objektschlüsselkatalog (OSK) ermöglicht. Anschließend werden die erfassten Daten mit den Katasterdaten abgeglichen, um eine hohe Datenqualität und Aktualität sicherzustellen. Die aggregierten Ergebnisse dieser Erhebung werden der Behörde für Stadtentwicklung und Wohnen (BSW) sowie der Behörde für Verkehr und Mobilitätswende (BVM) zur Verfügung gestellt. Diese Behörden nutzen die Daten für die Verkehrsplanung und die Entwicklung von Maßnahmen zur Verbesserung der Parkplatzsituation in Hamburg. Eine Veröffentlichung der erhobenen Daten ist nicht vorgesehen, um den Schutz der Privatsphäre und die Vertraulichkeit der Informationen zu gewährleisten.

Die Erhebung und Verarbeitung der Daten erfolgt auf Grundlage des Hamburgischen Vermessungsgesetzes (HmbVermG). Dieses Gesetz definiert die Erfassung von Geobasisdaten als öffentliche Aufgabe, insbesondere für Fachplanungen wie die Verkehrsplanung. Zudem regelt das HmbVermG die Integration der Stellplatzdaten in das Liegenschaftskataster, wodurch eine langfristige und nachhaltige Nutzung der Daten sichergestellt wird.

Die Datenübermittlung an die Behörde für Verkehr und Mobilitätswende dient insbesondere der Entwicklung und Bewertung von Planungen im öffentlichen Verkehrsraum. Dabei steht die Beurteilung des Parkdrucks in verschiedenen Stadtteilen im Vordergrund. Die gewonnenen Erkenntnisse ermöglichen es, Stellplatzschlüssel für belastete Stadtteile abzuleiten und gezielte Maßnahmen zur Entlastung des Parkraums zu entwickeln.

Die Erfassung von PKW-Stellplätzen auf Privatgrundstücken kann grundsätzlich die Erhebung personenbezogener Daten darstellen, da Rückschlüsse auf die Nutzung privater Flächen möglich sind. Im vorliegenden Projekt erfolgt die Datenerhebung jedoch auf Basis bereits vorhandener, rechtmäßig erhobener Geobasisdaten und ohne direkte Identifikation von Personen. Die Daten werden ausschließlich für fachplanerische Zwecke genutzt und nicht veröffentlicht. Aufgrund der begrenzten Eingriffstiefe in die Privatsphäre und der Einhaltung der gesetzlichen Vorgaben, insbesondere des Hamburgischen Vermessungsgesetzes, ist die Maßnahme datenschutzrechtlich als unbedenklich einzustufen. Eine hohe Eingriffstiefe in personenbezogene Rechte liegt nicht vor, sodass die Erfassung und Verarbeitung der Stellplatzdaten im Rahmen des Masterplans Parken datenschutzrechtlich zulässig ist.

7. Scan-Fahrzeuge zur automatisierten Parkraumkontrolle

Parkverstöße werden künftig noch seltener unentdeckt bleiben: Im Jahr 2026 könnten Scan-Fahrzeuge den Parkraum in ausgewählten Stadtteilen Hamburgs – zunächst testweise – kontrollieren. Dies erfordert auch die Erfassung von Kfz-Kennzeichen am Parkscheinautomaten. Anonymes Parken wird damit langfristig eingeschränkt; der HmbBfDI hat jedoch auf eine verkürzte Speicherdauer sowie geeignete Maßnahmen gegen Profilbildung hingewirkt.

Den rechtlichen Rahmen soll dabei das „Gesetz zum digitalen Parkraummanagement" schaffen. Kernelement des Gesetzesvorhabens, über das die Bürgerschaft im Jahr 2026 entscheiden wird, sind die Videokontrollen durch Scan-Fahrzeuge-. Die Scan-Fahrzeuge, wie sie im europäischen Ausland bereits zum Einsatz kommen, sollen dabei helfen, Parkverstöße effizienter aufzudecken, indem sie im Vorbeifahren Kennzeichen parkender Fahrzeuge kamerabasiert erfassen und automatisiert mit einer Datenbank abgleichen, in der gültige Park-

berechtigungen hinterlegt sind. Die Videokontrollen setzen damit zunächst voraus, dass alle einem Kfz-Kennzeichen zugeordneten kurz- oder langfristigen Parkberechtigungen und Ausnahmegenehmigungen zum Halten und Parken digital verzeichnet werden. Erst dann kann das beim „Vor-Ort-Scan" erhobene Kfz-Kennzeichen gültigen Parkberechtigungen gegenübergestellt und im Falle eines Negativergebnisses die Prüfung eines etwaigen Parkverstoßes veranlasst werden.

