Landesbeauftragte
für Datenschutz
und Akteneinsicht

Tätigkeitsbericht
Datenschutz 2024

Tätigkeitsbericht Datenschutz

der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht

zum 31. Dezember 2024

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat nach Artikel 59 Datenschutz-Grundverordnung und nach § 37 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz jeweils einen Jahresbericht über ihre Tätigkeit zu erstellen und dem Landtag sowie der Landesregierung zu übermitteln. Diese Berichte decken den Zeitraum vom 1. Januar bis zum 31. Dezember 2024 ab.

Die Tätigkeitsberichte können auch aus unserem Internetangebot unter www.LDA.Brandenburg.de abgerufen werden.

Impressum

Herausgeberin: Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Telefax: 033203 356-49
E-Mail: Poststelle@LDA.Brandenburg.de
Internet: https://www.LDA.Brandenburg.de

Titelbild: Forschungsgebäude des Potsdam-Instituts für Klimafolgenforschung
Foto: Maro Niemann, Potsdam

Druck: Landesvermessung und Geobasisinformation Brandenburg

Teil B: Bericht nach § 37 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz

Teil C: Die Dienststelle

Vorwort

Liebe Leserinnen, liebe Leser,

mit dem vorliegenden Tätigkeitsbericht möchte ich Sie über wichtige datenschutzrechtliche Themen sowie über ausgewählte Beratungs- und Beschwerdefälle informieren, mit denen sich meine Behörde im Berichtsjahr befasst hat.

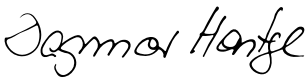
Bereits zum zweiten Mal thematisiere ich die Künstliche Intelligenz als Schwerpunkt. Daran zeigt sich, dass wir es hier mit einer rasanten technologischen Entwicklung zu tun haben, die einen zunehmend konkreten Einfluss auf unser Leben nimmt. Auch von legislativer Seite wird diese Herausforderung angenommen. So ist im Berichtsjahr die europäische KI-Verordnung in Kraft getreten. Sie lässt die Datenschutz-Grundverordnung unberührt. Die datenschutzrechtlichen Vorschriften, die beim Einsatz der Künstlichen Intelligenz zu beachten sind, bedürfen insoweit einer spezifischen Auslegung. Beispielsweise ist noch offen, inwieweit generative Sprachmodelle, die mit personenbezogenen Daten trainiert wurden, selbst einen Personenbezug aufweisen und wie die Rechte der betroffenen Personen bei der Nutzung solcher Modelle gewährleistet werden können. Die Datenschutzkonferenz und der Europäische Datenschutzausschuss haben bereits Handreichungen zur Künstlichen Intelligenz erarbeitet. Die Aufsichtsbehörden, die Wissenschaft und vor allem der Gesetzgeber sind aber auch weiterhin gefragt, Lösungen im Sinne der Bürgerinnen und Bürger zu erarbeiten.

Verantwortliche Stellen sind verpflichtet, der Datenschutzaufsichtsbehörde bestimmte Datenschutzverletzungen zu melden. Die Meldungen aus dem Berichtsjahr zeigen erneut, wie schwerwiegend sich menschliche oder technische Fehler auf die Gewährleistung der IT-Sicherheit auswirken können. Eine einzige falsche Entscheidung kann Tausende personenbezogener Daten betreffen. Trotz massiv angestiegener Sicherheitsbedrohungen aus dem In- und Ausland haben Verantwortliche oft keine ausreichenden Maßnahmen getroffen, um Datenschutz zu gewährleisten. Häufig sind Nachlässigkeiten, fehlende Fachkenntnisse oder Personalmangel die Ursache.

Die Videoüberwachung erweist sich in meiner Arbeit als Dauerbrenner. Erneut ist die Zahl der Beschwerden auf diesem Gebiet erheblich angestiegen. In diesem Zusammenhang hat meine Behörde im Berichtsjahr knapp 800 Kameras überprüft. Diese wurden z. B. zur Überwachung in der Nachbarschaft, in Schwimmbädern, Hotels, Unternehmen, Flüchtlingsunterkünften oder auf öffentlichen Plätzen eingesetzt. Immer wieder mussten meine Mitarbeiterinnen und Mitarbeiter korrigierend eingreifen; in einigen Fällen waren aufsichtsrechtliche Maßnahmen wie beispielsweise eine Anordnung erforderlich.

Darüber hinaus war meine Behörde im Berichtsjahr auch wieder mit umfangreichen Beratungen von verantwortlichen Stellen beschäftigt. Unter anderem warf die beabsichtigte Einführung einer Bezahlkarte für geflüchtete Menschen datenschutzrechtliche Fragen auf. Dies veranlasste mich, ausführlich zu dem Vorhaben Stellung zu nehmen und insbesondere auf die geplante Whitelist, eine Ausnahmeliste für Zahlungstransfers der Geflüchteten, einzugehen.

Die Themen der weiteren Beratungs- und Beschwerdefälle, über die ich in diesem Bericht informiere, sind wieder sehr vielfältig und betreffen fast alle Lebensbereiche. Ich wünsche Ihnen, liebe Leserinnen und Leser, eine interessante und angenehme Lektüre.



Dagmar Hartge

Bericht nach Artikel 59 Datenschutz-Grundverordnung

I Schwerpunkt: Künstliche Intelligenz

1 KI-Verordnung – Wirksamwerden und Aufsicht

Am 1. August 2024 trat die europäische Verordnung über Künstliche Intelligenz (KI-Verordnung, KI-VO)[1] in Kraft – die weltweit erste, umfassende gesetzliche Regulierung dieser neuen Technologie. Zweck der Verordnung ist die Förderung einer verantwortungsvollen Entwicklung und Verwendung Künstlicher Intelligenz in der Europäischen Union. In der KI-Verordnung ist u. a. festgelegt, wie KI-Systeme nach einem risikobasierten Ansatz eingestuft werden und welche Anforderungen Unternehmen wie auch öffentliche Verwaltungen bei der Entwicklung und Nutzung von KI-Systemen einzuhalten haben. Diese Regeln sollen das Vertrauen in die neue Technologie stärken und ebenso garantieren, dass die Sicherheit und die Grundrechte der Bürgerinnen und Bürger bei der Anwendung von KI-basierten Lösungen gewahrt werden. Mit der KI-Verordnung ergeben sich auch Chancen für innovative Produkte und Dienstleistungen, die den in der Europäischen Union geltenden sozialen und ethischen Standards entsprechen.

Die Regelungen der KI-Verordnung erlangen schrittweise Gültigkeit. Ab dem 2. Februar 2025 gelten die Kapitel I und II der Verordnung. Kapitel I enthält neben allgemeinen Bestimmungen insbesondere die Festlegung, dass Anbieterinnen bzw. Anbieter und Betreiberinnen bzw. Betreiber von KI-Systemen Maßnahmen zu ergreifen haben, damit ihr Personal beim Betrieb und bei der Nutzung von KI-Sys-

1 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024).

temen über ein ausreichendes Maß an KI-Kompetenz verfügt. Der europäische Gesetzgeber versteht hierunter u. a. Fähigkeiten und Kenntnisse, um KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von Künstlicher Intelligenz und der Schäden, die sie verursachen kann, bewusst zu werden. Kapitel II umfasst verbotene Praktiken im KI-Bereich. Hierzu gehören z. B. bestimmte Systeme zur Bewertung oder Einstufung von Personen auf der Grundlage ihres sozialen Verhaltens, zur Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen sowie zur Kategorisierung von Personen aufgrund ihrer biometrischen Merkmale. Verboten ist in diesem Zusammenhang grundsätzlich auch, das Risiko, dass eine Person eine Straftat begeht, ausschließlich anhand ihres Verhaltens oder ihrer persönlichen Merkmale zu bestimmen. Ab dem 2. August 2025 gelten insbesondere Regelungen zu KI-Modellen mit allgemeinem Verwendungszweck (Kapitel V) sowie zur Benennung zuständiger Behörden etwa für die Marktüberwachung von KI-Systemen (Kapitel VII). Die restlichen Vorschriften werden ein bzw. zwei Jahre später wirksam.

KI – Datenschutzaufsicht gefordert

Gemäß Artikel 2 Absatz 7 KI-VO bleiben datenschutzrechtliche Vorschriften der Europäischen Union – insbesondere die Datenschutz-Grundverordnung und die Datenschutz-Richtlinie für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sowie die Strafvollstreckung (sogenannte JI-Richtlinie) – von der KI-Verordnung unberührt. Da eine große Zahl von KI-Systemen mit personenbezogenen Daten trainiert wird oder derartige Daten bei der Nutzung solcher Systeme verarbeitet werden, kommen auf die Datenschutzaufsichtsbehörden im Zusammenhang mit der KI-Verordnung erweiterte Aufgaben zu. Sie müssen sich um die neue Klasse der überaus komplexen und komplizierten KI-Systeme kümmern, Beschwerden betroffener Personen über KI-Systeme bearbeiten, datenschutzrechtliche Beratungen für die Entwicklung, den Betrieb und die Nutzung von KI-Systemen erbringen und ggf. Verstöße gegen das Datenschutzrecht sanktionieren. Auch unsere Behörde hat sich deshalb bereits mit dem Thema befasst.[2] Diese Aktivitäten wurden im Berichtsjahr fortgesetzt und intensiviert.

2 Tätigkeitsbericht Datenschutz 2023, A I 1.

Im Land Brandenburg (und nicht nur dort) bestehen große Erwartungen im Hinblick auf den Einsatz von Künstlicher Intelligenz. Die entsprechende Landesstrategie, die im Juni 2024 verabschiedet wurde und bei deren Erarbeitung unsere Behörde einbezogen wurde, beschreibt vorhandene Strukturen in Wissenschaft und Forschung, Unternehmen, Verwaltungen und Zivilgesellschaft, strategische Ziele für den KI-Einsatz in Brandenburg sowie eine Vielzahl konkreter Einzelmaßnahmen. Für den Zeitraum bis 2030 gibt sie einen Weg vor, KI-Aktivitäten zu koordinieren, bestehende Ansätze weiter auszubauen und vorhandene Lücken zu schließen, um die Potenziale von Künstlicher Intelligenz im Land stärker zu nutzen.

Der Landesbeauftragten sind im Berichtszeitraum eine Reihe von Projekten im Bereich Künstliche Intelligenz bekannt geworden, die bereits umgesetzt sind, an denen gearbeitet wird oder die aktuell geplant werden. Im Regelfall ist damit auch eine Verarbeitung personenbezogener Daten verbunden, sodass eine datenschutzrechtliche und technische Projektbegleitung und Bewertung der Datenverarbeitung angezeigt ist. Dies trifft in besonderem Maß bei KI-Systemen der Polizei oder der Justiz zu. Darüber hinaus haben uns erste Anfragen und Beschwerden betroffener Personen erreicht, die der Auffassung sind, dass ihre Daten in KI-Systemen des Landes verarbeitet werden.

Der rasche technologische Fortschritt auf dem Gebiet der Künstlichen Intelligenz und die zusätzlichen Anforderungen an die datenschutzrechtliche Aufsichtstätigkeit, die sich gegenwärtig durch den Einsatz von KI-Systemen bei öffentlichen und nicht öffentlichen Stellen im Land Brandenburg ergeben bzw. zukünftig ergeben werden, erzeugen einen Bedarf an zusätzlichen personellen und materiellen Ressourcen bei der Landesbeauftragten. Zahlreiche Fragen sowohl rechtlicher als auch technisch-organisatorischer Art zur Einhaltung der gesetzlichen Anforderungen bei der Entwicklung, beim Betrieb oder bei der Nutzung von KI-Systemen sind zu klären. Dies muss im Regelfall auch in enger Zusammenarbeit mit den anderen deutschen sowie den europäischen Datenschutzaufsichtsbehörden geschehen. Besondere Herausforderungen ergeben sich dabei durch die Neuheit des Gegenstandsbereichs „Künstliche Intelligenz“ sowie durch die Komplexität und Kompliziertheit der technischen KI-Systeme. All dies leistete die Landesbeauftragte in der Vergangenheit mit dem bestehenden Personal und ohne zusätzliche Ressourcen. Eine Verstetigung und Ausweitung der Aktivitäten der Datenschutz-

aufsicht im Bereich KI – wie bei der Umsetzung der Landesstrategie geboten – wird ohne eine entsprechende personelle und materielle Aufstockung unserer Behörde nicht möglich sein.

Gleiches gilt, falls der Gesetzgeber der Landesbeauftragten die vollständig neue Aufgabe der Marktüberwachung für Hochrisiko-KI-Systeme gemäß Artikel 74 Absatz 8 i. V. m. Anhang III Nummern 1, 6, 7 und 8 KI-VO überträgt. Hierbei geht es um die Marktüberwachung für bestimmte biometrische KI-Systeme sowie für KI-Systeme für Strafverfolgungszwecke, für Migration, Asyl und Grenzkontrolle sowie für Rechtspflege und demokratische Prozesse. Nach der genannten Vorschrift sind die Datenschutzaufsichtsbehörden für diese Aufgabe prädestiniert.

2 Mitwirkung in Arbeitsgremien der Datenschutzkonferenz

Bereits seit dem Jahr 2019 beschäftigt sich eine Arbeitsgruppe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) – die sogenannte Taskforce KI – mit den Auswirkungen der Entwicklungen im Themengebiet Künstliche Intelligenz (KI) auf den Datenschutz. Unsere Behörde ist seit Anbeginn aktives Mitglied dieser Gruppe.

Bereits im vorigen Berichtszeitraum erhielt die Taskforce von der Datenschutzkonferenz den Auftrag, Leitlinien für den datenschutzkonformen Einsatz von KI-Systemen zu erarbeiten. Verantwortlichen und Auftragsverarbeitern sollten hiermit Hilfestellungen für die Konzeption des Einsatzes, die Implementierung und die Nutzung von KI-Systemen gegeben werden. Die Arbeitsgruppe entschied sich, die Leitlinien basierend auf Vorarbeiten des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit als Checkliste zu formulieren und kurze Antworten auf relevante Fragestellungen zu geben. Aufgrund der parallel stattfindenden, vielfältigen Diskussionen zum Einsatz großer Sprachmodelle (Large Language Models, LLMs) lag der Schwerpunkt der Leitlinien auf entsprechenden Anwendungen. Offene Rechtsfragen[3] führten zu der Entscheidung, das Training von KI-Modellen vorerst nicht zu behandeln. Auch die Entwicklung von KI-Anwendungen stand zunächst nicht im Vordergrund der Betrachtungen.

Im Mai 2024 verabschiedete die Datenschutzkonferenz die Orientierungshilfe „Künstliche Intelligenz und Datenschutz“, die die bis dahin vorliegenden Ergebnisse der Taskforce zusammenfasst und in unserem Internetangebot veröffentlicht ist. Die anschließende öffentliche Diskussion sowie Beratungsanfragen an unsere Behörde zeigten, dass insbesondere das Interesse von Verantwortlichen an konkreten, auf ihre Bedürfnisse zugeschnittenen Hinweisen nur teilweise erfüllt werden konnte. Angesichts der Vielfalt des Themas, der hohen Dynamik der Entwicklungen im Bereich KI und einer Rei-

3 Siehe A I 3.

he offener Fragen hinsichtlich des Umgangs mit personenbezogenen Daten in KI-Systemen mussten einige Fragestellungen offenbleiben. Auch aus diesem Grund wurde die Orientierungshilfe als „lebendes Dokument“ angelegt. Neue Erkenntnisse sollen bei Bedarf ergänzt werden.

Ein weiterer Arbeitsschwerpunkt der Taskforce KI war die Koordinierung der Prüftätigkeit der deutschen Datenschutzaufsichtsbehörden gegenüber dem Unternehmen OpenAI zum System ChatGPT. Hierüber hatten wir bereits im vergangenen Tätigkeitsbericht informiert.[4] Im Berichtszeitraum stand zunächst die gemeinsame Auswertung der Stellungnahmen des Unternehmens auf entsprechende Anhörungen im datenschutzrechtlichen Aufsichtsverfahren im Mittelpunkt. Nachdem bekannt wurde, dass OpenAI im Februar 2024 eine Niederlassung in Irland eröffnet hatte und die Aufsichtszuständigkeit damit auf unsere irischen Kolleginnen und Kollegen übergegangen war, galt es, das weitere Vorgehen abzustimmen. Beabsichtigt ist, die Ergebnisse in die Diskussionen auf europäischer Ebene einzubringen. Dies betrifft insbesondere Fragen der Zulässigkeit der Nutzung personenbezogener Daten für das Training von KI-Systemen und der Einbeziehung von personenbezogenen Daten besonderer Kategorien im Training sowie die Bestimmung der hierfür anwendbaren Rechtsgrundlagen.

Aufsicht mit einheitlichem Standpunkt

Neben datenschutzrechtlichen Leitlinien für Anwenderinnen und Anwender von KI-Systemen, die in der oben genannten Orientierungshilfe der Datenschutzkonferenz zusammengefasst werden, sind auch Hinweise und Empfehlungen für Entwicklerinnen und Entwickler bzw. Anbieterinnen und Anbieter derartiger Modelle und Systeme von großer Bedeutung. Die frühzeitige Beachtung datenschutzrechtlicher und technischer Vorgaben ist eine Grundvoraussetzung, dass der spätere Einsatz eines KI-Modells bzw. eines KI-Systems rechtskonform erfolgen kann. Die Datenschutzkonferenz hat deshalb im Berichtszeitraum ihren Arbeitskreis Technik damit beauftragt, entsprechende Leitlinien zu erarbeiten. Ziel soll es sein, geeignete und angemessene technische und organisatorische

4 Tätigkeitsbericht Datenschutz 2023, A I 1.2.

Maßnahmen zu empfehlen, die sich an den einzelnen Phasen des Lebenszyklus eines KI-Systems und den Gewährleistungszielen des Standard-Datenschutzmodells orientieren. Geplant ist, das bereits im Jahr 2019 von der Datenschutzkonferenz veröffentlichte „Positionspapier zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen“ fortzuschreiben. Die Arbeiten dauerten zum Ende des Berichtszeitraums an.

Die wachsende Bedeutung des Themenfelds Künstliche Intelligenz und dessen Auswirkungen auf den Datenschutz erfordern, die Arbeit der Taskforce KI der Datenschutzkonferenz zu verstetigen und zu intensivieren. Zum Ende des Berichtszeitraumes beschloss die Konferenz deshalb, die Taskforce in einen regulären Arbeitskreis umzuwandeln. Kommende Arbeitsschwerpunkte werden u. a. Fragen des Umgangs mit (personenbezogenen) Trainingsdaten, der Auswirkungen eines rechtswidrigen Trainings auf die Rechtmäßigkeit des Einsatzes eines KI-Modells und möglicher kompensierender Maßnahmen sowie der Umsetzung von Betroffenenrechten beim Einsatz von KI-Systemen sein. Wegen der hohen Durchdringung vieler Themengebiete mit Künstlicher Intelligenz wird der neu gebildete Arbeitskreis auch anderen Arbeitskreisen der Konferenz beratend zur Seite stehen.

3 Datenschutzfragen bei der Entwicklung und Nutzung von KI-Modellen

Der Europäische Datenschutzausschuss (EDSA) veröffentlichte zum Ende des Berichtszeitraums auf Ersuchen der irischen Datenschutzaufsichtsbehörde (Data Protection Comission, DPC) eine Stellungnahme, die sich mit der Verwendung personenbezogener Daten für die Entwicklung von KI-Modellen und der anschließenden Nutzung dieser Modelle befasst.[5] Eine solche Stellungnahme nach Artikel 64 Absatz 2 Datenschutz-Grundverordnung (DS-GVO) betrifft Fragen von allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat und dient einer europaweit einheitlichen Rechtsanwendung. Die DPC hatte sich mit mehreren konkreten Fragen an den Ausschuss gewandt. Trotz der Komplexität der Thematik hatte dieser entsprechend Artikel 64 Absatz 3 Sätze 2 und 3 DS-GVO lediglich 14 Wochen Zeit für die Beantwortung. Zur Vorbereitung der Stellungnahme des Ausschusses stimmten sich die europäischen Datenschutzaufsichtsbehörden während dieses Zeitraums in einem ressourcenaufwändigen Konsultationsverfahren, das mehrere Arbeitsgremien einzubeziehen hatte, intensiv ab.

Im Wesentlichen befasst sich die Stellungnahme damit, wann ein KI-Modell als anonym angesehen werden kann, inwiefern ein berechtigtes Interesse gemäß Artikel 6 Absatz 1 Buchstabe f DS-GVO als Rechtsgrundlage für Datenverarbeitungen im Rahmen der Entwicklung oder Nutzung von KI-Modellen dienen kann und wie sich unrechtmäßige Datenverarbeitungen in der Trainingsphase auf die spätere Nutzung eines KI-Modells auswirken können.

Das Datenschutzrecht ist nur dann anwendbar, wenn personenbezogene Daten verarbeitet werden. Die erste Frage der DPC zur Anonymität zielte deshalb auf den Anwendungsbereich datenschutzrechtlicher Vorschriften im Kontext von KI ab. Gemäß der EDSA-Stellungnahme sind KI-Modelle, die mit personenbezogenen

5 Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, angenommen am 17. Dezember 2024.

Daten trainiert wurden, nicht in allen Fällen als anonym anzusehen. Vielmehr muss stets im Einzelfall entschieden werden, ob Anonymität vorliegt. Die Stellungnahme enthält Kriterien, die für eine entsprechende Einschätzung herangezogen werden können. Damit ein Modell als anonym bewertet werden kann, sollte es insbesondere sehr unwahrscheinlich sein, dass Personen, deren Daten zur Erstellung des Modells verwendet wurden, direkt oder indirekt identifiziert oder solche personenbezogenen Daten durch Abfragen aus dem Modell extrahiert werden können. Diese Klarstellung ist zu begrüßen, da sie auf die Gewährleistung von Rechten betroffener Personen zielt.

Zu der Frage, ob und inwieweit Verantwortliche Artikel 6 Absatz 1 Buchstabe f DS-GVO als Rechtsgrundlage für die Entwicklung und den Einsatz von KI-Modellen nutzen können, sieht die EDSA-Stellungnahme einen dreistufigen Test vor: Zunächst müssen berechtigte Interessen des Verantwortlichen für die Verarbeitung personenbezogener Daten im Kontext von KI vorliegen. Weiterhin ist zu prüfen, ob die Verarbeitung zur Erreichung der beabsichtigten Zwecke erforderlich ist, es also keine weniger eingriffsintensive Alternative gibt. Darüber hinaus ist eine Abwägung mit den berechtigten Interessen der betroffenen Personen vorzunehmen – deren Interessen dürfen nicht überwiegen. Insbesondere stehen ihre Rechte und Freiheiten einer Verarbeitung dann entgegen, wenn die Personen mit der Verwendung ihrer Daten vernünftigerweise nicht rechnen müssen. Insofern dürfen beispielsweise nicht alle im Internet verfügbaren personenbezogenen Daten ohne Weiteres für das Training von KI-Modellen genutzt werden. Bei der Berücksichtigung der Interessen der betroffenen Personen sind z. B. auch ihre Beziehungen zum Verantwortlichen, die Art der personenbezogenen Daten oder mögliche Verwendungen eines KI-Modells zu beachten.