Das „Gesetz zum digitalen Parkraummanagement" regelt die Rechtsgrundlagen für diese Datenverarbeitungsvorgänge. Die Grundrechtseingriffe, die mit der Verarbeitung von personenbezogenen Kfz-Kennzeichen zum Zwecke der Ermittlung von Ordnungswidrigkeiten einhergehen, können nur bei Vorliegen eines gesetzlichen Erlaubnistatbestandes gerechtfertigt sein.

Einen entsprechenden Gesetzesentwurf zur Änderung des Straßenverkehrsrechts hatte der für das Projekt „Digitalisierung Parkraumkontrolle – DigiParK" verantwortliche Landesbetrieb Verkehr (LBV) zunächst auf Bundesebene vorgelegt. Die Gesetzesinitiative wird im Berichtszeitpunkt weiterhin in Bundesgremien beraten. Unter Annahme einer konkurrierenden Gesetzgebungskompetenz ist parallel dazu das hamburgische „Gesetz zum digitalen Parkraummanagement" ausgearbeitet worden, das vor den Bundesvorschriften in Kraft treten könnte.

Der neue Landesentwurf weist in seinem Regelungsgehalt Parallelen zum ursprünglichen Textvorschlag des LBV auf, wie er beim Bund eingereicht und durch den HmbBfDI im Tätigkeitsbereich aus dem Jahre 2023, 32. TB, Kap. VI 7, vorgestellt worden ist:

§ 2 Abs. 1 des „Gesetzes zum digitalen Parkraummanagement" erlaubt zunächst die Abfrage von Kennzeichen bei der Beantragung oder zum Nachweis von Berechtigungen und Genehmigungen zum Halten und Parken. Dies gilt ausweislich des § 2 Abs. 1 S. 2 des Gesetzesentwurfs insbesondere auch für das sog. Kurzzeitparken – was in der Praxis bedeuten würde, dass die Angabe des Kennzeichens

auch an Parkscheinautomaten verpflichtend werden kann, soweit die zuständige Behörde dies bestimmt.

§ 2 Abs. 2 trägt in seinem ersten Satz dem datenschutzrechtlichen Grundsatz der Zweckbindung Rechnung, indem er die Verarbeitung der anzugebenden Kennzeichen nur insoweit zulässt, wie sie den oben bezeichneten Antrags- und Nachweiszwecken sowie der „Überwachung des ruhenden Verkehrs in Bezug auf die Einhaltung der Vorschriften zum Halten und Parken" und der „Verfolgung und Ahndung von entsprechenden Verkehrsordnungswidrigkeiten" dient. Ergänzend wird die Übermittlung, Verwendung oder Beschlagnahme der Daten nach anderen Rechtsvorschriften durch § 2 Abs. 2 S. 3 untersagt.

Die Speicherfrist wird durch § 4 S. 1 des Gesetzesentwurfs geregelt. Danach sind die Angaben zum Kennzeichen nach Ablauf der Parkberechtigungsdauer zum Tagesende zu löschen. Ausweislich der Gesetzesbegründung wäre es bei einer früheren Datenlöschung nicht möglich, die tatbestandsmäßig verschiedenen Vorgänge des „Parkens ohne Parkberechtigung" und des „Überschreitens der Parkberechtigungsdauer" abzugrenzen.

Daneben wird die zuständige Behörde zur Durchführung von „Videokontrollen" ermächtigt, in deren Rahmen das „Bild des Kennzeichens des Fahrzeugs (vorne und hinten)" und der „Ort" und die „Zeit der Kontrolle" automatisiert verarbeitet werden, vgl. § 3 Abs. 1 des Gesetzesentwurfs, sowie zum automatisierten Abgleich der durch Kontrollfahrzeuge „gescannten" mit den digital hinterlegten Kennzeichen, vgl. § 3 Abs. 3 S. 1, wobei die obige Zweckbindung auch diese Verarbeitungsschritte determiniert.

Dass im Rahmen der Videokontrollen keine personenbezogenen Daten Dritter erfasst werden, ist dabei in Übereinstimmung mit § 3 Abs. 2 S. 1 1. HS des Gesetzesentwurfs durch technische Maßnahmen sicherzustellen. Auch müssen sowohl die überwachten Parkräume als auch die Kontrollfahrzeuge als solche gekennzeichnet sein, vgl. § 3 Abs. 2 S. 3 2. HS.

Ergibt der digitale Datenbankabgleich, dass das Fahrzeug in dem jeweiligen Bereich und Zeitraum geparkt werden durfte, sind die bei der Videokontrolle verarbeiteten Daten unmittelbar nach dem Abgleich zu löschen, vgl. § 4 S. 2 des Gesetzesentwurfs. Die Löschfrist gilt nicht, wenn ein Parkverstoß im Raum steht, vgl. § 4 S. 3. Wird eine einschlägige Parkberechtigung in der Datenbank nicht aufgefunden, soll die weitere unverzügliche Sachverhaltsaufklärung und ggf. die anschließende Verfolgung der Ordnungswidrigkeit ausweislich der Gesetzesbegründung entsprechend der heutigen Vorgehensweise behördlichem Kontrollpersonal übertragen werden. Das Ordnungswidrigkeitenverfahren selbst würde also nicht automatisiert.

Die behördliche Abstimmung zum Gesetzesentwurf hat im Sommer des Jahres 2025 stattgefunden. Der HmbBfDI hat den Entwurf aus datenschutzrechtlicher Perspektive bewertet und darauf hingewirkt, dass der Wortlaut stellenweise nachgeschärft wurde, sowie die Aufbewahrungsfrist für anzugebende Kfz-Kennzeichen hinterfragt. Die „Angaben zum Kennzeichen" sind nunmehr gemäß § 4 S. 1 des Gesetzesentwurfs – sowohl bei Dauerparkberechtigungen, wie etwa Bewohnerparkausweisen, als auch bei Berechtigungen zum Kurzzeitparken – nach Ablauf der Parkberechtigungsdauer zum Tagesende zu löschen. Diese Neufassung der Bestimmung ist aus datenschutzrechtlicher Sicht eine deutliche Verbesserung gegenüber den ursprünglich vorgesehenen Regelungen, die teilweise wesentlich längere Aufbewahrungsfristen festlegten und zwischen den Berechtigungsarten differenzierten.

Nach Annahme des „Gesetzes zum digitalen Parkraummanagement" durch die Bürgerschaft wird es insbesondere darauf ankommen, ein Sicherheitskonzept zu entwickeln, das den gesetzlichen Vorgaben gerecht wird und auch den Ausschluss jeder Profilbildung gewährleistet. Hierzu werden weitere Gespräche des HmbBfDI mit dem LBV stattfinden, bevor das Projekt zur Einführung der Scan-Fahrzeuge ggf. noch im Jahre 2026 in seine Pilotphase übergehen kann.

ÖFFENTLICHKEITSARBEIT UND MEDIENBILDUNG VIII.

Öffentlichkeitsarbeit und Medienbildung

1. Presse- und Öffentlichkeitsarbeit

Die Themen Künstliche Intelligenz, Videoüberwachung und die neuen EU-Digitalgesetze prägten im Berichtsjahr 2025 die Pressearbeit des HmbBfDI. Dabei stand das KI-Training mit personenbezogenen Daten durch Meta besonders im Fokus der Presse.

Pressearbeit

Im Jahr 2025 setzte sich der Trend aus 2024 fort: Presseanfragen mit Bezug zu Künstlicher Intelligenz machen einen immer größeren Anteil der Kommunikation des HmbBfDI aus. Während im Vorjahr noch 22 Prozent aller Anfragen einen KI-Bezug hatten, stieg dieser Anteil im Berichtsjahr auf 35 Prozent. Besonders häufig wurde der HmbBfDI zu datenschutzrechtlichen Fragen rund um das KI-Training des Meta-Konzerns mit Nutzer:innendaten kontaktiert. Mit dem Stichtag 27. Mai 2025 begann Meta, öffentliche Daten aller volljährigen Nutzer:innen für das Training von KI einzusetzen. Der HmbBfDI informierte durch eine Pressemitteilung und einen ausführlichen Fragen- und Antwortkatalog über das Vorhaben und die Widerspruchsmöglichkeiten der Betroffenen. Insbesondere im Mai 2025 gingen zum Thema zahlreiche, mehrheitlich von internationalen Medien stammende Presseanfragen beim HmbBfDI ein.