Sofern ein KI-Modell unter Verstoß gegen das Datenschutzrecht trainiert wurde, ist der spätere Einsatz gemäß der EDSA-Stellungnahme nicht in jedem Fall ausgeschlossen. Eine Nutzung wäre etwa möglich, wenn ein unrechtmäßig trainiertes KI-Modell vor dem weiteren Einsatz einen Anonymisierungsprozess durchläuft. Die ursprüngliche Unrechtmäßigkeit der Datenverarbeitung in der Trainingsphase sollte dann aus datenschutzrechtlicher Sicht keine Auswirkungen auf die in der Anwendungsphase folgenden Datenverarbeitungen haben. Der Ausschuss verdeutlicht darüber hinaus auch, dass Verantwortliche bei der Auswahl und Nutzung eines KI-Modells, das

mit personenbezogenen Daten trainiert wurde, in jedem Fall erhöhte Sorgfaltspflichten z. B. zum Nachweis der Einhaltung von Artikel 5 Absatz 1 Buchstabe a und Artikel 6 DS-GVO erfüllen müssen.

Die Stellungnahme des Ausschusses richtet sich zwar an die zuständigen Datenschutzaufsichtsbehörden, lässt jedoch die Verpflichtungen der für die Verarbeitung Verantwortlichen sowie der Auftragsverarbeiter nach der Datenschutz-Grundverordnung unberührt. Gemäß Artikel 5 Absatz 2 DS-GVO müssen Verantwortliche die Einhaltung aller Grundsätze für die Verarbeitung personenbezogener Daten nachweisen können.

II Datenschutzverstöße: Maßnahmen und Sanktionen

1 Videoüberwachung in Gemeinschaftsunterkunft für Geflüchtete

Im Berichtsjahr konnte die Landesbeauftragte ein umfangreiches aufsichtsrechtliches Verwaltungsverfahren abschließen, das bereits mehrere Jahre zuvor begonnen hatte.[6] Schwerpunkt war die Verarbeitung personenbezogener Daten mittels Videoüberwachung in einer Gemeinschaftsunterkunft für Asylbewerberinnen und Asylbewerber durch eine öffentliche Stelle.

In der Gemeinschaftsunterkunft wurden das Außengelände und die in den Häusern liegenden Eingangs-, Treppen- und Flurbereiche, von denen die Zimmer der Bewohnerinnen und Bewohner abgehen, großflächig mit mehr als 100 Videokameras überwacht. Im Laufe des Verfahrens konnten wir nach intensivem Schriftwechsel und persönlichen Besprechungen mit dem Verantwortlichen u. a. erreichen, dass dieser die Erfassungsbereiche zahlreicher Videokameras durch Schwärzungen derjenigen Bildausschnitte, die besonders sensible Bereiche zeigten, zumindest teilweise einschränkte. Hierzu gehörten ein Teil der von den Fluren abgehenden Zimmertüren und große Flächen des Fußballplatzes. Außerdem erstellte der Verantwortliche ein Sicherheitskonzept, worin die datenschutzrechtlichen Rollen der einzelnen Akteurinnen und Akteure sowie die Rechtsgrundlagen und – differenziert nach den betroffenen Erfassungsbereichen – die Zwecke der Videoüberwachung benannt wurden.

Allerdings reicht auch die geänderte Videoüberwachung auf dem Gelände der Gemeinschaftsunterkunft noch zu weit. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten mittels Videoüberwachung kommt Artikel 6 Absatz 1 Buchstabe e Datenschutz-Grundverordnung (DS-GVO) i. V. m. § 28 Absatz 1 Branden-

6 Tätigkeitsbericht Datenschutz 2022, A IV 7.

burgisches Datenschutzgesetz (BbgDSG) in Betracht. Danach ist eine Videoüberwachung öffentlich zugänglicher Räume zulässig, wenn dies zur Erfüllung der Aufgaben der öffentlichen Stelle, zur Wahrnehmung des Hausrechts, zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigungen erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen.

Die Videoüberwachung in der Gemeinschaftsunterkunft dient nach den Angaben des Verantwortlichen als öffentlicher Stelle u. a. der Erfüllung der im Zusammenhang mit der vorläufigen Unterbringung stehenden Aufgaben nach dem Landesaufnahmegesetz. Bei der vorläufigen Unterbringung ist u. a. sicherzustellen, dass der Schutz des Familienlebens der untergebrachten Personen gewährleistet wird (§ 8 Absatz 5 Nummer 1 Landesaufnahmegesetz-Durchführungsverordnung – LAufnGDV). In Gemeinschaftsunterkünften ist zudem sicherzustellen, dass im Gefahrenfall eine unverzügliche Alarmierung der zuständigen Stellen gewährleistet ist (§ 9 Absatz 3 LAufnGDV). Der Verantwortliche listete zwar zahlreiche Vorkommnisse, wie Gesundheitsprobleme von Bewohnerinnen und Bewohnern, Notfälle, Körperverletzungen und Hausfriedensbruch, auf. Diese betrafen jedoch nicht alle räumlichen Erfassungsbereiche der Videoüberwachung. Insbesondere war eine erhöhte Gefährdungslage durch einschlägige Vorfälle mit Bezug auf die Eingangsbereiche zu den Zimmern sowie der Gemeinschafts- und Sozialräume auf den Fluren weder dargetan noch ersichtlich. Darüber hinaus sind Orte, die den untergebrachten Personen – darunter viele Familien – zu einem Austausch untereinander dienen oder dem Privatbereich zuzuordnen sind, grundsätzlich frei von einer Videoüberwachung zu halten, weil deren schutzwürdige Interessen dort überwiegen.

Nach Artikel 58 Absatz 2 Buchstabe f DS-GVO ist es der Aufsichtsbehörde gestattet, eine vorübergehende oder endgültige Beschränkung der Verarbeitung personenbezogener Daten, einschließlich eines Verbots, zu verhängen. Um die Datenverarbeitung durch Videoüberwachung in diesem Fall in Einklang mit den datenschutzrechtlichen Vorgaben zu bringen, erließ die Landesbeauftragte eine Anordnung. Diese enthält u. a. die Verpflichtung des Verantwortlichen, die Erfassungsbereiche der auf den Fluren der Gemeinschaftsunterkunft angebrachten Innenkameras so zu beschränken, dass die Eingangsbereiche zu allen von den Fluren abgehenden Zimmern sowie Gemeinschafts- und Sozialräumen der Bewohnerinnen und Be-

wohner in Gänze nicht mehr erfasst werden. Zudem verpflichtet der Bescheid den Verantwortlichen, die auf dem Gelände befindlichen Kinderwagenboxen aus dem Erfassungsbereich der Außenkameras auszunehmen. Soweit die Kameras durch den blickdurchlässigen Zaun angrenzende Grundstücke und öffentliches Straßenland erfassen, ist die Datenverarbeitung auf das Gelände der Gemeinschaftsunterkunft zu beschränken. Zudem ist die Videoüberwachung der Randbereiche des Sportplatzes außerhalb der Ruhezeit von 22 Uhr bis 6 Uhr unzulässig. Der Verantwortliche hat gegen den Bescheid Klage vor dem Verwaltungsgericht erhoben.

2 Videoüberwachung in einem Hotel

Eine Beschwerde richtete sich gegen mehrere auf dem Dach eines Hotelneubaus installierte Kameras, die u. a. Fenster, Terrassen und Balkone der umliegenden Gebäude erfassten. Aus der im Rahmen der Anhörung von der Geschäftsführung erteilten Auskunft ergab sich, dass mehr als 40 Kameras betrieben wurden, u. a. auch in der Lobby, in den Aufzügen, in allen Fluren, von denen die Zimmer abgehen, und im Außenbereich. Zweck der Videoüberwachung war der Schutz von Personen und vor Vandalismus. In einem Gespräch mit der Betreiberin in der Dienststelle erörterten wir den Sachverhalt anhand der eingereichten Screenshots und bewerteten die Überwachung aus datenschutzrechtlicher Sicht.

Die Verarbeitung personenbezogener Daten ist nach Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) nur zulässig, wenn die betroffenen Personen eingewilligt haben oder die Verarbeitung auf Grundlage einer gesetzlichen Erlaubnisnorm erfolgt. Als eine solche kommt hier nur Artikel 6 Absatz 1 Buchstabe f DS-GVO in Betracht. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, soweit dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

Im Ergebnis des Gesprächs bewerteten wir die umfassende Videoüberwachung der Lobby nebst der Aufenthaltsbereiche für Gäste als überwiegend datenschutzrechtlich unzulässig. Ähnlich wie in der Gastronomie halten sich die Besucherinnen und Besucher dort typischerweise über längere Zeit auf, sie lesen, warten oder unterhalten sich. Ein solches Verhalten ist ihrer Freizeitgestaltung zuzuordnen. Persönlichkeitsrechte sind hier besonders zu schützen. Eine Videoüberwachung kann die unbeeinträchtigte Kommunikation sowie den unbeobachteten Aufenthalt der Hotelbesucherinnen bzw. Hotelbesucher stören und intensiv in deren Rechte eingreifen.

Zulässig blieb im Eingangsbereich nur die Videoüberwachung der Zone vor dem Tresen während der Öffnungszeiten der Rezeption, wenn dort Bargeschäfte wie die Zahlung der Übernachtungskosten

abgewickelt werden. Das Lesegerät für Kartenzahlungen ist von der Videoüberwachung auszunehmen. Arbeitsplätze von Beschäftigten, insbesondere an der Rezeption hinter dem Empfangstresen, dürfen ohne Anlass nicht dauerhaft überwacht werden.

Die umfassende Videoüberwachung der Flure, von denen die Zimmer abgehen, war ebenfalls datenschutzrechtlich unzulässig. Es standen mildere Mittel zur Zweckerreichung zur Verfügung, beispielsweise die Einrichtung einer Zutrittsbeschränkung, sodass nur Gästen, die ein Zimmer in der entsprechenden Etage gemietet haben, der Zutritt zu der jeweiligen Etage möglich ist. Auch die Videoüberwachung der Gänge im Erdgeschoss und des Gästeaufzugs bewerteten wir mangels einschlägiger Vorkommnisse wie beispielsweise Eigentums- oder Körperverletzungsdelikte als datenschutzrechtlich unzulässig.

Im Außenbereich war die Videoüberwachung von Sitzgelegenheiten auf dem hoteleigenen Gelände unzulässig, da sich die Gäste dort zur ungezwungenen Kommunikation aufhalten. Dasselbe galt für die davor befindliche Rasenfläche, die Kinder zum Spielen nutzen.

Die Videoüberwachung auf dem Dach des Hotels war nur unter der Bedingung zulässig, den Erfassungsbereich auf die eigene Dachfläche zu beschränken und die Nachbarbebauung hiervon auszunehmen.

Die Betreiberin sagte bereits in dem ersten Gespräch zu, die Videoüberwachung aller Flurbereiche vor den Zimmern sofort außer Betrieb zu nehmen. Immerhin handelte es sich dabei um mehr als ein Drittel der installierten Kameras. Dennoch teilte sie im weiteren Verlauf des Verwaltungsverfahrens weder Änderungen im Bereich der Videoüberwachung mit, noch nahm sie inhaltlich Stellung zu den Ergebnissen des Besprechungstermins.

Hotelaufenthalt ohne Beobachtung

Auf Grundlage der vorliegenden Angaben und Feststellungen untersagten wir die Verarbeitung personenbezogener Daten mittels zahlreicher Kameras, u. a. in den Fluren vor den Zimmern, im Eingangsbereich nebst Lobby und Aufenthaltsarealen, in den Aufzugskabinen und im Bereich der Außensitzgelegenheiten. Zudem verpflichteten wir die Betreiberin, den Erfassungsbereich einer auf dem Dach des Hotelgebäudes befindlichen Kamera so einzuschränken, dass – über die eigene Dachfläche hin-

aus – Nachbargebäude mit Fenstern, Terrassen und Balkonen nicht mehr erfasst werden. Sie hat gegen den Bescheid Klage vor dem Verwaltungsgericht erhoben.

3 Videoüberwachung in Schwimmbädern

Die Videoüberwachung in Schwimmbädern ist regelmäßig Gegenstand unserer aufsichtsrechtlichen Tätigkeit. Im Berichtszeitraum konnten wir zwei Verwaltungsverfahren nach einer umfangreichen Anpassung der Videoüberwachung an die datenschutzrechtlichen Anforderungen abschließen. Gleichwohl sprachen wir wegen vorheriger Rechtsverstöße Verwarnungen aus.

In beiden Verfahren erhielten wir Beschwerden, in denen die Videoüberwachung von Umkleidebereichen moniert wurde. Bei dem ersten Fall handelte es sich um ein Erlebnisbad. Im Rahmen der Anhörung teilte der Verantwortliche mit, dass deutlich mehr als 20 Videokameras betrieben wurden. Sie seien nicht auf Umkleidekabinen, sondern auf die Schränke gerichtet, da diese des Öfteren aufgebrochen würden. Zudem seien Videokameras zur Unterstützung der Badaufsicht bei der Überwachung der Becken, der Rutschen und des Kinderspielplatzes in Betrieb, außerdem u. a. auf dem Außengelände und im Foyer. Der zweite Fall betraf ein kleineres, auch für den Schulsport genutztes Schwimmbad. Dort waren nach Angaben des Verantwortlichen 9 Kameras in Betrieb. Umkleiden würden nicht videoüberwacht. Die Kameras befänden sich im Bereich der Gästeschränke sowie der Schwimmbecken, im Foyer und auf dem Außengelände.

Die Verarbeitung personenbezogener Daten ist nach Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) nur zulässig, wenn die betroffenen Personen eingewilligt haben oder die Verarbeitung auf Grundlage einer gesetzlichen Erlaubnisnorm erfolgt. Grundsätzlich kann eine Verarbeitung personenbezogener Daten mittels Videoüberwachung in Schwimmbädern jedoch nicht auf Einwilligungen der betroffenen Gäste und Beschäftigten gestützt werden. Mithin war zu prüfen, ob die Datenverarbeitung auf Artikel 6 Absatz 1 Buchstabe f DS-GVO gestützt werden kann. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

In beiden Verfahren wurde jede Videokamera anhand der übermittelten Screenshots bewertet, wobei die verschiedenen Erfassungsbereiche differenziert zu betrachten waren. Zusammengefasst lässt sich sagen, dass eine Überwachung von Umkleiden datenschutzrechtlich nicht zulässig ist. Dies gilt auch für Schränke, es sei denn, aus Vorfällen in der Vergangenheit – beispielsweise Eigentumsdelikte – lässt sich ausnahmsweise auf eine erhöhte Gefährdungslage schließen oder die Gäste haben eine echte Wahlmöglichkeit zwischen einem videoüberwachten und einem nicht videoüberwachten Areal.

Umkleiden frei von Beobachtung

Im Beckenbereich überwiegen regelmäßig die Interessen der betroffenen Gäste, die sich in einem Schwimmbad zum Zweck der ungezwungenen Freizeitgestaltung aufhalten und in der Regel nur leicht bekleidet sind. Ausnahmsweise kann die Badaufsicht Flächen in Echtzeit beobachten, wenn diese nur schwer einsehbar sind und keine milderen Mittel zur Erreichung der verfolgten Zwecke – etwa zur Unfallprävention – zur Verfügung stehen (sogenanntes verlängertes Auge). Bereiche, die zu einem längeren Aufenthalt bestimmt sind, u. a. Ruhe- bzw. Liegezonen oder gastronomische Einrichtungen im Schwimmbad, dürfen dagegen regelmäßig nicht videoüberwacht werden. Außerhalb der Betriebszeiten der Schwimmbäder ist eine Videoüberwachung in der Regel aus datenschutzrechtlicher Sicht zulässig.

Nachdem wir eine erste Bewertung vorgenommen hatten, baute der Verantwortliche in dem Erlebnisbad bereits einige Kameras ab, schränkte den Erfassungsbereich anderer Kameras ein, verpixelte Aufnahmen der Gänge zwischen den Umkleideschränken teilweise und begrenzte den Betrieb verschiedener Kameras auf Zeiten, in denen sich in dem Erlebnisbad weder Gäste noch Beschäftigte aufhalten. In einer nachfolgenden Besprechung erörterten wir die darüber hinaus noch erforderlichen Anpassungen. Die Kameras in den Gängen vor den Umkleideschränken mussten entweder während der Betriebszeiten des Schwimmbads gänzlich abgeschaltet oder die Verpixelung erheblich erweitert werden. Alternativ kam die Einrichtung eines optisch getrennten, nicht videoüberwachten Bereichs in Betracht. Soweit im Einzelfall eine Videoüberwachung der Becken zulässig war, war diese auf ein Live-Monitoring der Wasserflächen einschließlich der Beckenränder zu beschränken. Weg- und Aufenthaltsflächen außerhalb der Becken mussten von der Videoüberwa-

chung ausgenommen werden. Eine Aufzeichnung und Speicherung von Videobilddaten im Beckenbereich während der Betriebszeiten des Schwimmbads war unzulässig. Dasselbe galt für die Überwachung des Kinderspielplatzes während der Betriebszeiten des Schwimmbades.

In dem kleineren, auch für den Schulsport genutzten Schwimmbad ergab sich Nachbesserungsbedarf. Die Aufnahmen der Bereiche vor den Schränken – insbesondere, soweit nicht sicher auszuschließen war, dass sich dort Personen umziehen – waren zu verpixeln oder die Kameras während der Betriebszeiten des Schwimmbades abzuschalten. Im Beckenbereich war das Live-Monitoring während der Betriebszeiten des Schwimmbads auf die Wasserflächen und Beckenränder zu begrenzen. Eine Aufzeichnung der Bilddaten war im Beckenbereich unzulässig. Die Verarbeitung personenbezogener Daten mittels der Außenkamera, die den Zugang zum Schwimmbad erfasste, war unzulässig.

In beiden Schwimmbädern wurde die Videoüberwachung im erforderlichen Umfang angepasst, sodass die Verarbeitung personenbezogener Daten nicht mehr zu beanstanden war. Die Landesbeauftragte sprach in beiden Verwaltungsverfahren eine Verwarnung gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO aus, soweit die Verarbeitung personenbezogener Daten mittels Videoüberwachung gegen den Grundsatz der Rechtmäßigkeit der Datenverarbeitung gemäß Artikel 5 Absatz 1 Buchstabe a i. V. m. Artikel 6 Absatz 1 DS-GVO verstoßen hatte. In beiden Verfahren sind keine Rechtsmittel eingelegt worden.

4 Unverzügliches Löschen von Nutzerdaten

Ein Nutzer einer Online-Plattform beschwerte sich bei uns, weil sein Nutzerkonto durch den Verantwortlichen nicht gelöscht wurde. Das Konto war bereits vor längerer Zeit gesperrt worden; er entschied sich jedoch erst deutlich später, die Gründe der Sperrung bei dem Verantwortlichen zu erfragen. Dieser bezog sich lediglich pauschal auf Sicherheitsüberprüfungen. Der Nutzer beantragte daraufhin die Löschung seiner Daten. Dies blieb jedoch erfolglos. Als Begründung hielt ihm das Unternehmen nur allgemeine Erwägungen zur Erforderlichkeit der weiteren Datenspeicherung entgegen.

Der Verantwortliche trug im Rahmen der Anhörung seine Motive für Kontosperrungen in für uns nachvollziehbarer Weise vor. Nach seiner Darstellung müssen solche Sperrungen in Verdachtsfällen schnell erfolgen, um eine sichere Nutzung der Plattform für alle Nutzerinnen und Nutzer zu ermöglichen und um betrügerische Angebote zu ihren oder zu Lasten Dritter zu verhindern. Konten werden daher mitunter auch vorsorglich gesperrt. Nutzerinnen und Nutzer, die der Meinung sind, zu Unrecht von einer Kontosperrung betroffen zu sein, haben die Möglichkeit, gegen diese vorzugehen. Sie können sich in solchen Fällen an den Kundenservice wenden, der durch Einsicht in die Protokolle den konkreten Sperrgrund erkennen und die Konten nach einer Überprüfung wieder freischalten kann. Hierfür ist es erforderlich, dass der Sperrgrund tatsächlich nicht vorliegt oder zwischenzeitlich entfallen ist. Um das festzustellen, ist jedoch in der Regel die Mitwirkung der Nutzerinnen und Nutzer notwendig.

Im vorliegenden Fall – so teilte uns das Unternehmen weiter mit – waren die Protokolldaten des Beschwerdeführers, die Auskunft über den genauen Grund der Sperrung seines Kontos hätten geben können, bereits gelöscht. Die internen Aufbewahrungsfristen für derartige Protokolle waren abgelaufen, da seit der Sperrung über ein Jahr vergangen war. Insofern konnte das Unternehmen auch uns gegenüber den Grund der Kontosperrung lediglich abstrakt benennen, genauere Einzelheiten lagen jedoch nicht mehr vor.

Das Löschbegehren des Beschwerdeführers war von einer Mitarbeiterin des Kundenservice fälschlicherweise und entgegen der internen Anweisungen zunächst abgelehnt worden. Auf erneute

Nachfrage hin wurde ihm zwar mitgeteilt, dass nun eine Löschung erfolgen würde. Dies geschah jedoch aufgrund menschlichen Versagens nicht, da weitere Beschäftigte des Kundenservice internen Anweisungen zum Vorgehen in diesen Fällen nicht nachkamen. Erst als Reaktion auf unser Anhörungsschreiben löschte das Unternehmen die Daten des Kunden – ca. 6 Monate nach dem ersten Antrag des Beschwerdeführers.

Der Verantwortliche räumte in seiner Stellungnahme ein, dass es in diesem Fall mehrmals zu Fehlern gekommen war. Es handele sich aber um einen Einzelfall; grundsätzlich seien intern datenschutzkonforme Prozesse implementiert und ihre Umsetzung werde regelmäßig überprüft. Er trug weiter vor, dass die entsprechenden Mitarbeiterinnen und Mitarbeiter des Kundenservice sowie deren Teamleitungen nachgeschult und an die Befolgung interner Anweisungen erinnert worden seien.

Gemäß Artikel 17 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) hat eine betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden. Der Verantwortliche ist seinerseits verpflichtet, personenbezogene Daten u. a. dann unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Dabei bedeutet das Wort „unverzüglich“, dass die Handlung ohne schuldhaftes Zögern auszuführen ist. Im Hinblick auf einen Löschantrag hat der Verantwortliche zudem der betroffenen Person gemäß Artikel 12 Absatz 3 DS-GVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Antragseingang mitzuteilen, welche Maßnahmen aufgrund des Antrags ergriffen wurden oder aus welchen Gründen der Antrag abgelehnt wird.

Im vorliegenden Fall hatte der Beschwerdeführer den Plattformbetreiber aufgefordert, sein Nutzerkonto zu löschen. Damit war die Grundlage der weiteren Verarbeitung seiner Daten entfallen. Sie waren für die Erfüllung des Nutzungsvertrags nicht mehr erforderlich. Der Verantwortliche hatte die personenbezogenen Daten somit zu löschen. Er verweigerte dies, nannte dem Beschwerdeführer jedoch keine konkreten Gründe für die Ablehnung des Löschbegehrens. Dadurch hatte dieser keine Möglichkeit, die Ablehnung nachzuvollziehen, sie zu überprüfen oder etwaige Missverständnisse zu beseitigen.

Nach unserer Einschätzung hätte der Verantwortliche dem Beschwerdeführer die Gründe für die Kontosperrung spätestens dann präzise mitteilen müssen, als er ihn über die Entscheidung informierte, die Löschung der Kundendaten nicht vorzunehmen. Nur dann hätte er auch nachweisen können, dass deren weitere Verarbeitung auf einer tragfähigen Rechtsgrundlage beruht und etwa zur Wahrung der berechtigten Interessen des Verantwortlichen bzw. Dritter erforderlich ist (und die Interessen des Betroffenen nicht überwiegen). Die ausbleibende Datenlöschung war insoweit ein Rechtsverstoß.