Ein weiteres zentrales Thema war die Videoüberwachung und -aufzeichnung zum Zweck des KI-Trainings am Hansaplatz und Hachmannplatz in Hamburg. Der HmbBfDI arbeitete im Vorfeld eng mit der Polizei Hamburg zusammen, um alle relevanten datenschutzrechtlichen Fragen zu klären. Die Polizei konnte die Anforderungen hinsichtlich Sicherheit, Zugriff, Speicherung, Diskriminierungspotential und Löschung so beantworten, dass keine durchgreifenden datenschutzrechtlichen Bedenken gegen das Training der KI-Modelle mehr bestanden.

Neben diesen Leuchtturmthemen erreichten den HmbBfDI im Berichtsjahr eine große Bandbreite weiterer Anfragen. Dazu zählten unter anderem Fragen zum Angemessenheitsbeschluss EU-US Data Privacy Framework, zum Einsatz von KI in Schulen, zu chinesischen KI-Modellen wie DeepSeek, zu Palantir, zu verschiedenen Cyberangriffen sowie zur elektronischen Patientenakte (ePA). 54 Prozent der Anfragen stammten von überregionalen deutschen Medien. Der Anteil regionaler hamburgisch-norddeutscher Medien stieg von 21 auf 34 Prozent, während Anfragen ausländischer Medien von 17 auf 12 Prozent zurückgingen.

Presseanfragen	**2023**	**2024**	**2025**
regionaler Medien:	29 %	21 %	34 %
überregionaler Medien:	62 %	83 %	54 %
ausländischer Medien:	9 %	17 %	12 %

Tabelle1: Presseanfragen beim HmbBfDI 2023, 2024 und 2025

Im Berichtszeitraum veröffentlichte der HmbBfDI insgesamt 33 Pressemitteilungen und Website-Informationen, fast doppelt so viele wie im Vorjahr, in dem es 17 Veröffentlichungen gab. Ein Schwerpunkt lag auf Artikeln, die zur Beratung in datenschutzrechtlichen Fragen dienten, wie etwa der „digitale Frühjahrsputz" zu neuen Aufbewahrungsfristen und Löschkonzepten, „Fotografie in der Kita" und „Straßenfotografie". Im Rahmen einer anlasslosen Prüfaktion informierte der HmbBfDI ausführlich über das Tracking durch Drittdienste und die korrekte Gestaltung von Cookiebannern. Weitere Schwerpunkte bildeten Veröffentlichungen zu Geltung und Fristen der neuen EU-Digitalgesetze KI-Verordnung, Data Act und Digital Services Act. Zudem wurden mehrere Gerichtsurteile besprochen und eingeordnet, über Entwicklungen und Fristen beim Start der elektronischen Patientenakte berichtet und Medienbildungsthemen publik gemacht.

Darüber hinaus engagierten sich der HmbBfDI und zahlreiche Mitarbeiter:innen der Behörde in der öffentlichen Diskussion, indem sie Vorträge und Präsentationen zu verschiedenen Datenschutzthemen hielten und an Gesprächsrunden sowie Podiumsdiskussionen teilnahmen. Der HmbBfDI war regelmäßig in Nachrichten- und Ratgeberformaten nationaler Fernsehsender präsent und stand für Interviews zur Verfügung.

Die Durchdringung des Alltags mit KI spiegelt sich in der Pressearbeit des HmbBfDI wider. Anfragen zu sozialen Netzwerken, dem KI-Training mit personenbezogenen Daten, gesetzlichen Regelungen für KI-Anwendungen und neuen KI-Systemen sind für die Öffentlichkeit von großem Interesse. Die Pressearbeit des HmbBfDI wird daher weiterhin darauf ausgerichtet sein, aktuelle Entwicklungen zu beurteilen und die Öffentlichkeit umfassend aufzuklären.

Öffentlichkeitsarbeit

Der Tätigkeitsbericht 2024 konnte als HTML-Seite auf der Website veröffentlicht werden, wodurch es möglich ist, einzelne Kapitel anzuwählen, zu verlinken und auch die Auffindbarkeit von Themen in Suchmaschinen zu steigern.

Die vor zwei Jahren gelaunchte Website des HmbBfDI wird voraussichtlich in 2026 vollumfänglich barrierefrei sein. Dazu wurden in 2025 die technischen Weichen gestellt und entsprechende Anpassungen im Backend, wie die Hierarchisierung von Überschriften und die vorlesegerechte Einstellung der Unterseiten, vorgenommen. Videos in deutscher Gebärdensprache sind aktuell in Produktion.

2. #MoinDigitaleVorbilder – Datenschutz für Kultur und Bildung

Der HmbBfDI setzt mit dem von der EU gefördertem Projekt #MoinDigitaleVorbilder gezielte Impulse für den verantwortungsvollen Umgang mit personenbezogenen Daten in der Kultur- und Bildungsarbeit. Das Projekt richtet sich an pädagogische Fachkräfte und bietet praxisnahe Veranstaltungen, die aktuelle Herausforderungen wie Künstliche Intelligenz, Bildrechte und digitale Kommunikation aufgreifen. Ziel ist es, Datenschutzkompetenz zu stärken und digitale Selbstbestimmung in Hamburg nachhaltig zu fördern.

Der Schutz personenbezogener Daten ist in einer zunehmend digitalisierten Gesellschaft von zentraler Bedeutung. Pädagogische Fachkräfte, die mit Kindern und Jugendlichen arbeiten, stehen vor der Herausforderung, Datenschutz nicht nur rechtssicher umzusetzen, sondern auch alltagsnah und verständlich zu vermitteln. Der HmbBfDI unterstützt sie dabei mit dem EU-geförderten Projekt #MoinDigitaleVorbilder, das von Januar 2025 bis Dezember 2026 gemeinsam mit der LAG Kinder- und Jugendkultur durchgeführt wird. Das Projekt ist Teil der Bildungsstrategie des HmbBfDI und verfolgt das Ziel, Fachkräfte in Jugend- und Kultureinrichtungen für Datenschutzaspekte zu sensibilisieren, sie im sicheren Umgang mit Daten zu stärken und auf die wachsende Komplexität digitaler Technologien vorzubereiten.

Im Rahmen von #MoinDigitaleVorbilder werden verschiedene Veranstaltungsformate angeboten, die sich an den Bedarfen und Fragestellungen der Zielgruppen orientieren. Die Auftaktveranstaltung in 2025 ermöglichte einen praxisnahen Einstieg in das Thema Datenschutz: Mit Quiz, App-Sicherheitscheck und Infomaterialien konnten die Teilnehmenden ihr Wissen testen und direkt mit Expertinnen

und Experten ins Gespräch kommen. Die offene Atmosphäre förderte den Austausch und die Vernetzung zwischen pädagogischen Fachkräften, Kulturschaffenden und Datenschutzinteressierten.

Exkursionen boten die Möglichkeit, Datenschutz in der Praxis zu erleben. So öffnete der HmbBfDI seine Türen und gab Einblicke in die Aufgaben und Arbeitsweise der Behörde. Die Teilnehmenden erhielten Informationen darüber, wie Datenschutzaufsicht konkret funktioniert, welche aktuellen Themen die Behörde beschäftigen und wie sie bei Fragen und Problemen unterstützt werden können. Ein weiteres Highlight war die Exkursion zum Artificial Intelligence Center Hamburg (ARIC), bei der die Grundlagen von Künstlicher Intelligenz und Maschinellem Lernen vermittelt und praktische Anwendungsbeispiele vorgestellt wurden.

Die kompakten Bildungshappen greifen aktuelle Fragestellungen aus dem pädagogischen Alltag auf und bieten fundierte Informationen sowie praktische Tipps, direkt von Mitarbeitenden aus den Fachbereichen des HmbBfDI und weiteren Expert:innen. So wurden beispielsweise in 2025 Messengerdienste unter die Lupe genommen: Welche Apps sind datenschutzfreundlich, wie können Einstellungen sinnvoll genutzt werden und welche Risiken bestehen bei der Nutzung im schulischen oder kulturellen Kontext? Ein weiterer Bildungshappen widmete sich dem Bildrecht und klärte, wann Fotos von Veranstaltungen genutzt werden dürfen, welche Einwilligungen erforderlich sind und wie kulturelle Einrichtungen rechtssicher mit Bildern umgehen können.

Workshops wie „Das kleine Datenschutz-Einmaleins“ vermittelten Grundlagenwissen und gaben konkrete Hilfestellungen für die datenschutzfreundliche Gestaltung von Öffentlichkeitsarbeit und Teilnehmermanagement. Die Teilnehmenden diskutierten zentrale Fragen aus dem Arbeitsalltag, sammelten Tipps und entwickelten gemeinsam Lösungen für die Praxis. Die Ergebnisse werden grafisch aufbereitet und als Materialien auf der Projektwebsite www.digitale-vorbilder.eu zur Verfügung gestellt. Viele Veranstaltungen wurden zudem aufgezeichnet und stehen als Video sowie Präsentation zur Verfügung, sodass auch Interessierte, die nicht live teilnehmen konnten, von den Inhalten profitieren.