Zudem monierten wir, dass der Verantwortliche den Beschwerdeführer nicht über die Fristen aufgeklärt hatte, in denen er sich gegen die Sperrung seines Nutzerkontos hätte wehren und eine Überprüfung hätte veranlassen können. Zwar entsprechen die Festlegung und Umsetzung interner Löschfristen (wie hier bei den Gründen für eine Kontosperrung) den datenschutzrechtlichen Grundsätzen. Allerdings muss das Vorgehen transparent sein und darf nicht zur Verkürzung der Betroffenenrechte führen. Gemäß Artikel 12 Absatz 2 DS-GVO erleichtert der Verantwortliche betroffenen Personen die Ausübung ihrer Rechte. Die hierfür erforderlichen Informationen erteilt er nach Absatz 1 der Vorschrift in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Im Beschwerdefall gab es für den Nutzer mangels Kenntnis der konkreten Löschfristen keine Möglichkeit, die Handlungen des Plattformbetreibers zu überprüfen.

Daten: Wenn weg, dann weg

Wegen der datenschutzrechtlichen Verstöße haben wir den Verantwortlichen gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO verwarnt. Dabei fielen die deutliche Fristüberschreitung, das schuldhafte Zögern, die mehrfache Ablehnung des Löschbegehrens und die falsche Mitteilung der bevorstehenden Löschung erschwerend ins Gewicht. Der Beschwerdeführer wurde zudem nicht über konkrete Fristen für seine Mitwirkung informiert. Zu Gunsten des Verantwortlichen haben wir die erfolgten Nachschulungen des Personals, die internen Anweisungen zur zügigen Löschung, das Eingestehen der Fehler und das kooperative Verhalten im Verfahren berücksichtigt.

5 Bitte keine Werbung!

Auch im vergangenen Berichtszeitraum bildete der Umgang mit unerwünschter E-Mail-Werbung einen Schwerpunkt unserer Tätigkeit. Darüber hinaus ist die Zahl der Beschwerden über Werbemaßnahmen per SMS und WhatsApp gestiegen. Die betroffenen Personen sind teilweise in massivem Umfang mit Werbung konfrontiert. In vielen Fällen verstoßen Unternehmen dabei gegen ihre datenschutzrechtlichen Pflichten. Gegenüber den Verantwortlichen haben wir deswegen Verwarnungen gemäß Artikel 58 Absatz 2 Buchstabe b Datenschutz-Grundverordnung (DS-GVO) ausgesprochen. Dies gilt in allen nachfolgend geschilderten Beispielen.

5.1 Was ist Werbung?

Der Begriff der Werbung umfasst nach dem allgemeinen Sprachgebrauch alle Maßnahmen eines Unternehmens, die auf Förderung des Absatzes seiner Produkte oder Dienstleistungen gerichtet sind. Obwohl das Gesetz den Begriff an verschiedenen Stellen verwendet, gibt es keine einheitliche datenschutzrechtliche Definition. Nach Artikel 2 Buchstabe a Richtlinie 2006/114/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 ist Werbung „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern“. Diese Definition ist bemerkenswert weit und erfasst letztlich jede Äußerung, die unmittelbar oder mittelbar der Absatzförderung dient. Der Begriff der Direktwerbung bezeichnet einen Unterfall der Werbung, die eine unmittelbare Ansprache der Zielperson beinhaltet und damit stets datenschutzrelevant ist. Sie kann in unterschiedlicher Form und auf verschiedenen Kanälen erfolgen, z. B. postalisch, per E-Mail, Telefon, SMS oder Messenger-Dienst.

Ob es sich um eine Werbung im Sinne dieser Begriffsdefinition handelte, hatten wir in folgendem Fall zu bewerten: Ein Betroffener beschwerte sich bei uns, da er E-Mails an seine private E-Mail-Adresse von einem ihm bis dahin völlig unbekannten Unternehmen erhielt. In den E-Mails wurde er persönlich angesprochen und auf eine offene Stelle in der Tech- und Internetbranche bei einem anderen Unter-

nehmen aufmerksam gemacht. Im Rahmen der Anhörung trug der Verantwortliche vor, dass es sich bei der betreffenden E-Mail um ein Stellenangebot handele und nicht etwa um Werbung. Das Unternehmen ist auf die Rekrutierung von IT-Fachkräften spezialisiert und sucht nach eigenen Angaben hierfür in öffentlichen Netzwerken oder auf Webseiten nach Kontaktdaten. Für die Vermittlung bietet das Unternehmen eine Plattform an, auf der sich Expertinnen, Experten und Unternehmen dann vernetzen können. In den E-Mails wurde der Beschwerdeführer dazu eingeladen, die jeweilige Stellenanzeige in dem Jobportal anzusehen, wofür eine Anmeldung auf dem Portal erforderlich war. Mit den E-Mails wollte das Unternehmen auf seine Dienstleistung als Stellenvermittler hinweisen. Da die E-Mails zumindest auch dem Ziel dienten, diese Tätigkeit zu fördern, handelte es sich hierbei um Werbung. Die damit verbundene Verarbeitung der personenbezogenen Daten erfolgte ohne Rechtsgrundlage und war unzulässig.

5.2 Werbung auf Basis einer Einwilligung

Werbung ist im Rahmen der datenschutzrechtlichen Vorgaben erlaubt. Insbesondere ist sie nach Artikel 6 Absatz 1 Buchstabe a DS-GVO zulässig, wenn eine wirksame Einwilligung der betroffenen Person in Werbemaßnahmen vorliegt. Nach Artikel 4 Nummer 11 DS-GVO ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Einwilligung erlischt, sofern die betroffene Person sie widerruft. Im Falle von E-Mail-Werbung kann dies beispielsweise durch Abmeldung über einen vom Verantwortlichen bereitgestellten Link oder eine direkte, formlose Widerrufserklärung geschehen. Gemäß Artikel 7 Absatz 1 DS-GVO muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Dies gelingt nur bei guter Dokumentation der erteilten Einwilligungen und einem durchdachten Einwilligungsmanagement.

In einer großen Zahl von Fällen haben wir geprüft, ob die von den Werbemaßnahmen betroffenen Personen wirksam eingewilligt haben:

Uns erreichte beispielsweise die Beschwerde eines Betroffenen, der seit dem Jahr 2021 von einem Unternehmen durchschnittlich zwei unerwünschte Werbe-E-Mails pro Tag an seine private E-Mail-Adresse erhielt. Der Beschwerdeführer hatte sich nie für einen Newsletter des Unternehmens angemeldet oder anderweitig eine Einwilligung erteilt, mehrmals den Verantwortlichen kontaktiert und dem Erhalt von Werbe-E-Mails widersprochen. Trotzdem erhielt er sie weiterhin regelmäßig. Dies war rechtswidrig.

In einem weiteren Beschwerdefall verarbeitete ein Unternehmen die Daten des Beschwerdeführers zunächst rechtmäßig auf Grundlage einer Einwilligung zum Versand von Newslettern. Wir stellten jedoch fest, dass es die Verarbeitung fortsetzte, nachdem der Beschwerdeführer den Abmelde-Link betätigt hatte. Das Unternehmen sandte dem Beschwerdeführer anschließend weitere Werbe-E-Mails zu, obwohl er die Abmeldung noch mehrmals wiederholte. Erst nachdem er schließlich zusätzlich per E-Mail an den Datenschutzbeauftragten des Unternehmens den Widerruf erklärte und die Löschung seiner Daten verlangte, wurde sein Kontakt aus dem Newsletter-Verteiler gelöscht. Wir erkannten einen Verstoß gegen die Datenschutz-Grundverordnung. Mit der erstmaligen Austragung aus dem Newsletter über den Abmelde-Link in der E-Mail hatte der Beschwerdeführer seine Einwilligung in die Verarbeitung seiner Daten zu Zwecken des Newsletter-Versands widerrufen. Durch den Einwilligungswiderruf war gemäß Artikel 7 Absatz 3 Satz 2 DS-GVO die Rechtsgrundlage für die in Rede stehende Datenverarbeitung bereits ab diesem Zeitpunkt erloschen.

Werbung – ein häufiges Ärgernis

In anderen Fällen wurde das Merkmal der Freiwilligkeit der Einwilligung nicht hinreichend beachtet. Gemäß Artikel 7 Absatz 4 DS-GVO ist bei der Beurteilung insbesondere zu berücksichtigen, ob die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für dessen Erfüllung nicht erforderlich sind. Das Merkmal der Freiwilligkeit ist dann nicht gegeben, wenn das sogenannte Kopplungsverbot greift: Die betroffene Person muss die Möglichkeit haben, die Einwilligung zu verweigern, ohne dass ihr daraus Nachteile entstehen. In Fällen, in denen die Vertragserfüllung von der Einwilligung in die Datenverarbeitung abhängig gemacht wird, ist jedoch zu bezweifeln, ob die Einwilligung tatsächlich freiwillig erfolgt. Vor diesem Hintergrund ist zu beachten, dass eine Einwilligung in Werbemaßnahmen nicht durch diesel-

be Handlung erteilt werden kann, mit dem einem Vertragsabschluss oder den Allgemeinen Geschäftsbedingungen einer Dienstleistung zugestimmt wird. Allerdings können zusätzliche Leistungen wie Rabattierungen oder Gewährung von längeren Gewährleistungszeiten von einer Zustimmung in Werbemaßnahmen abhängig gemacht werden, da sie nicht dem eigentlichen Vertrag zuzurechnen sind.

Mit dem Kopplungsverbot hatten wir uns aus Anlass einer Beschwerde zu befassen: Der Beschwerdeführer hatte auf der Webseite eines Unternehmens seine E-Mail-Adresse angegeben, um eine der dort unentgeltlich angebotenen Bedienungsanleitungen herunterzuladen. Nur nach Setzen eines verpflichtenden Häkchens bei der Einwilligung zum Empfang eines Newsletters konnte die Bestellung aufgegeben werden. Nach Anklicken des Buttons „Jetzt kostenlos downloaden!“ erhielt der Beschwerdeführer eine E-Mail mit einem Link zum Herunterladen der Bedienungsanleitung, über den zugleich die Einwilligung in den Empfang des Newsletters bestätigt werden sollte. Die E-Mail enthielt auch den Hinweis, dass er die Nachricht ignorieren könne, wenn er den Newsletter nicht empfangen wolle. Der Beschwerdeführer erhielt daraufhin regelmäßig Werbe-E-Mails. Es ist jedoch nicht zulässig, eine Dienstleistung an den Empfang von Werbung zu koppeln. Die betroffene Person muss eine echte Wahl haben, die Einwilligung auch nicht zu erteilen. Wir haben deshalb festgestellt, dass in diesem Fall keine wirksame Einwilligung vorlag.

5.3 Werbung auf Basis einer Interessenabwägung

Unternehmen können sich auch auf Artikel 6 Absatz 1 Buchstabe f DS-GVO als Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu Werbezwecken stützen. Dies setzt voraus, dass die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Dem Erwägungsgrund 47 der Datenschutz-Grundverordnung ist zu entnehmen, dass Direktwerbung als eine dem berechtigten Interesse dienende Verarbeitung betrachtet werden kann.

Artikel 6 Absatz 1 Buchstabe f DS-GVO verlangt eine Abwägung im konkreten Einzelfall zwischen den Interessen des Verantwortlichen bzw. Dritten und der betroffenen Person. Ein bloßes Abstellen auf abstrakte oder vergleichbare Fälle ohne Berücksichtigung der

Besonderheiten des Einzelfalls – das heißt insbesondere des konkreten Werbevorhabens – genügt diesen Anforderungen nicht. In einer Vielzahl unterschiedlicher Beschwerdefälle haben wir daher überprüft, ob die Datenverarbeitung im Hinblick auf die Wahrung der berechtigten Interessen erforderlich war. Im Rahmen der Interessenabwägung nach Erwägungsgrund 47 der Datenschutz-Grundverordnung muss insbesondere die subjektive Erwartungshaltung der betroffenen Person berücksichtigt werden. Darüber hinaus gilt es zu prüfen, was objektiv vernünftigerweise erwartet werden kann. Von entscheidender Bedeutung ist, ob die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung im Rahmen des Kontaktes der betroffenen Person zu erwarten war oder nicht.

Kritisch sind insbesondere Fälle, in denen Unternehmen personenbezogene Daten beispielsweise durch die Nutzung einer sozialen Online-Plattform erhalten haben. Nutzerinnen und Nutzer sozialer Medien haben lediglich den Datenschutzbestimmungen der Plattform zugestimmt. Dritte, also z. B. werbende Unternehmen, können sich nicht auf eine in diesem Zusammenhang ggf. abgegebene Einwilligung berufen.

In einem Fall hatte der Beschwerdeführer Namen und E-Mail-Adresse in seinem Profil auf einer der Vernetzung von Software-Entwicklern dienenden Online-Plattform veröffentlicht. Ein Unternehmen nutzte diese Daten, um ihm Werbung zuzusenden. Uns gegenüber berief es sich darauf, dass der Beschwerdeführer seine Daten gerade zum Zweck der Kontaktaufnahme veröffentlicht habe. Darin sei eine Einwilligung in eine entsprechende Verarbeitung dieser Daten durch das Unternehmen zu sehen. Wir stellten jedoch fest, dass die Einwilligung des Beschwerdeführers – wenn überhaupt – nur gegenüber dem Betreiber der Plattform wirksam erteilt worden sein konnte. Eine Einwilligung gegenüber dem Unternehmen zum Zweck des Versands von Werbe-E-Mails hatte der Beschwerdeführer nicht erteilt. Auch die Interessenabwägung gemäß Artikel 6 Absatz 1 Buchstabe f DS-GVO erlaubte den Versand von Werbung nicht, da der Beschwerdeführer die Online-Plattform privat nutzte. In diesem Kontext musste er nicht erwarten, Ziel von Werbung eines Dritten zu werden. Die Verarbeitung seiner personenbezogenen Daten war damit nicht rechtmäßig.

5.4 Berücksichtigung wettbewerbsrechtlicher Regelungen

Im Rahmen der Interessenabwägung des Artikels 6 Absatz 1 Buchstabe f DS-GVO muss schließlich auch immer § 7 Absatz 3 Gesetz gegen den unlauteren Wettbewerb (UWG) Berücksichtigung finden. Sofern E-Mail-Adressen unmittelbar von Bestandskundinnen und -kunden im Zuge einer Vertragsbeziehung erhoben wurden, überwiegen die schutzwürdigen Interessen dieser Personen nach Artikel 6 Absatz 1 Buchstabe f DS-GVO regelmäßig dann nicht, wenn die in § 7 Absatz 3 UWG enthaltenen Voraussetzungen für elektronische Werbung kumulativ vorliegen.

Nach vorgenannter Vorschrift ist eine unzumutbare Belästigung bei Werbung unter Verwendung elektronischer Post dann nicht anzunehmen, wenn ein Unternehmen im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von Kundinnen und Kunden deren elektronische Postadresse erhalten hat. Darüber hinaus darf das Unternehmen die Adresse nur zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden. Die Art des Produktes muss also im Zusammenhang mit den bereits erworbenen Produkten stehen.

Unternehmen berücksichtigen die genannte Vorschrift häufig nicht: So haben wir einen Verantwortlichen verwarnt, der einem Kunden Angebote für Waren unterschiedlicher Produktkategorien, darunter Handstaubsauger, Espressomaschinen, Bierzapfanlagen und Smartwatches, zusandte, nachdem dieser einen Marderabwehrgürtel erworben hatte. Hier wurde nicht für ähnliche Produkte oder Dienstleistungen geworben. In einem anderen Fall hatte der Beschwerdeführer eine Gebrauchsanweisung für ein elektronisches Gerät heruntergeladen. In den anschließend erhaltenen Werbemails wurde jedoch für einen Kreditvergleich geworben. Auch hier bestand kein Zusammenhang mit der ursprünglichen Leistung.

In einem weiteren Fall erfuhr ein Beschwerdeführer durch eine Auskunft gemäß Artikel 15 DS-GVO, dass der Verantwortliche seine personenbezogenen Daten aus seinem öffentlich zugänglichen LinkedIn-Profil erhoben hatte. Der Verantwortliche gab an, dass er die Daten zum Zweck der „Kaltakquise“ im „B2B-Bereich“ (Business-to-Business-Bereich) erhoben habe. Er berief sich auf sein berechtigtes Interesse gemäß Artikel 6 Absatz 1 Buchstabe f DS-GVO als Rechtsgrundlage für die Verarbeitung. Die Verarbeitung

personenbezogener Daten zum Zweck der Direktwerbung kann nach Erwägungsgrund 47 der Datenschutz-Grundverordnung zwar grundsätzlich aufgrund eines berechtigten Interesses des Verantwortlichen erlaubt sein. Im Rahmen unserer Prüfung stellten wir jedoch fest, dass im vorliegenden Fall die schutzwürdigen Interessen der betroffenen Person unter Berücksichtigung des Gesetzes gegen den unlauteren Wettbewerb überwogen.

Selbst wenn Personen ihre Daten in sozialen Netzen anderen öffentlich zugänglich machen, dürfen diese – sofern nicht anderslautende Einstellungen vorgenommen und hiermit eine Einwilligung ausdrücklich erteilt wurde – gemäß § 7 Absatz 2 Nummer 2 UWG nicht für eine geschäftliche Kontaktaufnahme zu Werbezwecken verwendet werden. Dies gilt auch für Direktnachrichten im sozialen Netz, da diese elektronische Post im Sinne des Gesetzes darstellen.

Eine solche Datenverarbeitung unter Nutzung berufsbezogener Netzwerke zu Werbezwecken kann im Einzelfall auf Artikel 6 Absatz 1 Buchstabe f DS-GVO gestützt werden, wenn für den werbenden Verantwortlichen ein bestimmter Kontaktweg zu einer betroffenen Person nicht nach dem Gesetz gegen den unlauteren Wettbewerb verboten ist. Bei Werbung per elektronischer Post überwiegt das Interesse des Verantwortlichen, wenn die Voraussetzungen des § 7 Absatz 3 UWG vorliegen, ansonsten ist von einem überwiegenden Interesse der betroffenen Person auszugehen.

6 Krankentage im Dienstplan – trotz Einwilligung rechtswidrig

Im Rahmen einer Beschwerde wurde uns bekannt, dass ein Unternehmen für seine Beschäftigten monatlich Schichtpläne mit Angaben zur An- und Abwesenheit in den Räumlichkeiten der jeweiligen Abteilung aushängte. Die Beschäftigten hatten so ihren Arbeitsplan sowie die Abwesenheiten im Blick. Erkrankte jemand von ihnen, wurde der Schichtplan für diesen Tag handschriftlich mit dem Buchstaben „K“ ergänzt.

Das Unternehmen holte von den Beschäftigten im Rahmen der Aufnahme ihrer Tätigkeit Einwilligungen für diese Praxis ein. Das Formular enthielt Informationen über die ausgehängten Daten, den potenziellen Adressatenkreis, Hinweise zur Freiwilligkeit sowie zum Widerruf und seinen Folgen. Die Pläne waren ausweislich des Dokuments auch von Beschäftigten anderer Abteilungen einsehbar. Eine Einsichtnahme durch externe Dritte wurde ebenfalls nicht ausgeschlossen.

Das Aushängen der Schichtpläne und damit die Verarbeitung u. a. der krankheitsbedingten Abwesenheitstage der Beschäftigten des Unternehmens entsprach trotz Einwilligung nicht den gesetzlichen Anforderungen an den Datenschutz. Zwar kann eine Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe a Datenschutz-Grundverordnung (DS-GVO) rechtmäßig sein, wenn eine betroffene Person ihre Einwilligung hierzu erteilt hat. Allerdings waren im vorliegenden Fall die Einwilligungen nicht wirksam.

Nach Artikel 4 Nummer 11 DS-GVO ist eine Einwilligung der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Vorliegend fehlte es am Merkmal der Freiwilligkeit. Nach § 26 Absatz 2 Bundesdatenschutzgesetz (BDSG) sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungs-

verhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen, wenn die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung erfolgt. Freiwilligkeit kann gemäß § 26 Absatz 2 Satz 2 BDSG insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Diese Vorschrift gilt nach § 26 Absatz 3 Satz 2 BDSG auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 DS-GVO – wie vorliegend bei Gesundheitsdaten.

Keines der Regelbeispiele des § 26 Absatz 2 BDSG, wonach eine Freiwilligkeit angenommen werden kann, war im vorliegenden Fall erfüllt. Das Aushängen der Dienstpläne mit den angegebenen Krankheitstagen hatte für die Mitarbeiterinnen und Mitarbeiter weder einen rechtlichen noch einen wirtschaftlichen Vorteil. Die Dienstpläne dienten der Vorgabe der Arbeitszeiten für die Beschäftigten, sodass sie sich über ihre Schichten informieren und bei Bedarf einen Tausch mit Kolleginnen und Kollegen abstimmen konnten. Dass im Krankheitsfall Schichten durch andere Beschäftigte übernommen wurden, oblag allerdings der Organisation des Arbeitgebers und war nicht Aufgabe der Belegschaft, sodass hier kein Vorteil in der Eintragung der Krankheitstage in den Schichtplan für die Beschäftigten angenommen werden konnte. Auch verfolgten das Unternehmen und die beschäftigten Personen durch den Aushang der Krankheitstage keine gleichgelagerten Interessen.

„K“ wie krank – im Dienstplan tabu

Andere Gesichtspunkte, die für eine Freiwilligkeit sprachen, waren nicht ersichtlich. Vielmehr musste die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Personen sowie der Umstand berücksichtigt werden, dass die Einholung der Einwilligungserklärungen im Rahmen des „Welcome Day“ erfolgte. Dieser findet im betroffenen Unternehmen zwar immer erst nach der Unterzeichnung des Arbeitsvertrags statt, weshalb eine Kopplung mit der Einwilligungserklärung nicht zu konstatieren war. Jedoch möchten neue Mitarbeiterinnen und Mitarbeiter gerade zu Beginn des Arbeitsverhältnisses nicht negativ auffallen und sind trotz des Hinweises auf die Widerrufbarkeit und die Möglichkeit, die Einwilligung ohne Angabe von Gründen und ohne Nachteile zu verweigern,

eventuell diesbezüglich gehemmt. Hinzu kommt, dass das Abbilden von krankheitsbedingten Abwesenheiten ein nicht unerhebliches Diskriminierungspotenzial aufweist und die Daten deshalb besonders schutzwürdig sind. Im Beschäftigungsverhältnis kann es bei Kenntnisnahme der krankheitsbedingten Fehltage durch Kolleginnen und Kollegen zu Ausgrenzungen insbesondere von häufig bzw. lange erkrankten Beschäftigten kommen.

Hinzu kam, dass das Unternehmen keine Maßnahmen zur Sicherstellung der datenschutzkonformen Verarbeitung vorgenannter Beschäftigtendaten getroffen hatte, wie § 26 Absatz 3 Satz 3 i. V. m. § 22 Absatz 2 BDSG es verlangt. Vorkehrungen nach zuletzt genannter Vorschrift, insbesondere eine Beschränkung des Zugangs zu den personenbezogenen Daten, wurden nicht ergriffen und wären hier mit Blick auf den Sinn und Zweck des Aushangs auch nur schwer umsetzbar gewesen. Abteilungsfremde Personen als auch Unternehmensfremde hatten Zugang zum Aushang und konnten diesen so zur Kenntnis nehmen. Zudem war es problemlos möglich, die Beschäftigtendaten ohne Kenntnis der Betroffenen zu kopieren, zu fotografieren und weiterzuverarbeiten.