Das Projekt #MoinDigitaleVorbilder wird auch im Jahr 2026 weitergeführt und bietet eine Vielzahl unterschiedlicher Veranstaltungen an, die kontinuierlich an die aktuellen Entwicklungen und Bedarfe angepasst werden. Damit leistet der HmbBfDI einen wichtigen Beitrag zur Sensibilisierung und Qualifizierung von pädagogischen Fachkräften in Hamburg. Darüber hinaus entstehen Materialien, die einen nachhaltigen Nutzen nicht nur für einzelne Fachkräfte, sondern für ganze Einrichtungen und die breite Öffentlichkeit ermöglichen.

3. Datenschutzsprechstunde – Beratung und Sensibilisierung für den digitalen Alltag

Der HmbBfDI hat im Jahr 2025 mit der Datenschutzsprechstunde ein neues Beratungsangebot ins Leben gerufen. Das Format verbindet persönliche und digitale Beratung und trägt gezielt dazu bei, das Bewusstsein für Datenschutz in der Bevölkerung zu stärken und die Menschen bei den Veränderungen und Herausforderungen des digitalen Zeitalters unterstützend zu begleiten.

Mit dem Start der Datenschutzsprechstunde im Jahr 2025 hat der HmbBfDI auf die wachsenden Herausforderungen der Digitalisierung und die zunehmende Komplexität datenschutzrechtlicher Fragestellungen reagiert. Die Einführung der Datenschutzsprechstunde erfolgte im Rahmen des Teilersuchens der Bürgerschaft aus Drs. 22/17227 „Familien fit fürs Netz: Datenschutz-Sprechstunden und Webinare für Hamburgs digitale Zukunft“.

Die Datenschutzsprechstunde wird sowohl als Präsenzveranstaltung in Stadtteilzentren, Bibliotheken und Seniorencafés als auch als digitales Angebot über die Videoplattform BigBlueButton durchgeführt. Die Themen orientieren sich an den konkreten Fragestellungen und Bedürfnissen der Bevölkerung, darunter der Umgang mit Kinderfotos im Netz, Smartphone-Sicherheit, Künstliche Intelligenz, elektronische

Patientenakte, Datenschutz im Verein und Fotografie in der Kita. Die Veranstaltungen sind zielgruppenspezifisch konzipiert und bieten praxisnahe Hilfestellungen für den Alltag.

Die Kombination aus analogen und digitalen Angeboten ermöglicht eine breite Erreichbarkeit und trägt dazu bei, unterschiedliche Lebensrealitäten und Zugangswege zu berücksichtigen. Seit Oktober 2025 findet die Datenschutzsprechstünde in einem festen 14-tägigen Rhythmus statt. Die Einführung fester, regelmäßig wiederkehrender Termine hat die Planbarkeit und Bekanntheit der Datenschutzsprechstunde gestärkt. Durch gezielte Öffentlichkeitsarbeit, Plakataktionen und ein individuelles Design wurde die Sichtbarkeit des Formats erhöht.

Die enge Zusammenarbeit mit Kooperationspartnern wie Bibliotheken, Elternschulen, Gewerkschaften und weiteren Bildungseinrichtungen hat sich als besonders wertvoll erwiesen. Sie ermöglicht die Entwicklung passgenauer Inhalte und fördert den Austausch zwischen verschiedenen Akteuren im Bereich Datenschutz und Bildung. Die Datenschutzsprechstunde wird von den Teilnehmenden durchweg positiv bewertet. Besonders geschätzt werden die praxisnahen Informationen sowie die Möglichkeit, individuelle Fragen zu stellen. Auch komplexe datenschutzrechtliche Themen werden verständlich erklärt. Das zeigt sich nicht zuletzt daran, dass einzelne Veranstaltungen bis zu 50 Interessierte angezogen haben, die aktiv am Austausch teilgenommen und den Bedarf an niedrigschwelliger Datenschutzberatung deutlich gemacht haben.

Die Datenschutzsprechstunde leistet somit einen wichtigen Beitrag zur Förderung von Datenschutzkompetenz, indem sie komplexe gesetzliche Vorgaben verständlich vermittelt und praxisnah auf die alltäglichen Lebenssituationen der Bürgerinnen und Bürger herunterbricht. Sie trägt dazu bei, Unsicherheiten abzubauen und Wissen im Umgang mit persönlichen Daten zu vermitteln.

Die wachsende Nachfrage nach Beratungsangeboten verdeutlicht, dass die Sensibilisierung für Datenschutzfragen in der Bevölkerung steigt und die Angebote des HmbBfDI auf großes Interesse stoßen. Das Projekt zeigt, wie Datenschutzberatung bürgernah und verständlich gestaltet werden kann und leistet einen wichtigen Beitrag zur Sensibilisierung der Bevölkerung im Umgang mit personenbezogenen Daten. Der HmbBfDI wird das Format kontinuierlich weiterentwickeln, um den Anforderungen einer sich wandelnden digitalen Gesellschaft gerecht zu werden.

INFORMATIONEN ZUR BEHÖRDENTÄTIGKEIT IX.

Informationen zur Behördentätigkeit

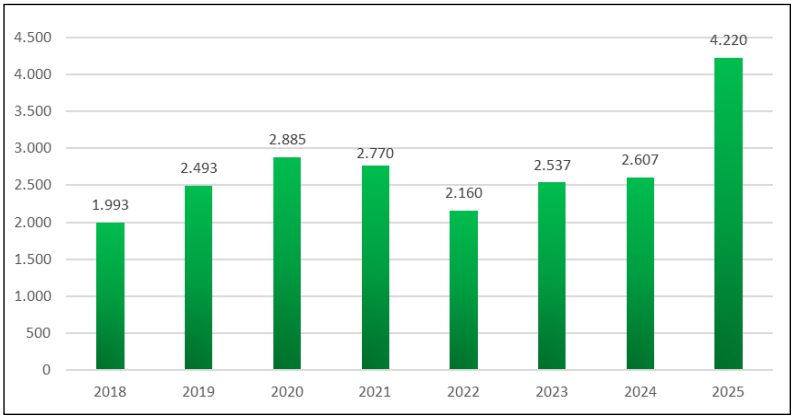
1. Statistische Informationen (Zahlen und Fakten)

Die Zahl der Eingänge hat mit 6.219 im Jahr 2025 nicht nur einen historischen Höchststand erreicht, sondern mit einer Steigerung alleine der datenschutzrechtlichen Beschwerden um 62 Prozent gegenüber der schon hohen Ausgangsbasis des Vorjahrs eine völlig neue Dimension erreicht.

1.1 Beschwerden und Beratungen

Die Beschwerden nach Art. 77 DSGVO machen nach wie vor den Löwenanteil der Tätigkeiten der Beschäftigten des HmbBfDI aus. Sie sind daher aber auch der Teil der Aufgaben, der die meisten personellen, Ressourcen beansprucht. Im Berichtsjahr 2025 haben den HmbBfDI 4.220 datenschutzrechtliche Beschwerden von Bürgerinnen und Bürgern erreicht, was nicht nur eine extreme Steigerung gegenüber den Zahlen des Vorjahres, sondern auch den bisherigen Höchstwert von eingegangenen Beschwerden nach der DSGVO aus dem Jahr 2020 in den Schatten stellt.

Art des Eingangs	Grundlage	Anzahl 2025	Anzahl 2024
Beschwerden Betroffener	Art. 57 Abs. 1 lit. f) DSGVO	4.220	2.607
Hinweise nicht betroffener Personen		436	290
Meldungen von Verletzungen des Schutzes personen-bezogener Daten	Art. 33 DSGVO	1.115	955
Beratung Personen	Art. 57 Abs. 1 lit. e) DSGVO	277	243
Beratung Verantwortlicher	Art. 57 Abs. 1 lit. f) DSGVO	128	102
Beratung Behörden	Art. 57 Abs. 1 lit. c) DSGVO	43	24
		6.219	**4.237**



Beschwerden nach Art. 77 DSGVO beim HmbBfDI seit 2018

Auch die schriftlichen Beratungsanfragen sind im Berichtszeitraum gegenüber dem Vorjahr gestiegen. Dies zwar bei Weitem nicht in dem Umfang, in dem die Beschwerdezahlen angestiegen sind, dennoch ist auch hier von einer signifikanten Steigerung von rund 32 Prozent zu berichten:

Schriftliche Beratungen von				
Jahr	**Betroffenen**	**Unternehmen**	**Behörden**	**Gesamt**
2025	277	128	43	488
2024	243	102	24	369

Die Gesamtzahl der datenschutzrechtlichen Beratungen setzt sich aus den schriftlichen und den telefonischen Beratungen zusammen. Dabei erreichten auch die telefonischen Beratungsanfragen 2025 mit 1.002 einen neuen Höchstwert. Insgesamt wurden beim Hamburgischen Datenschutzbeauftragten im Berichtsjahr also 1.490 dokumentierte datenschutzrechtliche Beratungen durchgeführt.