Aufgrund der Feststellung, dass das Unternehmen durch den Aushang der Schichtpläne, aus denen die krankheitsbedingten Abwesenheiten der Beschäftigten ersichtlich waren, unter Verstoß gegen den Grundsatz der Rechtmäßigkeit der Datenverarbeitung gemäß Artikel 5 Absatz 1 Buchstabe a i. V. m. Artikel 6 Absatz 1 DS-GVO personenbezogene Daten an Dritte übermittelt hat, sprachen wir gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO eine Verwarnung aus. Aufgrund der ausgesprochen guten Kooperation sowie des sofortigen Herstellens eines datenschutzgerechten Zustandes durch das Unternehmen sahen wir eine Verwarnung als ausreichendes, wenn auch nötiges Mittel, um den Verstoß gegen geltendes Recht zu ahnden und einer Wiederholung vorzubeugen.

7 Meldedaten Minderjähriger für Wahlwerbung

Ein Fehler in der Vorbereitung zur Landtagswahl 2024 führte zu einer unzulässigen Datenübermittlung in erheblichem Umfang. Kurz vor der Wahl informierte uns eine kreisangehörige Stadt, dass eine Partei auf Grundlage von § 50 Absatz 1 Bundesmeldegesetz (BMG) beantragt hatte, die Datensätze der in der Stadt gemeldeten Erstwählerinnen und Erstwähler zu erhalten. Die Meldebehörde hatte aber das als Kriterium für die Gruppenauskunft herangezogene Geburtsdatum versehentlich so gesetzt, dass unzulässigerweise auch Daten von etwa 1.500 Personen übermittelt wurden, die noch nicht wahlberechtigt waren.

Da die Partei nach der gesetzlichen Vorgabe keine Geburtsdaten erhalten durfte und auch nicht erhalten hat, konnte sie den Fehler nicht selbst erkennen und verwendete die Daten wie beabsichtigt zur Wahlwerbung. Wir erfuhren von dem Sachverhalt durch die Meldung einer Datenschutzverletzung gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) sowie durch Beschwerden von Eltern.

Die Stadt meldete den Vorfall fristgerecht, nachdem sie ihn festgestellt hatte. Sie forderte die Partei auf, die dort noch gespeicherten Daten zu löschen. Dieser Aufforderung kam die Partei umgehend nach. Im Rahmen der Meldung teilte die Stadt mit, für die Zukunft das Vier-Augen-Prinzip bei der Selektion und dem Versand der Daten einführen zu wollen. Dies kann bei konsequenter Umsetzung ein wirksames Mittel sein, um solche Fehler zu vermeiden.

Wir hielten es aus mehreren Gründen für geboten, den Rechtsverstoß der unzulässigen Datenübermittlung gegenüber der Stadt zu sanktionieren: Erstens bewegte sich die Anzahl der fehlerhaft herausgegebenen Datensätze im vierstelligen Bereich und war damit außerordentlich hoch – im Meldewesen nach unserer Erfahrung eine seltene Ausnahme. Zweitens waren alle betroffenen Personen minderjährig und somit nach den Wertungen des europäischen Datenschutzrechts besonders schutzwürdig. Drittens ließ sich der Verstoß auch durch die umgehend ergriffenen Maßnahmen der Stadt nicht mehr rückgängig machen. Eine Einstellung des Verfahrens kam auf-

grund der Schwere des Verstoßes nicht in Betracht. Insofern blieb der Landesbeauftragten nur der Erlass einer Verwarnung nach Artikel 58 Absatz 2 Buchstabe b DS-GVO.

8 Bericht der Bußgeldstelle

8.1 Zweckwidrige Nutzung von Zeugendaten durch Polizisten

Ein Polizeibediensteter war von einer durch ihn vernommenen Zeugin derart angetan, dass er ihre im Rahmen der Zeugenvernehmung erhaltenen Daten im Anschluss zu privaten Kontaktversuchen nutzte. Als die Zeugin auf seine WhatsApp-Nachricht nicht reagierte, schickte er ihr am Folgetag eine weitere Nachricht sowie zwei Freundschaftsanfragen über Facebook. Darüber hinaus folgte er der Zeugin auf der Plattform Instagram, worüber er ihr einen Smiley schickte. Einen Tag später verschickte er auch noch über Snapchat eine Freundschaftsanfrage. Die Zeugin war von den hartnäckigen Kontaktversuchen alles andere als begeistert.

Wir leiteten ein Bußgeldverfahren gegen den Polizeibediensteten wegen der unrechtmäßigen Verarbeitung personenbezogener Daten ein. Denn nach § 32 Absatz 1 Nummer 1 Brandenburgisches Datenschutzgesetz handelt u. a. ordnungswidrig, wer entgegen den Vorschriften der Datenschutz-Grundverordnung, des Brandenburgischen Datenschutzgesetzes oder einer anderen Datenschutzvorschrift, personenbezogene Daten, die nicht offenkundig sind, verwendet.

Bei dem Namen und der Telefonnummer der Zeugin handelt es sich um personenbezogene Daten, nämlich um Einzelangaben über die persönlichen Verhältnisse einer bestimmten natürlichen Person. Die Daten der Zeugin waren nicht offenkundig, da sie diese im Rahmen ihrer Vernehmung ausschließlich der Polizei zur Verfügung gestellt hatte und die Nutzung auf polizeiinterne Zwecke zu begrenzen war. Indem der Polizeibedienstete der Zeugin Nachrichten auf ihr Mobiltelefon schickte, ihren Namen in den sozialen Medien Facebook, Instagram und Snapchat suchte und die daraufhin angezeigten Profile der Zeugin kontaktierte, verwendete er ihre Daten.

Hierfür gab es keinen dienstlichen Anlass. Die Polizei kann rechtmäßig erlangte personenbezogene Daten nur unter den in § 39 Absatz 1 Satz 1 Brandenburgisches Polizeigesetz genannten Voraussetzungen nutzen, etwa soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Die Verwendung der Daten durch den Polizeibediensteten ziel-

te dagegen auf eine Kontaktaufnahme mit der Zeugin aus privaten Interessen.

Sein vorsätzliches Handeln stellte im Ergebnis einen datenschutzrechtlichen Verstoß dar, der mit einer Geldbuße in dreistelliger Höhe geahndet wurde. Dabei wurden insbesondere das hartnäckige Vorgehen sowie die Tatsache berücksichtigt, dass Verstöße dieser Art in hohem Maß geeignet sind, das Vertrauen der Allgemeinheit in die Rechtmäßigkeit des Umgangs mit personenbezogenen Daten durch die damit befassten öffentlichen Stellen empfindlich zu beeinträchtigen. Der Polizeibedienstete akzeptierte die Geldbuße.

8.2 Tausende polizeiinterne Dateien auf private Festplatte kopiert

Ein leitender Polizeibeamter kopierte 5.466 Dateien von seinem Dienstrechner auf eine private USB-Festplatte. Darunter befanden sich insbesondere Listen mit Angaben zu Beschuldigten, Geschädigten und Zeuginnen und Zeugen, u. a. Geburtsdaten, Adressen und Aktenzeichen, sowie Vernehmungsprotokolle. Ferner enthielten die kopierten Daten die Adressen und Telefonnummern von Mitarbeiterinnen und Mitarbeitern des Polizeipräsidiums sowie Angaben zu deren Gesundheit und dienstliche Beurteilungen. Außerdem kopierte er Schulungsunterlagen zum Thema Kinderpornografie mit einschlägigem Bildmaterial. Auf der privaten Festplatte befanden sich zudem Schadsoftware sowie diverse private Unterlagen, Spiele, Filme und Programme.

Die Polizei meldete uns diesen Datenschutzvorfall.[7] Wir leiteten ein Bußgeldverfahren gegen den Beamten wegen der unrechtmäßigen Verarbeitung personenbezogener Daten ein. Denn nach § 32 Absatz 1 Nummer 1 Brandenburgisches Datenschutzgesetz handelt u. a. ordnungswidrig, wer entgegen den Vorschriften der Datenschutz-Grundverordnung (DS-GVO), des Brandenburgischen Datenschutzgesetzes oder einer anderen Datenschutzvorschrift personenbezogene Daten, die nicht offenkundig sind, speichert. Bei den Angaben zu Beschuldigten, Geschädigten und Zeuginnen bzw. Zeugen, zu Mitarbeiterinnen und Mitarbeitern des Polizeipräsidiums

7 Siehe B 1.

sowie bei den Schulungsunterlagen zum Thema Kinderpornografie mit einschlägigem Bildmaterial, das auch Gesichter zeigt, handelt es sich um personenbezogene Daten. Diese waren nicht offenkundig, da der Zugang zu den Daten ausschließlich polizeiintern und selbst innerhalb der Polizei nur mit besonderer Berechtigung möglich ist.

Die Polizei kann gemäß § 39 Absatz 1 Satz 1 Brandenburgisches Polizeigesetz rechtmäßig erlangte personenbezogene Daten in Akten oder Dateien speichern, verändern und nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Sie ist dabei als Verantwortlicher nach § 3 Nummer 6 und § 17 Absatz 1 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz sowie nach Artikel 5 Absatz 1 Buchstabe f und Artikel 32 Absatz 1 Halbsatz 1 DS-GVO verpflichtet, personenbezogene Daten so zu verarbeiten, dass ihre Sicherheit, insbesondere Vertraulichkeit und Integrität, gewährleistet ist. Die Daten müssen durch geeignete technische und organisatorische Maßnahmen geschützt sein. Die Richtlinie „externe Speichermedien“ der brandenburgischen Polizei sieht daher unter Nummer 4 ausdrücklich vor, dass zur Verarbeitung dienstlicher Daten ausschließlich dienstliche Speichermedien verwendet werden dürfen.

Der Polizeibeamte kopierte die dienstlichen Daten allerdings entgegen dieser Richtlinie auf seine private Festplatte, auf der sich neben Schulmaterial seines Kindes und Steuerunterlagen auch diverse (Kinder-)Filme, Spiele und Programme befanden. Die Daten hätten damit einem erhöhten Risiko unberechtigten Zugriffs und unberechtigter Verarbeitung, insbesondere durch die Familie des Polizeibediensteten, ausgesetzt sein können, wenn die Festplatte in der privaten Sphäre genutzt worden wäre. Da sie zudem Schadsoftware enthielt, hätten polizeiliche Daten beschädigt oder zerstört werden können. Hinzu kommt, dass bei Wechseldatenträgern das Risiko von Datenverlusten etwa durch Diebstahl höher ist als bei stationären IT-Systemen. Im Ergebnis war der Polizeibeamte nicht befugt, dienstliche Dateien auf seiner privaten Festplatte zu speichern. Unabhängig davon, ob er die Absicht hatte, die Daten zu beruflichen Zwecken zu nutzen, war somit bereits das Speichern der dienstlichen Dateien auf der privaten Festplatte nicht zulässig.

Don’t bring your own device

Der Polizeibeamte entschied sich bewusst dazu, die dienstlichen Daten auf seine private Festplatte zu kopieren. Dabei wusste er, dass dies nicht erlaubt war. Sein vorsätzliches Handeln stellte im Ergebnis einen datenschutzrechtlichen Verstoß dar, der mit einer Geldbuße in vierstelliger Höhe geahndet wurde. Dabei wurde insbesondere die große Anzahl an Dateien und betroffenen Personen berücksichtigt. Daneben fiel schwer ins Gewicht, dass es sich um äußerst sensible Daten wie Gesundheitsdaten handelte, die bei Kenntniserlangung durch Unbefugte zum Nachteil der betroffenen Personen hätten eingesetzt werden können. Der Polizeibedienstete ließ sich geständig ein, was sich mildernd auf die Bußgeldhöhe auswirkte. Er akzeptierte das Bußgeld.

8.3 Unberechtigter Versand von Newslettern

Ein deutschlandweit agierendes Augenoptik-Unternehmen verschickte über einen Zeitraum von neun Monaten 63 Werbe-E-Mails an einen Kunden, der die Einwilligung in die Nutzung seiner E-Mail-Adresse zu Werbezwecken bereits dreieinhalb Jahre zuvor widerrufen hatte.

Auf seine Beschwerde hin hörten wir das Unternehmen im aufsichtsrechtlichen Verfahren an. Es teilte uns mit, ein Fehler bei der Datenmigration auf eine neue Plattform habe dazu geführt, dass die E-Mail-Adresse des Kunden wieder in den Verteiler aufgenommen wurde. Zwar gab es an, den Fehler behoben zu haben, jedoch entfernte das Unternehmen die E-Mail-Adresse nicht aus dem Newsletter-Verteiler. Dies geschah erst, als der Kunde sich erneut bei der Landesbeauftragten beschwerte und diese das Verfahren wieder aufgriff. Die Verarbeitung der E-Mail-Adresse als personenbezogenes Datum erfolgte in den neun Monaten unbefugt, da für ihre Verwendung keiner der in Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) genannten Erlaubnistatbestände erfüllt war. Wir leiteten deshalb ein Bußgeldverfahren ein.

Das Unternehmen hatte die Verarbeitung ausdrücklich auf die Einwilligung des Kunden nach Artikel 6 Absatz 1 Buchstabe a DS-GVO gestützt, welche dieser im Rahmen der Registrierung erteilt hatte. Gemäß Artikel 7 Absatz 3 DS-GVO hat die betroffene Person jedoch das Recht, ihre Einwilligung jederzeit zu widerrufen. Dies war in diesem Fall erfolgt. Der Kunde widerrief die erteilte Einwilligung in die Nutzung seiner E-Mail-Adresse zu Werbezwecken durch die

Abmeldung vom Newsletter-Versand. Damit entfiel die Einwilligung als Rechtsgrundlage für zukünftige Werbe-E-Mails. Es gab für den Kunden daher keinen Grund, sich erneut oder gar wiederholt über den in den Werbe-E-Mails vorgehaltenen Link vom Newsletter abzumelden. Die Möglichkeit, sich abzumelden, enthebt den Verantwortlichen nicht seiner gesetzlichen Verpflichtung zu prüfen, ob die Newsletter nach einem erkannten Fehler noch auf der Grundlage einer Einwilligung versendet werden dürfen. In einem solchen Fall muss er gemäß Artikel 7 Absatz 1 und Artikel 5 Absatz 2 DS-GVO das Vorliegen der Einwilligung auch nachweisen können. Der Verantwortliche kann nicht entgegen der gesetzlichen Bestimmungen erwarten und darauf vertrauen, dass sich die Empfängerinnen und Empfänger nach technischen Fehlern erneut vom Newsletter-Versand abmelden. Vielmehr ist er selbst dazu verpflichtet, sicherzustellen, dass die Abmeldung nach Widerruf der Einwilligung unverzüglich erfolgt und in der Folge keine weiteren Werbe-E-Mails verschickt werden.

Durchblick bei Werbung behalten

Die Tathandlung erfolgte grob fahrlässig: Das Unternehmen hatte es versäumt, den Kunden vom Newsletter-Versand abzumelden, obwohl es bereits im Rahmen der ersten Anhörung durch die Landesbeauftragte darauf aufmerksam gemacht worden war, dass der Kunde trotz Widerrufs seiner Einwilligung weiterhin Werbe-E-Mails erhielt, und es in seiner Stellungnahme angegeben hatte, den Migrationsfehler erkannt und behoben zu haben.

Das Unternehmen war wegen ähnlicher Verstöße bereits mehrfach im Fokus der Landesbeauftragten. Zudem zeigte es sich im Rahmen des Beschwerdeverfahrens bei der Aufklärung des Sachverhalts und der Abstellung des Verstoßes wenig kooperativ. Das Verhalten des Unternehmens gebot es daher, eine Geldbuße als eindeutige Pflichtenmahnung zu verhängen, um für die Zukunft auf ein rechtstreues Handeln hinzuwirken. Artikel 83 Absatz 1 DS-GVO bestimmt, dass die Geldbuße in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein muss. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag waren die Kriterien des Artikels 83 Absatz 2 DS-GVO gebührend zu berücksichtigen. So war für unsere Entscheidung insbesondere von Bedeutung, dass das grob fahrlässige Verhalten des Unternehmens erhebliche Nachlässigkeit und auch Gleichgültigkeit hinsichtlich der Einhaltung datenschutzrechtlicher Anforderungen erkennen ließ. Aufgrund des Verstoßes

wurde der Kunde erheblich belästigt und in sein allgemeines Persönlichkeitsrecht eingegriffen.

Die Landesbeauftragte verhängte gegen das Unternehmen ein Bußgeld in fünfstelliger Höhe. Der Bescheid ist noch nicht rechtskräftig.

III Anlasslose Prüfungen

1 Europaweite Prüfung zur Umsetzung des Auskunftsrechts

Im Berichtszeitraum beteiligten wir uns an der koordinierten Prüfaktion (Coordinated Enforcement Framework, CEF) der Datenschutzaufsichtsbehörden im Europäischen Wirtschaftsraum. Diese seit 2022 jährlich durchgeführten Prüfungen stellen einen Teil der Strategie des Europäischen Datenschutzausschusses (EDSA) dar, um die Zusammenarbeit, den Informationsaustausch sowie die einheitliche Durchsetzung des Datenschutzrechts unter den Datenschutzaufsichtsbehörden zu fördern. Im Oktober 2023 wurde als Schwerpunkt für die dritte Aktion dieser Art die Umsetzung der Auskunftsrechte für betroffene Personen festgelegt. Konkret wurde ein Fragebogen mit dem Ziel abgestimmt, festzustellen, wie gut Verantwortliche in der Praxis das Auskunftsrecht umsetzen bzw. an welchen Stellen Probleme auftreten. Auf Grundlage der Ergebnisse sollten die Datenschutzaufsichtsbehörden auch bestimmen können, welcher Bedarf an konkreten Hilfestellungen oder Maßnahmen bei den betroffenen Personen bzw. Verantwortlichen besteht. Weiterhin war beabsichtigt, Erkenntnisse der Prüfung in die ESDA-Leitlinien zum Thema Auskunftsrecht[8] aufzunehmen.

Das Auskunftsrecht ist in Artikel 15 Datenschutz-Grundverordnung (DS-GVO) verankert und ermöglicht einer betroffenen Person, von einem Verantwortlichen zu erfahren, welche ihrer personenbezogenen Daten er verarbeitet. Darüber hinaus müssen auch allgemeine Informationen über die konkreten Verarbeitungstätigkeiten zur Verfügung gestellt werden, z. B. über die Verarbeitungszwecke, Empfängerinnen und Empfänger der Daten oder die Speicherdauer bzw. Löschfrist. Somit ermöglicht das Auskunftsrecht einer Person nicht nur, sich über die Verarbeitung ihrer eigenen Daten bewusst zu

8 Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht (Version 2.1), angenommen am 28. März 2023.

werden. Es versetzt sie auch in die Lage, weitere Betroffenenrechte wie das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung wahrzunehmen. Verantwortliche haben bei der Erteilung der Auskunft an eine betroffene Person neben den allgemeinen Modalitäten zur Umsetzung der Betroffenenrechte nach Artikel 12 DS-GVO auch zu berücksichtigen, dass die Auskunftserteilung selbst eine Verarbeitung personenbezogener Daten darstellt und daher die Anforderungen der Datenschutz-Grundverordnung zu beachten sind. Eine Herausforderung besteht etwa darin, dass zur Auskunftserteilung alle Daten einer Person, die von dem Verantwortlichen verarbeitet werden, zusammengeführt werden. Daraus kann sich ein besonderes Risiko ergeben, welches bei der Planung und Umsetzung der Auskunftsprozesse berücksichtigt werden muss.

Auf Auskunft gut vorbereitet sein

Im Rahmen der Prüfaktion waren wir frei bezüglich der Auswahl der Verantwortlichen in unserem Zuständigkeitsbereich. Wir haben uns auf Institutionen im Bereich der Versicherungs- und Kreditwirtschaft im Land Brandenburg mit mittlerer bis hoher Kundenzahl konzentriert und einige stichprobenartig ausgewählt. Die Verantwortlichen waren sehr kooperativ bei der Beantwortung des europaweit abgestimmten Fragebogens; die gewonnenen Erkenntnisse konnten wir gut in den Abschlussbericht einbringen.

Auffällig war, dass viele Verantwortliche Schwierigkeiten bei der Auskunft über solche personenbezogenen Daten haben, die nur für einen kurzen Zeitraum gespeichert werden. Sie erkannten nicht, dass sich eine Rechtsgrundlage für die weitere Speicherung der beauskunfteten Daten aus den rechtlichen Pflichten im Zusammenhang mit der Auskunftserteilung selbst ergibt (z. B. Rechenschaftspflicht). Die Verantwortlichen sind daher berechtigt und verpflichtet, die nur kurzfristig vorgehaltenen Daten vorübergehend länger zu speichern, wenn diese Daten Teil einer Auskunft an die betroffene Person sind.

Eine weitere Schwierigkeit zeigte sich bei der Bestimmung der Speicherfrist. Nachdem Verantwortliche einer Person Auskunft erteilt hatten, bewahrten sie zur Erfüllung ihrer Rechenschaftspflicht und im Hinblick auf zu erwartende Rechtsstreitigkeiten die Kommunikation und die erteilten Auskünfte richtigerweise getrennt von den anderen Kundendaten auf. Dabei stellten wir jedoch fest, dass die Aufbewahrungsfristen der Verantwortlichen ohne ersichtlichen Grund zwischen drei und zehn Jahren variierten. Gerade vor dem

Hintergrund, dass es sich hier um eine Anhäufung personenbezogener Daten aus unterschiedlichen Verarbeitungskontexten handeln kann, sollte dem Grundsatz der Speicherbegrenzung in besonderem Maße Rechnung getragen werden. Wir werden Verantwortliche zu diesem Thema weiter sensibilisieren und halten die Entwicklung einheitlicher Kriterien für erforderlich.

Eine besondere Herausforderung für die Verantwortlichen besteht darin, dass Auskunftsanträge formlos über unterschiedliche Kommunikationskanäle eingehen können und nicht immer sofort als solche erkannt werden. Es hat sich jedoch gezeigt, dass Verantwortliche, die diese verschiedenen Möglichkeiten in ihren internen Prozessen berücksichtigen, weniger Probleme bei der Zuordnung haben. Hinsichtlich der Ausgangskanäle für die Auskunft sollten die Verantwortlichen die Wünsche der Antragstellerinnen und Antragsteller berücksichtigen, soweit dem nicht Gründe der Datensicherheit o. ä. entgegenstehen. Insbesondere darf der Zugang zu den Auskünften nicht durch besondere Vorgaben, wie etwa die Pflicht zur Einrichtung eines Benutzerkontos, limitiert werden.

Unter bestimmten rechtlichen Voraussetzungen kann die Auskunftserteilung durch den Verantwortlichen eingeschränkt oder sogar verweigert werden. Wir haben in der Prüfung jedoch festgestellt, dass die Verantwortlichen die Voraussetzungen unterschiedlich auslegen. So ist die Verfolgung datenschutzfremder Zwecke mit einer Auskunft nicht automatisch ein Grund für eine Auskunftsverweigerung. Auch die Regelung von Artikel 12 Absatz 5 DS-GVO zu offensichtlich unbegründeten oder exzessiven Anträgen wird in diesem Zusammenhang häufig zu weit ausgelegt. Die Rechtsprechung hat dies mittlerweile klargestellt.[9] Dagegen kann ein Grund für eine Einschränkung der Auskunft dann vorliegen, wenn Daten anderer Personen offenbart werden müssten. Ein häufiges Spannungsfeld sind z. B. Auskünfte über Zugriffe von Beschäftigten auf Daten der Antragstellerinnen bzw. Antragsteller. Hier sind immer Einzelfallentscheidungen zu treffen, in denen die einander entgegenstehenden Rechte abgewogen werden müssen.[10] Wichtig ist, dass die getroffene Entscheidung im

9 Urteil des Europäischen Gerichtshofs vom 26. Oktober 2023, C-307/22.

10 Urteil des Europäischen Gerichtshofs vom 22. Juni 2023, C-579/21.

Rahmen der Rechenschaftspflicht nachvollziehbar dokumentiert wird.