1.2 Meldepflicht nach Art. 33 DSGVO

Im Jahr 2025 sind 1.115 Meldungen zu Verletzungen des Schutzes personenbezogener Daten bei der Hamburger Datenschutzaufsicht eingegangen. Das sind erneut 160 Meldungen mehr als im Vorjahr. Getrieben wird diese Zahl, die weiterhin von Jahr zu Jahr ansteigt, von den Hackerangriffen, von denen im Berichtsjahr 88 mehr als 2024 (33. TB, 2024, Kap. IX 1.2) gemeldet wurden und die damit alleine für mehr als die Hälfte des Anstiegs der Gesamtzahl verantwortlich sind. Die Meldungen über Hackerangriffe machen mittlerweile rund 34% der Gesamtmeldungen aus und bildeten 2025 erstmals den höchsten Einzelwert der Meldungen nach Art. 33 DSGVO.

Grund der Meldung	Anzahl der Meldungen	
	2025	2024
Hackerangriff	376	288
Falschversand per Post oder E-Mail	307	311
Hard- oder Softwarefehler	61	41
offener E-Mail-Verteiler	44	31
Diebstahl, Einbruch (ohne Hacker)	33	37
physikalischer Verlust (Laptop, Handy etc.)	25	29
Mitarbeiterexzess	21	13
Sonstiges	248	205
Gesamt	1.115	955

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 2025 folgende Maßnahmen ergriffen:

Maßnahme	Rechtsgrundlage	Anzahl 2025
Verwarnungen	Art. 58 Abs. 2 lit. b	22
Anweisungen und Anordnungen	Art 58. Abs. 2 lit. c – g und j	2
Verhängte Geldbußen	Art. 58 Abs. 2 lit. i	19

Im Jahr 2025 betrug die Gesamtsumme der verhängten Geldbußen 776.571 €.

1.4 Europäische Verfahren

Europäische Verfahren sind als datenschutzrechtliche Sachverhalte definiert, die aufgrund ihrer Thematik für mehrere Mitgliedstaaten der Europäischen Union von Belang sein könnten. In der Regel sind das Fälle, in denen sich eine Bürgerin oder ein Bürger eines Mitgliedstaats gegen ein international, also über die Landesgrenzen hinaus tätiges Unternehmen beschwert. Die Fälle werden dann in das Binnenmarkt-Informationssystem der Europäischen Kommission, das sogenannte IMI (Internal Market Information System), eingetragen. Die jeweilige Datenschutzaufsichtsbehörde ist dann entweder federführend („lead") tätig oder ist beteiligt („concerned").

Im Berichtsjahr wurden beim HmbBfDI 96 neue europäische Verfahren bearbeitet, davon in fünf Fällen federführend. Damit hat sich die Gesamtzahl, der europäischen Verfahren im Vergleich zum Vorjahr fast verdoppelt, die Zahl der Federführungen jedoch halbiert (2024: 51 Verfahren, davon 11 als Federführer, 33. TB 2024, Kap. IX 1.4).

1.5 Stellungnahmen in Gesetzgebungsverfahren (Förmliche Begleitung bei Rechtsetzungsvorhaben)

Im Jahr 2025 wurde der HmbBfDI an 68 Senatsdrucksachenabstimmungen beteiligt. Davon hatten 33 tatsächliche Rechtsetzungsverfahren zum Gegenstand.

ABKÜRZUNGSVERZEICHNIS
STICHWORTVERZEICHNIS

Abkürzungsverzeichnis

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

Stichwortverzeichnis

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

Auflage: 400 Exemplare
Bild Titelseite: Adobe Stock / Westend61
Layout: Verena Münch
Druck: Druckservice Nord Sedelky

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

Der Hamburgische
Beauftragte für Datenschutz
und Informationsfreiheit