Trotz der festgestellten Herausforderungen haben die von uns geprüften Verantwortlichen einen sehr guten Gesamteindruck hinterlassen. Besonders positiv fielen die internen Prozesse auf, mit denen die Einhaltung des Datenschutzes unter Einbeziehung der bzw. des (betrieblichen) Datenschutzbeauftragten regelmäßig überprüft wird. Neben der aktuellen Rechtsprechung waren den Verantwortlichen auch die entsprechenden Leitlinien 01/2022 des EDSA bekannt. Vor dem Hintergrund, dass die Nichtgewährung von Auskünften einer der häufigsten Beschwerdegründe bei uns ist, waren wir überrascht, dass die Gesamtanzahl an Auskunftsersuchen bei den Verantwortlichen relativ gering war. Weil das Auskunftsrecht häufig die Grundlage für die Inanspruchnahme weiterer Betroffenenrechte bildet, steht zu vermuten, dass die betroffenen Personen diese Rechte relativ selten geltend machen. Dies könnte zum einen an einem mangelnden Bewusstsein für die Betroffenenrechte liegen, zum anderen daran, dass Transparenz und Vertrauen durch die Verantwortlichen bereits auf anderem Wege geschaffen wurden.

Wir werden die Erkenntnisse, die wir durch die Teilnahme an der europaweiten Prüfaktion und die Mitarbeit am Abschlussbericht[11] gewonnen haben, auswerten und in unsere zukünftige Aufsichts- und Beratungstätigkeit einfließen lassen.

11 https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-implementation-right-access_en

2 Prüfung von Krankenhäusern zum Umgang mit Datenschutzverletzungen

Immer wieder melden uns Gesundheitseinrichtungen, insbesondere Krankenhäuser, Datenschutzverletzungen nach Artikel 33 Datenschutz-Grundverordnung (DS-GVO). Da diese Einrichtungen regelmäßig Gesundheitsdaten, eine besondere Kategorie personenbezogener Daten gemäß Artikel 9 Absatz 1 DS-GVO, verarbeiten, können Datenschutzverletzungen hier erhebliche Risiken für die Rechte und Freiheiten der betroffenen Personen verursachen. Wir haben deshalb im Berichtsjahr mittels Fragebogen eine stichprobenartige Prüfung in 10 brandenburgischen Krankenhäusern durchgeführt. Unser Ziel war, einen besseren Einblick in das dortige Datenschutzmanagement zu erhalten, potenzielle Problemfelder zu identifizieren, mögliche Hinweise und Hilfestellungen abzuleiten sowie insgesamt sensibilisierend auf die Gesundheitseinrichtungen einzuwirken.

Zu den folgenden vier Prüfbereichen haben wir Informationen von den Krankenhäusern eingeholt:

1. interne Prozesse beim Auftreten von Datenschutzverletzungen, Meldewege, beteiligte Personen, Fristen, Vorgaben zur Bewertung möglicher Risiken und Ableitung von technischen und organisatorischen Maßnahmen, Anforderungen zur Dokumentation von Vorfällen,

2. Austausch von Patientendaten mit Externen wie anderen Gesundheitseinrichtungen, dem zuständigen Gesundheitsamt oder Patientinnen und Patienten, Geschäftsanweisungen hierfür, interne Prozesse und umgesetzte technische und organisatorische Maßnahmen zur Verhinderung eines fehlerhaften Versands bzw. einer fehlerhaften Übermittlung,

3. Umgang mit elektronischen Datenträgern, insbesondere mit externen Massenspeichern, mobilen Endgeräten und mit von außen erreichbaren Cloud-Speichern, Geschäftsanweisungen hierfür, umgesetzte technische und organisatorische Maßnahmen, insbesondere zur Verschlüsselung, Absicherung des Datenträgertransports,

4. Umgang mit Papierunterlagen, Geschäftsanweisungen hierfür, umgesetzte technische und organisatorische Maßnahmen, Absicherung des Transports von Papierunterlagen.

Die Prüfbereiche 2 bis 4 spiegeln wider, dass der Großteil der bei uns eingehenden Meldungen von Krankenhäusern zu Datenschutzverletzungen sich auf Mängel oder Fehler beim Transport oder bei der Übermittlung von Daten bezieht.

Erfreulich war, dass fast alle Krankenhäuser zeitgerecht und teilweise auch sehr umfassend Auskunft gaben. Lediglich eine Institution lieferte Informationen nicht in ausreichendem Umfang bzw. Detailgrad. Wir werden diese Einrichtung gesondert prüfen.

Als positives Ergebnis konnten wir festhalten, dass unsere Fragen zu den Prüfbereichen 2 bis 4 von den Krankenhäusern in der Regel zufriedenstellend bis sehr gut beantwortet wurden. Sehr häufig existierten Geschäftsanweisungen zum Transport oder zur Übermittlung von Patientendaten auf elektronischem Weg sowie zur Auswahl der Empfängerin bzw. des Empfängers und der richtigen Datenquelle. Die umgesetzten technischen und organisatorischen Maßnahmen nach Artikel 32 DS-GVO erwiesen sich meist als angemessen und zielführend für die Absicherung der sensiblen Patientendaten. Hervorzuheben ist eine Einrichtung, die über eine zentrale Verwaltung und ein zentrales Sicherheitsmanagement aller Endgeräte und Speichermedien berichtete. Eine solche Konstellation erleichtert auch die nach Artikel 32 Absatz 1 Buchstabe d DS-GVO regelmäßig durchzuführende Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen.

Auch hinsichtlich des Umgangs mit Patientendaten auf Papier waren die Krankenhäuser überwiegend gut aufgestellt. Sie lieferten detaillierte Informationen z. B. über Geschäftsanweisungen zum Umgang mit und zum Transport von Papierunterlagen sowie zu Schutzmaßnahmen. In einigen Fällen wurde über eine doppelte Datenhaltung in Papierform und in elektronischer Form berichtet, insbesondere bei von Patientinnen bzw. Patienten unterschriebenen Formularen, die nachträglich digitalisiert wurden. Kein Krankenhaus erlaubte das Mitnehmen von Patientenakten in den häuslichen Bereich für Heimarbeitszwecke.

An dieser Stelle sei noch eine Besonderheit erwähnt: Daten an das zuständige Gesundheitsamt übermitteln Krankenhäuser teilweise noch immer per Fax. Dies geschieht in der Regel nicht, weil das Krankenhaus das so will, sondern weil das Gesundheitsamt jenes Medium bevorzugt. Die rein elektronische Übermittlung über ein Portal oder über verschlüsselte E-Mails ist insoweit noch nicht der Regelfall. Die Nutzung der Fax-Kommunikation betrachten wir jedoch als kritisch, insbesondere bei der Übermittlung von Gesundheitsdaten.[12]

Weniger positiv waren die Ergebnisse im Prüfbereich 1 zum Umgang mit Datenschutzverletzungen und zu internen Meldeprozessen. Hier lagen teilweise deutliche Defizite vor. Insbesondere hatten viele Krankenhäuser keine etablierten Handlungsanweisungen oder Standardvorgaben. Die Erkennung, Bearbeitung und Auswertung von Datenschutzverletzungen ist dann sehr vom Einzelfall und zum Teil vom „Bauchgefühl" der handelnden Personen abhängig. Es ist Aufgabe der Unternehmensleitung unter Beteiligung der bzw. des (betrieblichen) Datenschutzbeauftragten, hier nachzubessern und für geeignete und angemessene Datenschutzmanagementvorgaben zu sorgen.

Gesundheitseinrichtungen fit machen

Gleiches gilt für die Ermittlung der jeweils konkreten Risiken für die Rechte und Freiheiten betroffener Personen und für die Ableitung geeigneter Maßnahmen zur Abmilderung der Folgen einer Datenschutzverletzung. Die Bewertung der Risiken ist nicht nur für die betroffenen Personen von Bedeutung. Sie entscheidet auch, ob ein Vorfall lediglich intern zu dokumentieren ist (Artikel 33 Absatz 5 DS-GVO, kein Risiko), an uns als Aufsichtsbehörde gemeldet werden muss (Artikel 33 Absatz 1 bis 4 DS-GVO, es besteht ein Risiko) oder zusätzlich die Patientinnen und Patienten zu informieren sind (Artikel 34 DS-GVO, es besteht ein hohes Risiko). Gleichartige Vorfälle sollten im Krankenhaus auch gleichartig bewertet werden. Deshalb ist es wichtig, Kriterien für die Einstufung möglicher Risiken zu erarbeiten sowie innerhalb der Einrichtung abzustimmen und bekanntzugeben. Auch bei der Ermittlung von Maßnahmen zur Abmilderung der Folgen einer Datenschutzverletzung ist die Risikobeurteilung wesentlich: Bei hohen Risiken sind andere Schutzmaßnahmen erforderlich als bei niedrigen.

12 Tätigkeitsbericht Datenschutz 2019, A IV 3.2.

Zu kritisieren war in vielen Fällen die unzureichende Dokumentation von Datenschutzvorfällen ohne Risiken für betroffene Personen. Fehlende hausinterne Vorgaben oder uneinheitliche Beurteilungen erschweren es, angemessene Auswertungen vorzunehmen, Schlussfolgerungen abzuleiten und eine dauerhafte Verbesserung des Datenschutzniveaus im Krankenhaus zu erreichen.

Wie bei vielen unserer Prüfungen zeigten sich auch bei dieser sowohl Licht als auch Schatten. Wir werden die Ergebnisse nutzen, insbesondere diejenigen Einrichtungen mit vielen Defiziten zu befähigen, ihre Prozesse zum Umgang mit Datenschutzverletzungen zu verbessern. Viel lieber wäre uns allerdings, wenn derartige Vorfälle gar nicht erst aufträten.

IV Ausgewählte Fälle

1 Wer hilft beim Umzug? Die Namen, bitte!

Die Kundin eines Jobcenters beantragte im Rahmen ihres Wohnungsumzugs einen Pauschalbetrag für die Verpflegung befreundeter Helferinnen und Helfer (sogenanntes Erfrischungsgeld). Die Behörde wollte deren Namen zur Leistungsakte nehmen, womit sich die Betroffenen nicht einverstanden zeigten. Die Beschwerde, die uns hierzu erreichte, nahmen wir zum Anlass, das Vorgehen des Jobcenters zu überprüfen.

Eine Datenverarbeitung des Jobcenters ist rechtmäßig, wenn sie für die Erfüllung seiner gesetzlichen Aufgaben erforderlich ist. Das war hier nicht der Fall. Die gesetzliche Aufgabe des Jobcenters ergibt sich im Zusammenhang mit der Beschwerde aus § 22 Absatz 6 Zweites Buch Sozialgesetzbuch. Sie besteht darin, Ansprüche im Rahmen des Wohnungsumzugs einer Kundin bzw. eines Kunden auf Antrag zu prüfen und ggf. Leistungen zu gewähren. Hierzu gehört auch das sogenannte Erfrischungsgeld, das in der Rechtsprechung und der Praxis allgemein anerkannt ist. Allerdings wird der Anspruch weder dem Grunde noch der Höhe nach an die Identität der helfenden Personen geknüpft, sondern bemisst sich allein an deren Anzahl bis zur Erreichung der Höchstgrenze (grundsätzlich vier Personen). Die Namen der befreundeten Umzugshelferinnen und -helfer sind hingegen für die Anspruchsprüfung irrelevant.

Wir wandten uns zur Aufklärung des Sachverhalts an das zuständige Jobcenter und baten um eine Stellungnahme. In seiner Antwort räumte es ein, die Daten zu Unrecht angefordert zu haben, und verzichtete in der Folge darauf.

2 Datenschutzverletzungen durch Vandalismus gegen Briefkästen

Wie bereits im vorherigen erhielten wir auch im aktuellen Berichtszeitraum mehrere Meldungen über Datenschutzverletzungen, deren Ursache die Sprengung von Briefkästen öffentlicher Stellen durch den Einwurf von Pyrotechnik war. Von dieser Form des Vandalismus waren insbesondere Sozialleistungsbehörden und andere kommunale Stellen betroffen. Zumeist wurde der Briefkasten dadurch gewaltsam geöffnet und der Inhalt zerstört, entwendet oder in der Umgebung verteilt. Damit einher ging in der Regel auch eine Verletzung der Vertraulichkeit oder der Verfügbarkeit der in den Briefen enthaltenen personenbezogenen Daten.

Im Rahmen der Aufarbeitung eines solchen Vorfalls stehen Verantwortliche oftmals vor mehreren Herausforderungen. Nachfolgend geben wir einige Hinweise zu möglichen technischen und organisatorischen Maßnahmen, um Risiken für betroffene Personen zu mindern.

Briefe werden durch die Pyrotechnik vollständig oder teilweise vernichtet bzw. durch die Sprengkraft in der unmittelbaren Umgebung verstreut und entwendet. Entsprechend sind die betroffenen Personen meist nicht bekannt. Um sie dennoch zu informieren, sollte eine Bekanntmachung über ein geeignetes Medium veröffentlicht werden, die von möglichst vielen Personen zur Kenntnis genommen werden kann. Abhängig vom Verantwortlichen und den örtlichen Gegebenheiten bietet sich z. B. ein lokaler Aushang, eine Mitteilung auf der eigenen Webseite oder eine Anzeige in einer lokalen Tageszeitung an.

Um zukünftige Vorfälle zu verhindern, wäre denkbar, den Einwurf von Pyrotechnik zu erschweren, indem beispielsweise ein Briefkasten mit reduziertem Briefschlitz verwendet wird. Größere Briefe wären dann allerdings persönlich abzugeben oder in einen anderen, ggf. besonders gesicherten Kasten einzuwerfen. Als weitere Möglichkeit zur Reduzierung der negativen Folgen sollten das räumliche Verlegen des Briefkastens oder eine andere Form der Anbringung in Erwägung gezogen werden. So kann es sinnvoll sein, einen freistehenden oder außen am Gebäude angebrachten Briefkasten an die Innenseite der

Eingangstür montieren oder in das Mauerwerk einbauen zu lassen. Dies hätte den Vorteil, dass sich Briefe bei Vandalismus der genannten Form eher im Herrschaftsbereich des Verantwortlichen und nicht auf der Straße wiederfinden. Sollte eine Alarmanlage verbaut sein, besteht auch die Möglichkeit, diese z. B. mit zeitlich begrenzt wirkenden Erschütterungssensoren zu ergänzen, um schnell reagieren zu können. Da sich die entsprechenden Vorfälle bisher durchgehend nach den Öffnungszeiten der Behörden oder an Wochenenden ereigneten, bieten sich auch organisatorische Festlegungen an. So kann z. B. vorgesehen werden, dass der Briefkasten zum Ende der Öffnungszeit zu leeren ist oder ein evtl. vorhandener Wachschutz nachts bzw. an Wochenenden häufigere Bestreifungen gefährdeter Gebiete durchführt. Auch eine mechanische Blockierung des Briefschlitzes mit entsprechenden Schlössern außerhalb der regelmäßigen Öffnungszeiten könnte helfen.

Briefe sichern, Zerstörung vorbeugen

Bei einigen der uns gemeldeten Vandalismusvorfälle trat darüber hinaus noch eine Besonderheit auf: Die betroffenen Immobilien oder Teile dieser befanden sich im Eigentum einer oder eines Dritten und die öffentliche Stelle hatte diese lediglich gemietet bzw. besaß eine sonstige Nutzungserlaubnis. In diesem Fall ist es wichtig, sich vor Nutzungsübernahme eines Gebäudes rechtlich dahingehend abzusichern, geeignete und angemessene Maßnahmen zum Schutz des Postempfangs und der Briefkästen auch tatsächlich umsetzen zu dürfen.

Letztendlich muss jedoch festgehalten werden, dass es sich bei Vandalismus um einen eher unüblichen und schwer einzuschätzenden Risikofaktor handelt. Je nach Motivlage bei den zerstörungswilligen Personen sowie den ihnen zur Verfügung stehenden Mitteln und Methoden können entsprechende Vorfälle wohl nicht immer vollständig verhindert werden. Zu empfehlen ist, auch nach Rücksprache mit den zuständigen Sicherheitsbehörden, rechtzeitig präventive Maßnahmen in Erwägung zu ziehen.

3 Versäumte Löschung von Bewerberdaten

Ein ehemaliger Bewerber wandte sich mit einer Beschwerde an uns. Er hatte sich bei einem Unternehmen auf eine ausgeschriebene Stelle beworben und hierfür seine personenbezogenen Daten in dem unternehmenseigenen Stellenportal hinterlassen. Dort waren die Daten auch ca. drei Jahre nach der Besetzung der Stelle mit einer anderen Person noch immer gespeichert, obwohl der Beschwerdeführer die Löschung gegenüber einer Mitarbeiterin verlangt hatte. Eine Reaktion des Unternehmens war jedoch ausgeblieben. Regelmäßig hatte der Bewerber in den drei Jahren im Portal nachgesehen und festgestellt, dass seine Daten noch vorhanden waren.

Wir kontaktierten den Datenschutzbeauftragten des Unternehmens und baten um Aufklärung. Das Problem erledigte sich innerhalb sehr kurzer Zeit: Die Daten des Bewerbers waren tatsächlich noch im Stellenportal gespeichert. In seinem Profil hatte er angekreuzt, nur „mit dem für die Bewerbung zuständigen Recruiting Manager kommunizieren“ zu wollen. Vermutlich hatte er gegenüber dieser Person auch die Löschung seiner Daten verlangt. Die betreffende Mitarbeiterin hatte das Unternehmen jedoch in der Zwischenzeit verlassen und das Löschbegehren weder selbst bearbeitet noch ihrer Nachfolge übergeben. Im Ergebnis löschte das Unternehmen die Daten umgehend.

Bei der Aufklärung des Sachverhalts fiel uns auf, dass in der Datenschutzerklärung des Stellenportals auch zwei Fristen für eine automatische Löschung von Bewerberdaten erwähnt waren, die im vorliegenden Fall jedoch nicht wirkten: Zum einen sollten Bewerbungen automatisch gelöscht werden, wenn 183 Tage seit Bekanntgabe der erfolgreichen Besetzung vergangen waren. Hierzu war es nach Auskunft des Datenschutzbeauftragten erforderlich, dass im Bewerbermanagementsystem des Unternehmens die Stelle als „besetzt“ gekennzeichnet wird. Wegen des Weggangs der zuständigen Mitarbeiterin war dies offensichtlich nicht erfolgt.

Darüber hinaus war eine automatische Löschung von solchen Bewerberprofilen vorgesehen, auf denen über einen Zeitraum von 183 Tagen keine Aktivität zu verzeichnen war. Diese Löschroutine kam im vorliegenden Fall jedoch deshalb nicht zur Anwendung, weil die

Frist mit jeder Neuanmeldung des Beschwerdeführers am Portal erneut begann. Jedes erfolgreiche Login setzte den Zähler entsprechend zurück, sodass die Frist von vorn anfing und die automatische Löschung ausblieb. Wie der Datenschutzbeauftragte nach interner Rücksprache mit der IT-Abteilung des Unternehmens mitteilte, konnte zumindest die letzte Anmeldung des Beschwerdeführers nachvollzogen werden.

Das Unternehmen nahm die Angelegenheit zum Anlass, die Prozesse des Bewerbermanagements und die technische Umsetzung im IT-System einer Revision zu unterziehen. Auch sollten interne Regelungen beim Ausscheiden von Mitarbeiterinnen und Mitarbeitern, Vertretungsregelungen im Personalbereich sowie die Information für Interessierte zur Nutzung des Stellenportals überprüft werden. Aufgrund der überaus schnellen, kooperativen und sachgerechten Reaktion des Unternehmens war ein weiteres aufsichtsbehördliches Tätigwerden entbehrlich.

4 Digitaler Telefonassistent einer Arztpraxis

Der Vater eines kranken Kindes wollte telefonisch in der Kinderarztpraxis eines Medizinischen Versorgungszentrums einen Termin vereinbaren. Er erreichte dort jedoch nur den digitalen Telefonassistenten, der auf Datenschutzhinweise im Internet verwies und nach einer Einwilligung zur Datenverarbeitung fragte. Diese werde benötigt, falls der Anrufer eine Nachricht mit seinem Anliegen hinterlassen wolle. Nachdem er die Einwilligung verweigert und eine erneute Nachfrage ebenfalls ablehnend beantwortet hatte, erhielt der Anrufer die Mitteilung, er könne unter diesen Umständen lediglich einen Rückruf vereinbaren. Da er das Kind aber so schnell wie möglich zum Arzt bringen wollte, machte er sich ohne weitere Absprache auf den Weg zur Praxis.

Die Datenschutzhinweise, auf die der digitale Telefonassistent in seiner Ansage verwies, nannten zwar zunächst ein Unternehmen mit Sitz im Freistaat Bayern als Verantwortlichen, stellten dieses aber gleichzeitig als Auftragsverarbeiter dar. Auf Nachfrage teilte uns das Versorgungszentrum mit, selbst für die Datenverarbeitung verantwortlich zu sein und einen Auftragsverarbeitungsvertrag mit der bayerischen Firma geschlossen zu haben. Auch eine Datenschutz-Folgenabschätzung sei vorgenommen worden.

Wie sich herausstellte, sollte der digitale Telefonassistent in der Kinderarztpraxis ganztätig, also auch während der Sprechzeiten, im Einsatz sein. Die uns vorgelegte Datenschutz-Folgenabschätzung sah hingegen vor, den Einsatz auf die Pausen- und Schließzeiten der Einrichtung zu beschränken. Dass dies nicht umgesetzt wurde, monierten wir. Schließlich waren die Mitarbeiterinnen oder Mitarbeiter der Praxis dadurch auch während der Öffnungszeiten aus der Ferne nicht direkt zu erreichen. Ohne Erteilung einer Einwilligung mindestens für einen Rückruf war selbst eine Terminvereinbarung somit nur vor Ort möglich. Dies stellte für die Eltern oder Sorgeberechtigten kranker Kinder eine erhebliche Hürde dar. Die datenschutzrechtlich vorgeschriebene Freiwilligkeit der Einwilligung wurde damit wesentlich beeinträchtigt. Wir haben dem Versorgungszentrum empfohlen, den digitalen Telefonassistenten, wie ursprünglich vorgesehen, nur während der Pausen- und Schließzeiten zu verwenden.

Im Ergebnis setzte das Medizinische Versorgungszentrum unsere Empfehlung um.

5 Auskunftsrecht gegenüber einer Bibliothek

Im Berichtszeitraum wandte sich eine Bürgerin mit einer Anfrage an uns. Sie nutzte häufig die örtliche Leihbücherei und hatte diese um eine Liste der von ihr in der Vergangenheit ausgeliehenen Literatur gebeten. Zwar lägen ihr noch Ausleihquittungen vor, jene seien aber aufgrund des kleinen Formats wenig ergiebig. Das Online-Konto bei der Bücherei enthalte dagegen nur die gegenwärtig ausgeliehenen Bücher und selbst diese Angaben ließen sich nicht als Liste ausdrucken. Die Bücherei habe ihre Bitte um Herausgabe einer Übersicht über die ausgeliehenen Bücher „aus datenschutzrechtlichen Gründen“ abgelehnt, obwohl in der Datenschutzerklärung zu lesen war, dass ein Recht auf Auskunft und Information zu den erhobenen Daten besteht.

Gemäß Artikel 15 Datenschutz-Grundverordnung (DS-GVO) hat jede Person das Recht auf Auskunft zu den über sie verarbeiteten personenbezogenen Daten. Hierunter fallen auch die Informationen über die Leihaktivitäten und damit die Liste der von der Betroffenen ausgeliehenen Bücher. Die Begründung der Weigerung der Bibliothek, die Daten herauszugeben, war unrechtmäßig. Die Notwendigkeit, die Daten vor dem Zugriff Dritter zu schützen, ändert nichts am Anspruch der Betroffenen, ihre eigenen Daten zu erfahren.

Kein Schutz vor eigenen Daten

Dass in der Praxis Auskunftsansprüche ins Leere laufen, liegt nicht selten auch an der Ungewissheit, ob die beantragten Daten überhaupt noch vorhanden sind. Im konkreten Fall stellte sich die Frage, ob die abgeschlossenen Ausleihvorgänge überhaupt noch nachvollziehbar waren. Denn Daten sind gemäß Artikel 17 Absatz 1 Buchstabe a DS-GVO zu löschen, wenn ihre Weiterspeicherung nicht mehr zur Aufgabenerfüllung nötig ist. Sind die Speicherzwecke mit der Rückgabe des Buches erschöpft, so sind die entsprechenden Daten zu löschen. Danach besteht naturgemäß keine Möglichkeit mehr, sie zu beauskunften.

Artikel 11 Absatz 1 DS-GVO regelt ausdrücklich, dass Daten nicht deswegen länger personenbezogen gespeichert bleiben dürfen, um Betroffene zu einem späteren Zeitpunkt zu rein datenschutzrechtlichen Zwecken – wie im vorliegenden Fall zu Auskunftszwecken –

wieder identifizieren zu können. Soweit die Bibliothek beispielsweise statistische Daten zur Bücherausleihe benötigt, dürfen diese nur ohne Personenbezug gespeichert werden.

Eine Ausnahme von dieser Regel besteht nur dann, wenn der Auskunftsanspruch vor dem Zeitpunkt der Löschung geltend gemacht wird. Der Auskunftsanspruch darf durch die Löschung der Daten nicht vereitelt werden. Dies gilt regelmäßig auch, wenn die Daten unzulässig gespeichert waren, da es gerade auch ein typisches Ziel von Auskunftsansprüchen ist, herauszufinden, ob und in welchem Umfang eine unzulässige Speicherung erfolgt.

Wir haben der Antragstellerin geraten, ihren Wunsch unter Berücksichtigung unserer Hinweise noch einmal vorzubringen und insbesondere zu klären, ob die beantragten Daten überhaupt noch vorhanden sind.

V Ausgewählte Beratungen

1 Brandenburgisches Kinder- und Jugendgesetz: Gesetz der 1.000 Stimmen

Das neu geschaffene Brandenburgische Kinder- und Jugendgesetz (BbgKJG) stärkt die Rechte von Brandenburgs Kindern, Jugendlichen und jungen Erwachsenen deutlich. Es regelt u. a. die umfassende Pflicht zur Erstellung von Konzepten zum Schutz vor Gewalt und zur Vermeidung von Kindeswohlgefährdungen, die Förderung von Netzwerken zum Kinderschutz sowie eine Beteiligung und Mitbestimmung von Kindern und Jugendlichen. 1.000 von ihnen wirkten aktiv an der Erstellung des Gesetzes mit. Es setzt geänderte bundesrechtliche Anforderungen in Landesrecht um und löst das Erste Gesetz zur Ausführung des Achten Buches Sozialgesetzbuch – Kinder- und Jugendhilfe ab. Der Bereich der Kindertagesbetreuung wird aber weiterhin durch das Zweite Gesetz zur Ausführung des Achten Buches Sozialgesetzbuch – Kinder- und Jugendhilfe, das Kindertagesstättengesetz[13], geregelt.

Das Ministerium für Bildung, Jugend und Sport gab uns zunächst Gelegenheit, zu einem Arbeitsentwurf des neuen Gesetzes Stellung zu nehmen. Schließlich beteiligte es uns im Rahmen der Ressortabstimmung des zwischenzeitlich wesentlich veränderten Gesetzentwurfs. Hierzu hatten wir eine Reihe datenschutzrechtlicher sowie redaktioneller Anmerkungen und Hinweise, die jedoch nur zum Teil Berücksichtigung fanden:

Die nach § 10a Achtes Buch Sozialgesetzbuch (SGB VIII) vorgesehene Beratung junger Menschen, von Müttern, Vätern sowie Per-

13 Zweites Gesetz zur Ausführung des Achten Buches des Sozialgesetzbuches – Kinder- und Jugendhilfe – (Kindertagesstättengesetz – KitaG) in der Fassung der Bekanntmachung vom 27. Juni 2004 (GVBl. I Nr. 16 S. 384), zuletzt geändert durch Gesetz vom 11. Dezember 2024 (GVBl. I Nr. 55).

sonensorge- und Erziehungsberechtigten kann gemäß § 8 Absatz 1 BbgKJG auch videogestützt oder telefonisch durchgeführt werden. Bereits frühzeitig hatte das Ministerium unsere Empfehlung aufgenommen, in diesem Zusammenhang eine gesetzliche Regelung zu schaffen, welche die Datensicherheit bei der Nutzung technischer Mittel gewährleistet.

Zu begrüßen ist zudem die Aufnahme einer Bestimmung in § 28 Absatz 3 BbgKJG, nach der im Rahmen eines Vollzeitpflegeverhältnisses die Vertrauenspersonen der Kinder oder Jugendlichen nur mit deren Zustimmung Einblick in das zur Vermeidung von Kindeswohlgefährdungen zu entwickelnde individuelle Schutzkonzept nehmen können.

Rechte von Kindern und Jugendlichen gestärkt

Weiterhin hatten wir im Rahmen unserer Beteiligung am Gesetzgebungsverfahren angemahnt, für konkrete Datenverarbeitungen klare Rechtsgrundlagen zu schaffen, Verarbeitungszwecke festzulegen, Datenerhebungen und -übermittlungen zu präzisieren sowie Vorkehrungen zur Wahrung der Betroffenenrechte im Gesetz zu integrieren.

So hatten wir z. B. vorgeschlagen, die Trägerinnen und Träger der öffentlichen und freien Jugendhilfe zu verpflichten, den in der Ombudsstelle im Sinne des § 9a SGB VIII mit der Konfliktberatung befassten Personen unter Beachtung der geltenden datenschutzrechtlichen Bestimmungen Auskunft zu erteilen und bei der Klärung des Sachverhaltes sowie der Konkretisierung der Interessenlagen der betroffenen jungen Menschen und Familien mitzuwirken. Darüber hinaus hatten wir angeregt, das konkrete Verfahren zur Akteneinsicht bei Trägerinnen bzw. Trägern der Jugendhilfe durch die Ombudsstellen in § 45 BbgKJG zu regeln.

Hinsichtlich der neu geschaffenen Vorschriften für Verfahrenslotsinnen und -lotsen im Sinne des § 10b SGB VIII ist festzuhalten, dass diese bei ihrer unterstützenden und beratenden Tätigkeit für junge Menschen und deren Familien als Beschäftigte des Jugendamts dem Sozialdatenschutz unterliegen. Wir verwiesen in unseren Erörterungen mit dem Ministerium darauf, dass es zur Aufgabenerfüllung der Lotsinnen und Lotsen grundsätzlich nicht erforderlich ist, Fallakten einzusehen oder Informationen bei anderen Einrichtungen einzuholen. Soweit im Einzelfall dennoch eine solche Datenverarbeitung erforderlich sein sollte, kann sie nur auf einer Einwilligung der Fami-

lien als Rechtsgrundlage basieren. Weiter machten wir darauf aufmerksam, dass auch für die im Unterstützungsfall durch die Verfahrenslotsinnen bzw. -lotsen zu führenden Akten der Grundsatz der Datenminimierung gilt.

§ 91 BbgKJG stellt zwar klar, dass Schulsozialarbeit im Sinne des § 13a SGB VIII eine Leistung der Jugendhilfe ist, die keiner schulischen Verantwortung unterliegt. Wir hatten eine klare Rechtsgrundlage für die Datenverarbeitungen der auf diesem Gebiet pädagogisch und organisatorisch kooperierenden Stellen gefordert. Dazu gehören die jeweiligen Trägerinnen und Träger der Schulsozialarbeit, das Jugendamt, die Schule sowie die Schulträgerinnen und Schulträger. Die im Gesetzentwurf vorgesehenen und noch zu erarbeitenden „Empfehlungen" für solche Datenverarbeitungen genügen diesen Anforderungen mangels Bindungswirkung nicht.

Das Ministerium ist auf unsere konkreten Vorschläge und Forderungen nicht eingegangen. Im Ergebnis beschränkt sich das Gesetz auf eine zentrale Datenschutzvorschrift, die die Anwendung allgemeiner datenschutzrechtlicher Regelungen wie der Datenschutz-Grundverordnung und des Sozialdatenschutzes vorsieht. Konkrete Einzelregelungen zu den oben genannten Datenverarbeitungen lässt das Gesetz vermissen.

Das Brandenburgische Kinder- und Jugendgesetz ist am 1. August 2024 in Kraft getreten.[14]

14 Gesetz zur Förderung und zum Schutz junger Menschen (Brandenburgisches Kinder- und Jugendgesetz – BbgKJG) vom 25. Juni 2024 (GVBl. I Nr. 34).

2 Brandenburgisches Abfall- und Bodenschutzgesetz: Videoüberwachung zur Vermeidung von Vermüllung

Im Rahmen der Novellierung des Brandenburgischen Abfall- und Bodenschutzgesetzes (BbgAbfBodG)[15] erfolgte eine frühzeitige Beteiligung der Landesbeauftragten. Der Gesetzentwurf sollte u. a. um eine Rechtsgrundlage für eine Videoüberwachung bestimmter Flächen erweitert werden. Zur Begründung verwies das Ministerium für Landwirtschaft, Umwelt und Klimaschutz des Landes Brandenburg auf die Verwaltungsaufgabe der Abfallwirtschaftsbehörden, Vermüllung und illegale Abfallentsorgung zu bekämpfen. Das bisherige Landesrecht bot keine ausreichende Rechtsgrundlage, auf die eine Videoüberwachung von öffentlichen Orten durch die Abfallwirtschaftsbehörden hätte gestützt werden können.

Die Landesbeauftragte äußerte erhebliche datenschutzrechtliche Bedenken. Daraufhin konnte erreicht werden, dass die ursprünglich vorgesehene verdeckte Videoüberwachung keinen Eingang in das Änderungsgesetz fand. Für eine Pilotphase von drei Jahren ist nunmehr in Absatz 2 der Regelung des § 40 BbgAbfBodG eine Rechtsgrundlage für die Durchführung einer räumlich begrenzten, offenen Videoüberwachung geschaffen worden. Aus Gründen der Normenklarheit hatte sich die Landesbeauftragte für eine separate Regelung, die sich allein mit der Videoüberwachung befasst, eingesetzt.

Zudem forderte die Landesbeauftragte vor dem Hintergrund des Grundsatzes der Verhältnismäßigkeit eine strikte Zweckbindung und ausreichend präzise formulierte, enge Tatbestandsvoraussetzungen. Denn mit einer Videoüberwachung von öffentlich zugänglichen Orten, an denen wiederholt Müll illegal abgelagert wurde, können auch viele unbeteiligte Personen erfasst werden, die sich in diesen Bereichen zum Zweck der Freizeitgestaltung aufhalten, und deren Rechte es zu wahren gilt.

---

15 Artikel 1 des Dritten Gesetzes zur Änderung des Brandenburgischen Abfall- und Bodenschutzgesetzes vom 20. Juni 2024 (GVBl. I Nr. 24, ber. Nr. 40).

In das Gesetz hat mit § 40 Absatz 2 BbgAbfBodG nunmehr eine Regelung Eingang gefunden, die eine räumliche Begrenzung der Videoüberwachung vorsieht. Es kommen nur Flächen in Betracht, auf denen wiederholt kompakte Ablagerungen illegal entsorgter Abfälle von mehr als einem Kubikmeter festgestellt wurden. Als für eine Videoüberwachung geeignete Flächen sind Zufahrten und Einmündungsbereiche von Bundes- und Landesstraßen zu nicht dem öffentlichen Verkehr gewidmeten Forststraßen und Waldwegen in der Nähe von Autobahnabfahrten oder vergleichbare Verkehrsknotenpunkte genannt. Zudem sind ein Entscheidungsvorbehalt auf Ministeriumsebene und Berichtspflichten vorgesehen. Die Regelung ist auf die Dauer einer Pilotphase von drei Jahren begrenzt. Die Landesbeauftragte plant, die Umsetzung der Neuregelung innerhalb dieser Zeit zu überprüfen. Ob sich die Videoüberwachung als geeignetes und erforderliches Mittel darstellt, um Vermüllung zu bekämpfen, oder ob es lediglich zu einer Verdrängung kommt, muss sich erst noch herausstellen.

3 Brandenburgisches Brand- und Katastrophenschutzgesetz: Drohnen für Rettungseinsätze?

Das Ministerium des Innern und für Kommunales beteiligte uns frühzeitig an dem Vorhaben zur Änderung des Brandenburgischen Brand- und Katastrophenschutzgesetzes (BbgBKG). Aus datenschutzrechtlicher Sicht zentral war hierbei § 17a des Arbeitsentwurfs, mit dem eine Rechtsgrundlage für den Einsatz von kamerabewehrten, unbemannten Flugobjekten (sogenannte Drohnen) zur Unterstützung von Rettungseinsätzen geschaffen werden sollte. Eine solche Rechtsgrundlage ist im bisherigen Gesetz nicht enthalten. Sie ist aber erforderlich; schließlich können mit einer optischen Überwachung, der Speicherung und Auswertung von Bildmaterial sowie mit der Verarbeitung von gemäß Artikel 9 Datenschutz-Grundverordnung (DS-GVO) besonders geschützten Gesundheitsdaten im Kontext von Rettungseinsätzen erhebliche Eingriffe in die Rechte und Freiheiten betroffener Personen verbunden sein.

Die Initiative des Ministeriums zur Schaffung einer Rechtsgrundlage für die Datenverarbeitung bei Nutzung von Drohnen und unsere Einbindung begrüßten wir sehr. Sowohl im Gesetzestext als auch in seiner Begründung war der besonderen Eingriffstiefe Rechnung zu tragen, die mit der beabsichtigten Verarbeitung personenbezogener Daten verbunden ist. Wir hatten den Entwurf deshalb sowohl an den Anforderungen von Artikel 6 Absatz 3 Buchstabe b DSGVO (hinsichtlich der Datenverarbeitung zur Erfüllung einer öffentlichen Aufgabe) als auch an denjenigen von Artikel 9 Absatz 2 Buchstabe g DS-GVO (hinsichtlich der Verarbeitung von Gesundheitsdaten) zu messen. Schwerpunkte unserer Bewertung waren insofern die Normenklarheit, die Begrenzung des Umfangs und der Zwecke der Datenverarbeitung, die Verhältnismäßigkeit sowie die Maßnahmen zur Wahrung der Grundrechte der betroffenen Personen.

Gemäß dem Arbeitsentwurf sollen Aufgabenträgerinnen und -träger während des Einsatzes personenbezogene Daten mittels Bildaufnahmen durch unbemannte Fluggeräte verarbeiten dürfen, wenn dies von der Einsatzleitung angewiesen wurde, es zur Abwehr von Gefahren für Leib, Leben oder Freiheit von Personen oder für erhebliche Sachwerte erforderlich ist und keine Anhaltspunkte bestehen, dass

überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. In unserer Stellungnahme monierten wir, dass sich die Bandbreite der gewünschten Verarbeitungsvorgänge klar aus dem Gesetzestext ergeben muss. Lediglich aus dem Umstand, dass die Daten später weiterverarbeitet werden sollten, ging hervor, dass offenbar sowohl Echtzeitbildbeobachtung als auch die Speicherung und die Auswertung der Videobilddateien zu Einsatzzwecken beabsichtigt waren. Weiterhin regten wir an zu prüfen, ob der verwendete, vergleichsweise weite Gefahrenbegriff geschärft werden kann, etwa indem der Drohneneinsatz ausdrücklich an das Vorhandensein einer konkreten oder unmittelbaren Gefahr geknüpft wird. Darüber hinaus baten wir darum, das nicht näher definierte Schutzgut „erhebliche Sachwerte“ zu konkretisieren und darzulegen, inwieweit die entsprechende Datenverarbeitung der Anforderung eines (erheblichen) öffentlichen Interesses aus der Datenschutz-Grundverordnung gerecht wird.

Im Hinblick auf den Bereich der privaten Lebensführung schließt der Entwurf eine absichtliche Überwachung und Aufnahme damit verbundener Bilder durch Drohnen mit Recht aus. Problematisch bleibt indes die Frage der versehentlichen oder zufälligen Aufnahmen. Als Lösung schlugen wir für einen solchen Fall eine ausdrückliche Pflicht zur Anordnung des unverzüglichen Abbruchs der Videoüberwachung und Löschung des gespeicherten Materials vor; zusätzlich sollte das Vorgehen jeweils dokumentiert werden.

Rettungseinsätze unter Beobachtung

Wir wiesen das Ministerium auch auf den Umstand hin, dass ggf. zahlreiche Unbeteiligte am Einsatzort oder in dessen unmittelbarer Umgebung von der Kamera erfasst werden können, teils auch auf ihren eigenen Grundstücken und bei rein privaten Tätigkeiten. Derart intensive Eingriffe würden jedoch auch den Schutz des Privat- und Familienlebens nach Artikel 7 EU-Grundrechtecharta berühren. Weiterhin machten wir darauf aufmerksam, dass durch den Drohneneinsatz auch das Rettungspersonal selbst von der Überwachung bzw. Aufzeichnung des Bildmaterials betroffen ist und – z. B. durch eine spätere Auswertung der Aufnahmen – eine Leistungs- und Verhaltenskontrolle einzelner Mitarbeiterinnen und Mitarbeiter möglich wird, die ihrerseits in deren Rechte eingreift.

Die neuen Regelungen sehen eine Anonymisierung der personenbezogenen Daten unverzüglich nach Einsatzende vor. Wir erinnerten

in unserer Stellungnahme daran, dass hierdurch die Zuordnung der Bilder zu den jeweiligen natürlichen Personen zuverlässig ausgeschlossen werden muss und eine (automatisierte) Verfremdung der Aufnahmen ggf. nicht ausreicht. Zudem führten wir aus, dass die Anonymisierung auch Voraussetzung zu jeglicher Weiterverwendung der Bilder über den Einsatz hinaus und zu anderen Zwecken ist (z. B. für die Aus- und Fortbildung von Einsatzkräften).

Hinsichtlich der Transparenz- und Informationspflichten gemäß Artikel 12 ff. DS-GVO, denen Verantwortliche bei der Verarbeitung personenbezogener Daten im Zuge eines Drohneneinsatzes unterliegen, rieten wir zu einem gestuften Verfahren. Wir verwiesen auf Empfehlungen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, nach denen Hinweisschilder und Durchsagen als das effektivste Mittel zu betrachten sind. Auch die Drohnen selbst sollten gut erkennbar sein.

Neuerungen gibt es im Arbeitsentwurf für die Gesetzesänderung auch im Bereich der Ausbildung und Jugendfeuerwehren. Vorgesehen ist, dass die Aufgabenträgerinnen und -träger die Polizei unverzüglich über konkrete Anhaltspunkte zu informieren haben, die die Annahme einer Gefahr durch Straftaten gegen Leib, Leben, Freiheit oder die sexuelle Selbstbestimmung zu Lasten einer bzw. eines Angehörigen der Jugendfeuerwehr rechtfertigen. Zur Beachtung des Grundprinzips der Datenminimierung regten wir mit einem konkreten Formulierungsvorschlag an vorzusehen, dass beim Erstkontakt mit den Strafverfolgungsbehörden der Sachverhalt zunächst hinsichtlich der konkreten Personen möglichst anonym vorgetragen werden sollte, die Strafverfolgungsbehörden dann jedoch – wie dies nach der Strafprozessordnung möglich ist – im Dialog die für die Aufklärung erforderlichen personenbezogenen Daten selbst erheben können. Dies würde den Verantwortlichen von der Gefahr entlasten, schützenswerte, möglicherweise intime personenbezogene Daten etwa des möglichen Opfers offenzulegen, die aus Sicht der Strafverfolgungsbehörden für die Aufklärung nicht relevant sind. Diese von den Aufgabenträgerinnen und -trägern initiierte, aber von den Strafverfolgungsbehörden geführte Sachaufklärung könnte der Schutzbedürftigkeit der beteiligten Personen Rechnung tragen, ohne dass die Aufklärung behindert würde.

Weiterhin legten wir im Falle der – ohne Weiteres zulässigen – Einholung eines erweiterten Führungszeugnisses für Beschäftigte im

Bereich der Jugendfeuerwehren nahe, die diesbezüglich geplanten Protokoll- und Löschbestimmungen mit dem § 30a Absatz 3 Bundeszentralregistergesetz zu harmonisieren. Die dortige Regelung enthält bereits geeignete Festlegungen und bindet die Empfängerinnen und Empfänger von Führungszeugnissen unmittelbar.

Zu erwähnen ist letztlich, dass § 17 Absatz 3 des Entwurfs nunmehr explizit die Gruppe der Hilfesuchenden als Personen nennt, deren Daten im Zusammenhang mit Einsätzen erhoben werden dürfen. Da Notrufe bereits zuvor zulässigerweise aufgezeichnet wurden, lag hierin aus unserer Sicht keine Erweiterung des Kreises der Betroffenen. Soweit für Einsatzdaten die Löschfrist unter bestimmten Umständen um weitere zwölf Monate verlängert wurde, schlugen wir vor, dies mit Hinblick auf Artikel 17 Absatz 1 Buchstabe a DS-GVO am tatsächlichen Bedarf zur Erfüllung der Verarbeitungszwecke und nicht an starren Fristen auszurichten.

Das Gesetzgebungsverfahren dauert noch an. Ob und in welchem Umfang unsere Anregungen aufgegriffen werden, ist nicht sicher. Bereits jetzt haben wir jedoch empfohlen, für die Regelung zur Nutzung von Drohnen bei Rettungseinsätzen aus Gründen der Transparenz und zur Überprüfung der Erforderlichkeit eine Berichtspflicht (beispielsweise in Anlehnung an eine entsprechende Norm im Brandenburgischen Polizeigesetz) oder eine Evaluation zu einem späteren Zeitpunkt vorzusehen.

4 Hundehalteverordnung: offene Auslegungsfragen

Im Berichtszeitraum erhielt die Landesbeauftragte Gelegenheit, Stellung zur Neufassung der Hundehalteverordnung (HundehV)[16] zu nehmen, die trotz unserer Kritik nahezu unverändert im Folgemonat in Kraft trat.

§ 6 Absatz 3 der Verordnung erfordert eine Erlaubnis, bestimmte Hundearten halten zu dürfen. Halten juristische Personen einen solchen Hund, muss es eine volljährige, sachkundige und zuverlässige natürliche Person geben, die im Auftrag der juristischen Person handelt. Zwar verpflichtet § 9 Absatz 5 Nummer 7 HundehV dazu, einen Wechsel der für die Betreuung des Tiers verantwortlichen natürlichen Person anzuzeigen. Eine ausdrückliche Zuweisung der Pflicht zur Erstmeldung der Betreuerin bzw. des Betreuers konnten wir indes nicht auffinden. Dies hielten wir für unschlüssig.

Für begründungsbedürftig hielten wir auch, dass Daten von Personen, die eine zur Sachkundeprüfung äquivalente Prüfung gemäß § 7 Absatz 2 Nummer 6 HundehV absolviert haben, im Amtsblatt für Brandenburg veröffentlicht werden sollten. Für diesen Eingriff müssten mindestens die Zwecke – etwa die Erleichterung der Nachprüfung der Sachkunde durch öffentliche und private Stellen – nebst Überlegungen zur Erforderlichkeit dargelegt werden.

Weiter befugt § 8 Absatz 3 der Verordnung die Ordnungsbehörde, Anfragen an Strafverfolgungsbehörden über Ermittlungsverfahren zu stellen und sonstige Erkenntnisse einzufordern, die geeignet sind, bestehende Bedenken gegen die Zuverlässigkeit der Halterin bzw. des Halters zu klären. Wir wiesen darauf hin, dass, soweit Nachforschungen bei anderen Stellen zugelassen werden sollten, dies normenklar zu regeln wäre.

---

16 Ordnungsbehördliche Verordnung über das Halten und Führen von Hunden (Hundehalteverordnung – HundehV) vom 24. Juni 2024 (GVBl. II Nr. 42).

Inwieweit die aufgezeigten Unklarheiten in der Praxis zu Auslegungsschwierigkeiten führen werden, bleibt abzuwarten.

Nach Inkrafttreten der Verordnung erreichten uns Anfragen zur Vereinbarkeit insbesondere des § 1 Absatz 3 der Verordnung mit dem Datenschutzrecht. Gemäß dieser Vorschrift müssen Hunde außerhalb von befriedetem Besitztum generell Namen und Anschrift der Halterin oder des Halters am Halsband tragen. Die Anfragenden argumentierten, dass dies nicht erforderlich sei, weil die Feststellung deren oder dessen Identität indirekt auch über die Hundemarke möglich sei.

Bellen und Beißen – Haltung verpflichtet!

Im Gegensatz zu den Fragestellenden halten wir diese – im Übrigen bereits nach der alten Rechtslage sinngemäß bestehende – Verpflichtung datenschutzrechtlich für vertretbar:

Erstens sind Halsbänder in der Regel so klein, dass die Daten durch Unbefugte nicht unmittelbar zur Kenntnis genommen werden können. Zweitens können Dritte die personenbezogenen Daten auf dem Halsband typischerweise gerade dann lesen, wenn die für den Hund verantwortliche Person etwa im Fall seines Entlaufens nicht in der Lage ist, die Aufsicht über das Tier auszuüben. Drittens schließlich trägt die Hundehalteverordnung als Werkzeug der Gefahrenabwehr dem Umstand Rechnung, dass das Freilaufen von Hunden tendenziell eine Gefahr für die Sicherheit und Ordnung, insbesondere für die körperliche Unversehrtheit anderer Menschen und für Sachwerte darstellen kann. Tritt ein Schadensfall auf, hat die oder der Geschädigte ohnehin in der Regel ein Recht auf Kenntnis der Daten der Halterin oder des Halters.

5 Verwaltungsdigitalisierung

5.1 Onlinezugangsgesetz: Klarstellung der datenschutzrechtlichen Verantwortlichkeiten

Am 24. Juli 2024 trat das OZG-Änderungsgesetz[17] in Kraft. Es umfasst sowohl Änderungen des Onlinezugangsgesetzes (OZG) und des E-Government-Gesetzes des Bundes (EGovG) als auch Anpassungen einzelner Bücher des Sozialgesetzbuches, der Abgabenordnung und einer Reihe weiterer Gesetze. Im Gesetzgebungsverfahren konnten die Datenschutzaufsichtsbehörden Hinweise und Empfehlungen einbringen.[18] Nachfolgend werden wesentliche datenschutzrechtlich relevante Fortschreibungen und Ergänzungen des Onlinezugangsgesetzes selbst (das sogenannte OZG 2.0) sowie des E-Government-Gesetzes des Bundes betrachtet.

Wichtiges Ziel des ursprünglichen Onlinezugangsgesetzes, das bereits im Jahr 2017 verabschiedet wurde, war die Schaffung der rechtlichen Rahmenbedingungen für die Digitalisierung der öffentlichen Verwaltung in Deutschland. Bund, Länder und Kommunen standen anschließend vor der Herausforderung, ca. 6.000 Verwaltungsdienstleistungen, welche in ca. 575 Leistungsbündeln zusammengefasst wurden, zu digitalisieren. Die geplanten Vorhaben decken alle Lebensbereiche ab, von A wie „Abbrennen von Pyrotechnik“ und „Abfallentsorgung“ bis Z wie „Zwangsvollstreckung“ und „Zweitwohnungssteuer“. Um mehrfachen Entwicklungs- und Umsetzungsaufwand für dieselbe Dienstleistung in unterschiedlichen Bundesländern zu vermeiden, hat der IT-Planungsrat das sogenannte EfA-Prinzip (Einer-für-Alle) entwickelt: Ein Dienst wird zentral federführend von einem Land entwickelt und kann anschließend in allen anderen Ländern nachgenutzt werden. Im Kontext der Bereitstellung und Nachnutzung von OZG-Onlinediensten nach dem EfA-Prinzip begegneten uns oftmals Schwierigkeiten im Hinblick auf die Fest-

17 Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG) vom 19. Juli 2024 (BGBl. 2024 I Nr. 245).

18 Tätigkeitsbericht Datenschutz 2023, A I 2.4.

legung der datenschutzrechtlichen Verantwortlichkeit, die Bestimmung der Rechtsgrundlagen der Datenverarbeitung (insbesondere für die Erhebung und Übermittlung der personenbezogenen Daten in bzw. aus einem zentral bereitgestellten Antragsformular) sowie die Gestaltung der Beziehungen zwischen bereitstellender und nachnutzender Behörde. Hierüber hatten wir mehrfach berichtet.[19]

Der bisherigen Rechtsunsicherheit trägt das o. g. Änderungsgesetz Rechnung. So wird zunächst in § 2 Absatz 8 OZG eine Legaldefinition für Onlinedienste eingeführt. Danach ist ein solcher Dienst eine IT-Komponente, die ein eigenständiges elektronisches Angebot an Nutzerinnen und Nutzer darstellt, welches die Abwicklung einer oder mehrerer elektronischer Verwaltungsleistungen von Bund und Ländern ermöglicht. Der Onlinedienst dient dem elektronischen Ausfüllen der Online-Formulare für Verwaltungsleistungen, der Offenlegung dieser Daten an die zuständige Fachbehörde sowie der Übermittlung elektronischer Dokumente und Informationen zu Verwaltungsvorgängen an Nutzerinnen und Nutzer. Der Dienst kann nach der Definition auch verfahrensunabhängig und länderübergreifend, insbesondere in der Verantwortung einer Landesbehörde zur Nutzung durch weitere Länder, bereitgestellt werden.

Darauf aufbauend enthält der neu geschaffene § 8a OZG eine Festlegung zur datenschutzrechtlichen Verantwortlichkeit der einen länderübergreifenden Onlinedienst betreibenden Behörde (Absatz 4) sowie Rechtsgrundlagen für diese Behörde zur Erhebung der personenbezogenen Daten in einem Antragsformular und zur Offenlegung dieser Daten an die jeweils zuständige Fachbehörde (Absatz 1). Auch ausweislich der Gesetzesbegründung wird insoweit eine strikte Trennung zwischen dem Antragsverfahren mit der Beantragung einer Verwaltungsleistung und dem eigentlichen Fachverfahren mit der Antragsbearbeitung und ggf. Erstellung eines Bescheids vorgenommen. Die beiden Verfahren werden somit per Gesetz jeweils eigenständig datenschutzrechtlich Verantwortlichen zugewiesen. Die Regelung hilft bei der Klärung der o. g. Herausforderungen im Kontext der Nachnutzung länderübergreifender EfA-Onlinedienste.

19 Zuletzt im Tätigkeitsbericht Datenschutz 2023, A I 2.

Es ist darauf hinzuweisen, dass § 8a OZG ausschließlich auf länderübergreifende Onlinedienste beschränkt ist und nicht für Onlinedienste gilt, die lediglich in einem Bundesland entwickelt und betrieben werden. Ferner macht die Regelung das Abschließen von Auftragsverarbeitungsverträgen nicht komplett überflüssig. In Fällen, in denen sich die den länderübergreifenden Onlinedienst betreibende Behörde eines IT-Dienstleisters bedient, handelt dieser auch nach der Gesetzesänderung als Auftragsverarbeiter. Weitere Hinweise zu § 8a OZG enthält eine Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, die wir in unserem Internetangebot bereitstellen.

Geändert und konkretisiert wurden mit dem OZG 2.0 auch die Festlegungen zu Nutzerkonten. Sie dienen der Identifizierung und Authentisierung von Nutzerinnen und Nutzern bei der Inanspruchnahme von Verwaltungsleistungen unter Berücksichtigung des erforderlichen Vertrauensniveaus. Insbesondere stellt der Bund gemäß § 3 Absatz 1 OZG zentral Bürgerkonten bereit. Deren Verwendung ist (wie zuvor schon) freiwillig. Bisher bereitgestellte Nutzerkonten der Länder oder von Fachportalen sollen nur noch für eine Übergangszeit verwendet werden können. Das zentrale Bürgerkonto des Bundes wird zu einer „DeutschlandID“ weiterentwickelt.

Einer für alle – Zuständigkeiten geregelt

Ein weiterer wichtiger Punkt sind Änderungen im E-Government-Gesetz des Bundes (EGovG), mit denen die Voraussetzungen für die Nutzung des Once-Only-Prinzips geschaffen werden. Danach sollen Bürgerinnen und Bürger sowie Unternehmen bei der Inanspruchnahme von elektronischen Verwaltungsleistungen beizubringende Nachweise nur einmal an „die Verwaltung“ übermitteln müssen. Gemäß § 5 EGovG kann in einem elektronisch abgewickelten antragsgebundenen Verwaltungsverfahren die Nachweiserbringung nach Wahl der Antragstellerin bzw. des Antragstellers entweder durch elektronisches Einreichen des Nachweises oder durch automatisierten Abruf des Nachweises bei einer anderen Stelle, bei der dieser Nachweis bereits vorliegt, erfolgen. Zum Nachweisabruf berechtigt sind sowohl Stellen, die für die fachliche Entscheidung zuständig sind (also Fachbehörden), als auch Stellen, die dafür zuständig sind, Nachweise einzuholen und an Fachbehörden weiterzuleiten. Letztere können z. B. auch die bereits angesprochenen, einen länderübergreifenden Onlinedienst betreibenden Behörden sein.

Bei der Bereitstellung und Nachnutzung von Onlinediensten im Sinne des Onlinezugangsgesetzes sind stets die datenschutzrechtlichen Dokumentations- und Nachweispflichten zu beachten. Die beschriebenen Gesetzesänderungen, die neu geschaffenen Zuweisungen der datenschutzrechtlichen Verantwortlichkeit und die Klarstellung der Beziehungen der beteiligten Behörden bei länderübergreifenden Diensten erfordern oftmals auch die Fortschreibung der vorzuhaltenden Dokumente. Wir werden darauf hinwirken, dass die Behörden in unserem Zuständigkeitsbereich diese zeitnah vornehmen.

5.2 Elektronische Beantragung von Wohngeld

Bereits im letzten Tätigkeitsbericht hatten wir über die Umsetzung des EfA-Onlinedienstes nach dem Onlinezugangsgesetz (OZG) zur Beantragung von Wohngeld berichtet.[20] Die Abkürzung EfA steht dabei für das „Einer für Alle"-Prinzip – eine Dienstleistung wird deutschlandweit zentral realisiert und zur Nachnutzung angeboten. Für das Thema Wohngeld ist das Land Schleswig-Holstein das umsetzende Bundesland. Die dortige Staatskanzlei verantwortet das Antragsportal, das von einem beauftragten IT-Dienstleister betrieben wird. Elektronisch gestellte Anträge werden an die jeweils zuständige Wohngeldstelle weitergeleitet und dort im Rahmen der eigenen Verantwortlichkeit bearbeitet und beschieden.

Nachdem die Staatskanzlei Schleswig-Holstein zunächst den Abschluss von Auftragsverarbeitungsverträgen nach Artikel 28 Datenschutz-Grundverordnung (DS-GVO) zwischen den Wohngeldstellen und dem IT-Dienstleister in Aussicht gestellt hatte, favorisierte sie anschließend Vereinbarungen nach Artikel 26 DS-GVO über eine gemeinsame datenschutzrechtliche Verantwortung. Diese sollten zwischen der Staatskanzlei und den teilnehmenden Wohngeldstellen abgeschlossen werden. Wie wir bereits im letzten Tätigkeitsbericht ausführten, sahen wir diese Lösung kritisch und rieten dazu, die zuerst Genannte zu verfolgen.

Im Berichtszeitraum trat nun nach einigen parlamentarischen Verzögerungen das geänderte Onlinezugangsgesetz (OZG) in Kraft. Es enthält in dem neuen § 8a eine ausdrückliche Regelung zur da-

20 Tätigkeitsbericht Datenschutz 2023, A I 2.3.4.

tenschutzrechtlichen Verantwortlichkeit bei länderübergreifenden Onlinediensten. Danach soll die den jeweiligen Onlinedienst betreibende Behörde datenschutzrechtlich verantwortlich im Sinne von Artikel 4 Nummer 7 DS-GVO sein. Sie hat auch eine eigene Rechtsgrundlage, Antragsdaten zu erheben und an die zuständige Fachbehörde zu übermitteln. Insoweit sind Auftragsverarbeitungsverträge oder Vereinbarungen zur gemeinsamen Verantwortung mit nachnutzenden Behörden obsolet.

Die neue Vorschrift des Onlinezugangsgesetzes könnte jedoch möglicherweise zu datenschutzrechtlichen Problemen führen. Zum einen werden im Falle des Wohngelds von der Staatskanzlei Schleswig-Holstein hochsensible Daten verarbeitet, die dazu geeignet und bestimmt sind, eine Bedürftigkeit der antragstellenden Person und ggf. ihrer Familie nachzuweisen. Die Daten sind allerdings zum Antragszeitpunkt per Definition keine Sozialdaten, da sie hierfür von einer in § 35 Erstes Buch Sozialgesetzbuch (SGB I) genannten Stelle im Rahmen ihrer Aufgabenwahrnehmung verarbeitet werden müssten. Hierzu gehört die Staatskanzlei Schleswig-Holstein nicht, sodass die entsprechenden Daten nicht dem besonderen Schutz des Sozialgeheimnisses unterfallen.

Zudem bedarf jede Datenverarbeitung einer hinreichenden Rechtsgrundlage. Zwar darf die Staatskanzlei Schleswig-Holstein gemäß § 8a Absatz 1 OZG Daten im Rahmen des länderübergreifenden Onlinedienstes verarbeiten. Allerdings ist denkbar, dass diese generalklauselartige Rechtsgrundlage nicht hinreichend bestimmt ist, um derart sensible Daten zu verarbeiten, auch wenn sie nicht unter die Definition von Sozialdaten fallen.

Hinzu kommt, dass § 8a OZG eine strikte Trennung von Antrags- und Fachverfahren vorsieht, wohingegen die Vorschriften aus dem Ersten Buch Sozialgesetzbuch sowie dem Wohngeldgesetz eine solche Trennung gerade nicht vermitteln. So sind Anträge gemäß § 16 Absatz 1 SGB I bei der zuständigen Stelle zu stellen. Zuständig sind nach § 1 Absatz 1 Verordnung zur Durchführung des Wohngeldgesetzes und des Wohngeldsondergesetzes im Land Brandenburg die Landkreise, die kreisfreien Städte sowie alle Städte und Ämter mit 20.000 und mehr Einwohnerinnen und Einwohnern. Es stellt sich somit auch die Frage, welche Stelle zu welchem Zeitpunkt und nach welcher Rechtsvorschrift für die Datenverarbeitung rechtlich zuständig und damit verantwortlich ist.

Die parallel existierenden Normen des neueren, allgemeineren Onlinezugangsgesetzes und des älteren, spezielleren Sozialrechts führen nach unserer gegenwärtigen Auffassung zu gewissen datenschutzrechtlichen Unsicherheiten. Wir diskutieren diese Fragen gegenwärtig auch intensiv mit den Kolleginnen und Kollegen der anderen Datenschutzaufsichtsbehörden und arbeiten an einer deutschlandweit einheitlichen Haltung.

5.3 Einführung der Bezahlkarte für Geflüchtete

Wer nach Deutschland flüchtet und einen Asylantrag stellt, hat grundsätzlich Anspruch auf Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG). Diese Leistungen wurden bislang insbesondere in regelmäßigen Vor-Ort-Terminen in den Leistungsbehörden in Form von Bargeld an die Geflüchteten ausgegeben. Künftig ist jedoch beabsichtigt, diese Leistungen auf eine guthabenbasierte Bezahlkarte mit Debitfunktion zu buchen, ohne den Geflüchteten unmittelbaren Zugriff auf ein dahinterstehendes Konto zu gewähren. Eine Rechtsgrundlage wurde im Berichtszeitraum auf Bundesebene durch die Änderung des Asylbewerberleistungsgesetzes geschaffen. Die konkrete Ausgestaltung der Bezahlkarte ist Ländersache. Auch brandenburgische Landkreise und kreisfreie Städte beabsichtigen, die Bezahlkarte für Geflüchtete einzuführen.

Mit der Karte soll es möglich sein, Waren und Dienstleistungen an jedem üblichen Kartenzahlterminal zu bezahlen und Bargeld in begrenzter Höhe abzuheben. Neben einer Entlastung der Verwaltung hat die Bezahlkarte auch den Zweck, den Geldtransfer ins Ausland zu unterbinden. Daher sind Überweisungen und Lastschriften grundsätzlich ausgeschlossen. Das stellt die Geflüchteten jedoch vor erhebliche Herausforderungen, da die unmittelbare Kartenzahlung nicht immer möglich ist, beispielsweise bei dem Abonnement des Deutschlandtickets, bei medizinischen Zusatzleistungen oder Rechtsberatungen. Daher beabsichtigen Leistungsbehörden, sogenannte Whitelists zu führen. Dabei handelt es sich um Listen mit geprüften und freigegebenen Zahlungsempfängerinnen und -empfängern, an welche die Geflüchteten ausnahmsweise überweisen dürfen bzw. welche Gelder von deren Konten abbuchen können.

Um Überweisungen vornehmen zu können, müsste die geflüchtete Person bei der Leistungsbehörde beantragen, dass bestimmte Zahlungsempfängerinnen oder -empfänger (z. B. eine Rechtsanwältin,

ein Physiotherapeut) in die Whitelist aufgenommen werden. Bei der Antragstellung sollte deren Name und Zahlungsverbindung angegeben werden. Zur Prüfung bedürfte es zudem der Einreichung zahlungsbegründender Unterlagen, z. B. eines Belegs der Leistung oder einer Rechnung. Nach erfolgreicher Prüfung würden die Zahlungsempfängerinnen bzw. -empfänger sodann in die Whitelist aufgenommen.

Das zuständige Ministerium bat uns, die datenschutzrechtliche Zulässigkeit dieses Verfahrens zu prüfen, um eine einheitliche Handhabung der Leistungsbehörden sicherzustellen. Wir haben während der Beratung auf folgende datenschutzrechtliche Gesichtspunkte hingewiesen:

Die oben beschriebene Vorgehensweise ist mit der Verarbeitung einer Vielzahl von personenbezogenen Daten verbunden. Das betrifft einerseits Daten der Geflüchteten (Name, Vertragsbeziehung, Höhe und Grund der Zahlungsverpflichtung), andererseits auch personenbezogene Daten der Zahlungsempfängerinnen und -empfänger (Name und Bankverbindung), soweit es sich hierbei um natürliche Personen handelt. Den zahlungsbegründenden Unterlagen lassen sich zudem meist sensible Informationen entnehmen, etwa Daten eines Kindes zur Anmeldung in einem Verein. Darüber hinaus können auch hoch schutzbedürftige Daten besonderer Kategorien nach Artikel 9 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) betroffen sein, etwa bei Leistungen an Institutionen, die einer bestimmten Ethnie, Religion, politischen Überzeugung oder Weltanschauung nahestehen.

Whitelist – der Inhalt macht den Unterschied

Bei der Frage, ob die Führung einer Whitelist zulässig ist, ist zunächst zu beachten, dass jede Datenverarbeitung einer Rechtsgrundlage bedarf. Das Asylbewerberleistungsgesetz enthält selbst keine einschlägigen Datenverarbeitungsregelungen. Auch die §§ 67 ff. Zehntes Buch Sozialgesetzbuch (SGB X) sind nicht auf die Leistungserbringung nach dem Asylbewerberleistungsgesetz anwendbar, da es sich um keine Sozialleistungen handelt. Insofern könnte die Datenverarbeitung im Zusammenhang mit der Führung einer Whitelist lediglich auf Artikel 6 Absatz 1 Buchstabe e DS-GVO i. V. m. §§ 3 ff. AsylbLG und § 5 Absatz 1 Brandenburgisches Datenschutzgesetz gestützt werden. Hiernach ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig, wenn sie zur Erfüllung der in

der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich ist. Dies gilt jedoch nicht, soweit es sich um personenbezogene Daten besonderer Kategorien (Artikel 9 Absatz 1 DS-GVO) handelt.

Die Aufgabe der Verantwortlichen besteht darin, Leistungen zur Sicherung des Lebensunterhalts für Asylbewerberinnen bzw. Asylbewerber und andere vergleichbare ausländische Staatsangehörige ohne verfestigtes Bleiberecht zu gewähren. Hierzu gehört vor allem, dass die Geflüchteten nach § 3 Absatz 1 Satz 1 AsylbLG Anspruch auf Deckung des notwendigen Bedarfs haben, also an Ernährung, Unterkunft, Heizung, Kleidung, Gesundheitspflege sowie Gebrauchs- und Verbrauchsgütern des Haushalts. Zudem haben die Geflüchteten Anspruch auf Deckung des notwendigen persönlichen Bedarfs nach § 3 Absatz 1 Satz 2 AsylbLG, welcher ihnen zur freien Verwendung gewährt wird.

Wir halten die Führung einer Whitelist auf die oben genannte Art und Weise und die damit verbundene Verarbeitung personenbezogener Daten für die Leistungserbringung nicht für erforderlich und damit für unzulässig, da die Auszahlung der Leistungen auch ohne Führung einer solchen Whitelist erfolgen kann. Auch sehen wir es nicht als Aufgabe der Leistungsbehörde an, das Ausgabeverhalten der Geflüchteten durch Beschränkungen und punktuelle Freigaben zu beeinflussen. Dies gilt vor allem dann, wenn die Leistungen zumindest teilweise zur freien Verwendung gewährt werden, da eine freie Verwendung nur gewährleistet ist, wenn diese frei von Kontrolle und Einwirkung ist.

Etwas anderes gilt zumindest in datenschutzrechtlicher Hinsicht dann, wenn mit der Führung einer Whitelist keine Verarbeitung personenbezogener Daten einhergeht, da das Datenschutzrecht dann nicht mehr anwendbar ist. Das wäre der Fall, wenn Überweisungen an große Institutionen (z. B. Deutsche Bahn, Telekommunikationsdienstleister, medizinische Versorgungszentren, Großkanzleien etc.) ohne vorherige Prüfung ermöglicht würden. Ob dieses Vorgehen zulässig ist, entscheidet sich dann allein an fachrechtlichen Regelungen.

6 Personaldaten in die Cloud?

Mehrere Kommunalverwaltungen wandten sich im Berichtsjahr mit der Frage an uns, ob die Verarbeitung von Beschäftigtendaten – also die Verarbeitung der Daten von Verwaltungsmitarbeiterinnen und -mitarbeitern für Zwecke des Beschäftigungsverhältnisses – auch im Rahmen des sogenannten Cloud Computing erfolgen dürfe. Hintergrund war ein spezielles Angebot eines deutschlandweit agierenden Softwareherstellers. Dieser stellte bestimmte Funktionen in der von ihm entwickelten Personalmanagementsoftware nur noch „in der Cloud“ zur Verfügung. Die in Rede stehenden Kommunalverwaltungen hatten Produkte des Unternehmens zur Personaldatenverarbeitung seit vielen Jahren im Einsatz und wollten auch auf die neuen Funktionen nicht verzichten, z. B. wegen der erleichterten Erfüllung gesetzlicher Meldepflichten. Während die Software bislang jedoch bewusst lokal innerhalb der Verwaltung und unter eigener Administration lief, sollte der Betrieb nun an den Hersteller „in die Cloud“ ausgelagert werden.

Der Begriff Cloud Computing wird im Allgemeinen verwendet, wenn Daten oder IT-Dienste (z. B. Speicherdienste, Rechendienste, Netzwerkdienste, Software) durch Verantwortliche an andere Stellen ausgelagert und die hierbei erforderlichen IT-Ressourcen automatisch und bedarfsgerecht angepasst werden. Die hohe Flexibilität und die optimale Auslastung der Ressourcen können sich in reduzierten Kosten niederschlagen, da Cloud-Dienste meist nach dem konkreten Verbrauch abgerechnet werden.

Aus datenschutzrechtlicher Sicht handelt es sich beim Cloud Computing in der Regel um eine Auftragsverarbeitung gemäß Artikel 28, 29 Datenschutz-Grundverordnung (DS-GVO). Anbieterinnen und Anbieter entsprechender Dienste agieren als Auftragsverarbeiter und führen ihre Aufgaben dementsprechend weisungsgebunden im Auftrag des Verantwortlichen aus. Dieser hat das Recht und auch die Pflicht, die ordnungsgemäße Erbringung der Dienstleistungen zu kontrollieren. Zur Ausgestaltung des Verhältnisses zwischen Verantwortlichem und Auftragsverarbeiter(n) ist ein Vertrag zu schließen, dessen Mindestinhalt Artikel 28 Absatz 3 DS-GVO regelt.

Risiken können u. a. dadurch entstehen, dass Auftragsverarbeiter Teilaufgaben ihrerseits an einen oder mehrere Unterauftragsverarbeiter (Subdienstleisterinnen bzw. Subdienstleister) auslagern. Diese Kette kann lang, komplex und dynamisch sein. Gegebenenfalls ist die Erbringung von Subdienstleistungen auch weltweit verteilt, wenn keine anderweitigen Vorkehrungen getroffen werden. Dies erschwert nicht nur die Kontrolle der Vertragsausführung durch Verantwortliche, sondern auch die Durchsetzung der rechtlichen Anforderungen, die Gewährleistung der Transparenz und Nachvollziehbarkeit der Datenverarbeitung sowie die Wahrung von Betroffenenrechten (z. B. auf Auskunft und Löschung). Weitere Risiken können sich dadurch ergeben, dass Cloud-Anbieterinnen und -Anbieter personenbezogene Daten unbefugt zur Kenntnis nehmen oder gar für eigene Zwecke verwenden. Letzteres bedarf stets einer eigenen Rechtsgrundlage sowohl für die Datenübermittlung an als auch für die Datennutzung durch die Anbieterinnen bzw. Anbieter. Öffentliche Stellen verfügen in der Regel jedoch nicht über eine solche Rechtsgrundlage, um personenbezogene Daten an Auftragsverarbeiter zur Nutzung für deren eigene Zwecke zu übermitteln.

Cloud ist nicht gleich Cloud

Im konkreten Fall stellte sich nach einer kurzen Recherche und der Rücksprache mit den Verantwortlichen heraus, dass die oben beschriebenen Eigenschaften des Cloud Computing hier nur zum Teil vorlagen. Der Softwareanbieter benutzte den Begriff lediglich, um seine Produkte besser zu bewerben. Das „Cloud-Angebot“ bestand darin, einzelne Softwaremodule buchen und deren Nutzung abrechnen zu können. Die gesamte Software sollte jedoch im Rechenzentrum des Herstellers laufen. Für jede (Kommunal-)Verwaltung war geplant, einen eigenen, dedizierten Kundenserver bereitzustellen. Der Hersteller beabsichtigte, die Systemadministration, Softwarepflege und Wartung zu übernehmen und so die Verwaltungen zu entlasten. Es handelte sich datenschutzrechtlich insoweit um eine klassische, einfache Auftragsverarbeitung.

Hiergegen hatten wir keine Bedenken. § 94 Absatz 6 Landesbeamtengesetz regelt ausdrücklich, dass die Verarbeitung von Personalaktendaten der Beamtinnen und Beamten im Auftrag gemäß Artikel 28, 29 DS-GVO möglich ist. Für Tarifbeschäftigte gilt wegen § 26 Absatz 4 Brandenburgisches Datenschutzgesetz nichts anderes. Auch hinsichtlich der Verarbeitung von Personaldaten, die keine Per-

sonalaktendaten sind, sahen wir wegen deren geringerer Sensibilität kein Hindernis für eine Auftragsverarbeitung.

Wir wiesen die Anfragenden darauf hin, Einzelheiten der Auftragsverarbeitung mit dem Softwarehersteller in dem gesetzlich vorgeschriebenen Auftragsverarbeitungsvertrag festzulegen und hierbei die Anforderungen von Artikel 28 Absatz 3 DS-GVO zu beachten. Darüber hinaus machten wir sie darauf aufmerksam, dass durch die Auslagerung der Datenverarbeitung neue Risiken im Vergleich zum Eigenbetrieb entstehen können. Diese sind durch geeignete technische und organisatorische Maßnahmen zu minimieren. Und weiterhin regten wir an – falls dies noch nicht geschehen war – die Fach- und Beratungskompetenz der jeweiligen behördlichen Datenschutzbeauftragten bei der Umsetzung des Projekts einzubeziehen.

7 Kinderfotos auf Internetseiten und in sozialen Medien

Auch in diesem Berichtsjahr erhielt die Landesbeauftragte regelmäßig Beschwerden, Meldungen zu Datenschutzverletzungen und Anfragen zur Anfertigung, Nutzung und Verbreitung von Fotos der Kinder aus Kindertagesstätten. Das Thema war bereits früher praktisch relevant, jedoch haben sowohl die Anzahl der Fälle und Konflikte, gleichzeitig aber auch die Sensibilität für die Persönlichkeitsrechte von Kindern zugenommen.

Die an uns herangetragenen Fälle lassen zwei Muster erkennen:

Entweder fertigen Erzieherinnen bzw. Erzieher oder Beauftragte die Fotos für die Einrichtung an und stellen sie auf deren Webseite, über einen Hosting-Dienst oder in sozialen Medien zur Verfügung. Der Zugang kann dabei auf die Eltern beschränkt sein. Teilweise dienen die Bilder auch der Öffentlichkeitsarbeit. In anderen Fällen nehmen die Eltern die Bilder für private Zwecke auf, um sie Dritten zugänglich zu machen, z. B. in Elterngruppen auf Messenger-Diensten. Nicht selten posten diese Dritten die Fotos dann in sozialen Medien, ohne dass eine Einwilligung hierzu vorliegt.

Uns liegt in diesem Zusammenhang besonders am Herzen, Verantwortliche rechtzeitig für die Anforderungen an Datenschutz und Datensicherheit zu sensibilisieren. Ein behördlicher Datenschutzbeauftragter bat uns im Berichtszeitraum um Prüfung seiner Rechtsauffassung zur Veröffentlichung von Bildern von Kindergartenkindern zum Zweck der Öffentlichkeitsarbeit auf verschiedenen Online-Präsenzen.

Zu Recht ging der Datenschutzbeauftragte davon aus, dass ein solches Vorhaben nicht auf gesetzliche Grundlagen gestützt werden kann, sondern stets eine Einwilligung einzuholen ist. Dies ergibt sich aus § 22 Satz 1 Kunsturhebergesetz (KunstUrhG); die Ausnahmetatbestände des § 23 Absatz 1 KunstUrhG griffen hier nicht. Liegt keine Einwilligung vor, ist die Verbreitung der Aufnahme einer Person grundsätzlich unzulässig. Insbesondere kann sich der Verantwortliche nicht darauf berufen, dass die Öffentlichkeitsarbeit eine öffentliche Aufgabe der Trägerin bzw. des Trägers der Kita und das Werben

mit Fotos hierfür erforderlich im Sinne von Artikel 6 Absatz 1 Buchstabe e Datenschutz-Grundverordnung (DS-GVO) sei.

Damit eine Einwilligung wirksam ist, sind verschiedene Kriterien zu beachten: Zunächst muss sie freiwillig erteilt werden, in diesem Fall durch die Sorgeberechtigten. Dies bedeutet vor allem, dass dem betroffenen Kind oder der bzw. dem Sorgeberechtigten kein Nachteil daraus erwachsen darf, wenn eine Einwilligung nicht erteilt wird. Selbstverständlich darf auch ansonsten kein Druck ausgeübt werden. Problematisch ist – ausweislich mehrerer Beschwerden von Eltern, die eine Einwilligung nicht erteilt hatten und feststellen mussten, dass Bilder ihrer Kinder dennoch angefertigt und verbreitet wurden – oft der praktische Umgang mit einer verweigerten Einwilligung. Es ist sicherzustellen, dass die Anfertigung und Verbreitung von Fotografien von Kindern, für die keine Einwilligung vorliegt, wirksam verhindert wird.

Keine Fotos ohne elterliches OK

Die Einwilligung muss auch informiert erfolgen, insbesondere muss sie die konkreten Modalitäten und Zwecke der Verarbeitung enthalten. Dies geschieht durch Information gemäß Artikel 13 DS-GVO gewährleistet werden. Von besonderer praktischer Bedeutung ist dabei die umfassende Aufklärung über Orte und Formen der Veröffentlichung sowie über den Personenkreis, welcher Zugang zu den Fotos haben soll. Je umfangreicher dieser Personenkreis und je höher damit das Risiko ist, desto mehr ist darauf zu achten, dass die Belehrung ihre Warnfunktion erfüllen kann. Aufgrund der Gefahr einer Verbreitung von Bildern durch andere Eltern ist schließlich ein Hinweis angebracht, dass die Weiterverarbeitung von Bildern fremder Kinder ohne Rechtsgrundlage nicht zulässig ist. Eine Ausnahme kann bei rein persönlichen oder familiären Tätigkeiten vorliegen. Sollten sich die Verarbeitungszwecke bzw. Orte und Formen der Veröffentlichung der Fotos ändern, ist die Einwilligung entsprechend zu ergänzen bzw. zu erneuern.

Gemäß Artikel 7 Absatz 3 DS-GVO ist die Einwilligung jederzeit für die Zukunft widerruflich. Über dieses Widerrufsrecht müssen die Sorgeberechtigten ebenfalls belehrt werden, seine Ausübung ist weder von dem Vorliegen bestimmter Umstände abhängig noch begründungsbedürftig. Die Kita muss bei Widerruf einer Einwilligung sicherstellen, dass Veröffentlichungen existierender Bilder nicht fortgesetzt und die Aufnahmen ggf. gelöscht werden.

Für das Vorliegen aller Elemente einer Einwilligung ist der Verantwortliche (z. B. die Gemeinde als Trägerin der Einrichtung) gemäß Artikel 7 Absatz 1 DS-GVO nachweispflichtig, sodass es sich empfiehlt, sowohl ihre Einholung als auch die Belehrung trotz der grundsätzlichen Formfreiheit in Textform zu dokumentieren.

Zudem hat der Verantwortliche auch die Plattform, auf der eine Veröffentlichung erfolgt, sorgfältig auszuwählen. Insbesondere muss die Plattform die Nutzung der Kinderfotos ausschließlich zu den festgelegten Zwecken ermöglichen und in diesem Kontext technische und organisatorische Schutzmaßnahmen umsetzen, z. B. eine Zugangsbeschränkung auf die Eltern und eine Verschlüsselung.

Gegen die Nutzung von sozialen Medien wie Facebook durch öffentliche Stellen zum Zweck der Selbstdarstellung bestehen nach wie vor datenschutzrechtliche Bedenken.[21]

Die Landesbeauftragte wird durch Empfehlungen, Hinweise und ggf. aufsichtsbehördliches Tätigwerden auf die Einhaltung der datenschutzrechtlichen Anforderungen bei der Verarbeitung von Kinderfotos sowie auf das Verantwortungsbewusstsein und die Sensibilität aller Beteiligten hinwirken.

21 Tätigkeitsbericht Datenschutz 2023, A I 3.

8 Risikobewertung bei Datenschutzverletzungen

Tritt bei einem Verantwortlichen – trotz aller präventiven technischen und organisatorischen Maßnahmen – eine Datenschutzverletzung auf, so muss er diese gemäß Artikel 33 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) der zuständigen Datenschutzaufsichtsbehörde melden, falls die Verletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten einer natürlichen Person führt. Hat sie voraussichtlich sogar ein hohes Risiko zur Folge, so ist der Verantwortliche gemäß Artikel 34 Absatz 1 DS-GVO verpflichtet, auch die betroffenen Personen zu informieren. Die Einstufung des Risikos ist für die Aufarbeitung eines Datenschutzvorfalls somit essenziell, gleichwohl stellt das nachvollziehbare Bewerten oder das Begründen der eigenen Bewertung Verantwortliche regelmäßig vor Probleme.[22] Auch vermeiden einige Verantwortliche, von einem hohen Risiko auszugehen – vermutlich, um eine positive Selbstwahrnehmung aufrechtzuerhalten, keine negativen Schlagzeilen zu verursachen und den Aufwand für die Information betroffener Personen zu vermeiden. Nachfolgend werden zwei Beispielfälle eines Jobcenters dargestellt, welches zwar das richtige Gespür beim Bewerten des Risikos hatte, die Ergebnisse aber nicht korrekt begründen konnte. Dies verhinderte auch, einen möglichen Ansatz zur methodischen und standardisierten Ermittlung bzw. Bewertung möglicher Risiken bei Datenschutzverletzungen abzuleiten.

Im ersten Fall hatte das Jobcenter Bewilligungsbescheide über Bildung und Teilhabe an einen unberechtigten Empfänger übermittelt. Dieser sandte die Dokumente, nachdem er sie geöffnet hatte, an das Jobcenter zurück. Die Bewilligungen beziehen sich in der Regel auf eine besondere Erkrankung der betroffenen Person und lassen somit einen Rückschluss auf personenbezogene Daten besonderer Kategorien gemäß Artikel 9 Absatz 1 DS-GVO – nämlich auf Gesundheitsdaten – zu. Das Jobcenter bewertete das Risiko für die Rechte und Freiheiten des Betroffenen als gering, ohne dies zu begründen. Es teilte auf unsere Rückfrage mit, dass die Bewertung aufgrund der

22 Siehe A III 2.

mangelnden Konkretisierung und des Aussagegehalts zum Gesundheitszustand erfolgt sei.

Im zweiten Fall wurde von dem Jobcenter ein Erwerbsminderungsbescheid, welcher nur aufgrund bestimmter gesundheitlicher Einschränkungen beim Bestreiten des Lebensunterhalts erlassen wird, an eine dritte Person fehlgeleitet. Diesen Bescheid erhielt das Jobcenter ebenfalls zurück, nachdem der unberechtigte Empfänger ihn geöffnet und festgestellt hatte, nicht der richtige Adressat zu sein. Auch hier sah das Jobcenter nur ein geringes Risiko für die Rechte und Freiheiten der betroffenen Person und begründete erst auf Nachfrage die Einstufung damit, dass lediglich der Umstand der Erwerbsminderungsfähigkeit, nicht jedoch der konkrete Anlass bekannt geworden sei.

In beiden Fällen waren die unberechtigten Empfänger dem Jobcenter aus vorherigem Kontakt als zuverlässig und redlich bekannt. Außerdem sind die jeweiligen Dokumente – wenn auch geöffnet – im Original zurückerlangt worden. Die Annahme eines nicht hohen Risikos liegt daher nahe, kann jedoch nicht mit einer reduzierten Auslegung des Begriffs personenbezogener Daten besonderer Kategorien begründet werden. Daher haben wir dem Jobcenter geraten, die Risikobewertung nach der nachfolgenden Methodik vorzunehmen:

Risiken rechtzeitig systematisch einschätzen

Um ein Risiko konkret bestimmen zu können, muss zunächst der Risikobegriff geklärt werden. Hierbei gilt es, sich an bekannten und bewährten Ansätzen des Stands der Technik zu orientieren, wie beispielsweise dem IT-Grundschutz (Managementsystem für IT-Sicherheit), dem Standard-Datenschutzmodell (Methode zur systematischen Umsetzung von Datenschutz) oder den Normen ISO 31000 (Internationaler Standard für Risikomanagement) bzw. ISO 27005 (Managementsystem für IT-Risikomanagement). Denn die Datenschutz-Grundverordnung selbst enthält keine Legaldefinition des Risikobegriffs und keine Methodik zur Risikoermittlung. Infrage kommt jeder Lösungsansatz, der evident logisch und wiederholbar ist. Für vergleichbare Sachverhalte sollte er reproduzierbar analoge Ergebnisse liefern. Entsprechend muss zunächst das „Was“ der Risikobewertung identifiziert werden, um im Anschluss das „Wie“ zu klären.

Hierzu bietet es sich an, zunächst korrelierende Bedrohung-Schwäche-Paare zu bilden und dabei die Perspektive der betroffenen Person einzunehmen. Eine Bedrohung ist ein abstrakt-generelles negatives Ereignis, welches jedoch nur in Verbindung mit einer korrelierenden Schwäche realisiert werden bzw. eintreten kann. In den vorliegenden Fällen wäre als Bedrohung z. B. die „Stigmatisierung und Benachteiligung auf dem Arbeitsmarkt aufgrund einer gesundheitlichen Beeinträchtigung“ und als korrelierende Schwäche die „mangelhafte Absicherung des Postausgangsprozesses gegen Falschadressierung“ anzunehmen. Beides zusammen ergibt ein konkretes Gefährdungsszenario wie „Stigmatisierung und Benachteiligung auf dem Arbeitsmarkt aufgrund einer gesundheitlichen Beeinträchtigung resultierend aus der mangelhaften Absicherung des Postausgangsprozesses gegen Falschadressierung und der damit einhergehenden Übermittlung personenbezogener Daten an Dritte“.

Zur eigentlichen Bewertung des Risikos sind zwei Aspekte zu betrachten: die Eintrittswahrscheinlichkeit und die individuelle Schadenshöhe (aus Perspektive der betroffenen Person). Um die Bewertung beherrschbar zu halten, empfiehlt es sich, eine mehrstufige qualitative Bewertungsskala anzuwenden und sich bei der Anzahl der Abstufungen an bewährten Vorgehensweisen bzw. Standards zu orientieren. Nach Festlegung der Skala und Anzahl der Abstufungen (z. B. drei Stufen – niedrig, mittel, hoch) werden diese für die Schadenshöhe aufsteigend an die Y-Achse und für die Eintrittswahrscheinlichkeiten aufsteigend an die X-Achse eines Koordinatensystems geschrieben. Im Ergebnis entsteht eine sogenannte Risikomatrix, aus der sich für jede Eintrittswahrscheinlichkeit und jede Schadenshöhe an deren Schnittpunkt die Schwere des Risikos ablesen lässt.

In den beiden zugrundeliegenden Fällen war bei der Bewertung der möglichen Schadenshöhe zu berücksichtigen, dass es sich um personenbezogene Daten besonderer Kategorien handelte. Aufgrund der Sensibilität der verarbeiteten Daten und deren Kategorisierung gemäß Artikel 9 Absatz 1 DS-GVO war von einer potenziell hohen Schadenshöhe auszugehen. Die besondere Zuverlässigkeit und Redlichkeit der unberechtigten Empfänger – und alle sonstigen technischen und organisatorischen Maßnahmen – trugen zur Reduzierung der Eintrittswahrscheinlichkeit in Bezug auf die Verletzung der datenschutzrechtlichen Gewährleistungsziele, z. B. der Vertraulichkeit, bei. In beiden vorliegenden Fällen ließ sich anhand der Risikomatrix aufgrund einer niedrigen Eintrittswahrscheinlichkeit und einer mitt-

leren bis hohen Schadenshöhe im Ergebnis kein hohes Risiko ermitteln.

Letztendlich führte die gezeigte Methodik zu keinem anderen Ergebnis als das ursprüngliche Bauchgefühl des Verantwortlichen. Jedoch ermöglicht ihm die vorgeschlagene Vorgehensweise zukünftig, reproduzierbare und verlässliche Risikobewertungen vorzunehmen und diese auch nachvollziehbar zu begründen. Wir empfehlen jedem Verantwortlichen, derartige Überlegungen zur systematischen Bewertung von Risiken durchzuführen und – vorzugsweise organisationsweite – Festlegungen für die Bearbeitung von Datenschutzverletzungen zu treffen.

9 19. Jahrestreffen mit den behördlichen Datenschutzbeauftragten

Im Berichtsjahr führten wir erneut das Jahrestreffen mit den Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Gemeinden durch. Gemeinsam berieten wir datenschutzrechtlich relevante Themen aus ihrer täglichen Arbeit. Traditionelles Ziel dieser ganztägigen Veranstaltung war es, Problemfelder frühzeitig zu erkennen und entsprechende Hilfestellungen zu geben sowie die künftige Begleitung von Projekten in die Wege zu leiten.

Schwerpunkte waren wie im Vorjahr der Einsatz von IT-Systemen mit künstlicher Intelligenz und Datenverarbeitungen auf Grundlage des Onlinezugangsgesetzes, insbesondere die aktuellen Neuregelungen[23] hierzu. Ebenfalls ein wiederkehrendes Thema war der Einsatz von sozialen Medien und Messenger-Diensten in der Verwaltung. Die hohe Aktualität zeigten zahlreiche Anwendungswünsche, die die Datenschutzbeauftragten aus ihrer Praxis einbrachten und intensiv mit uns erörterten. Dies betraf z. B. die Nutzung von YouTube für das Streaming von Gemeindevertretersitzungen, von WhatsApp zur Verteilung von Newslettern und Kontaktaufnahme mit Jugendlichen oder von TikTok zur Öffentlichkeitsarbeit. Auch der aktuelle Stand der Einführung von Microsoft 365 in den Kommunen sowie die hierfür geltenden datenschutzrechtlichen Anforderungen wurden diskutiert. Darüber hinaus war es uns wichtig, über unsere Bewertung der Datenverarbeitung im Zusammenhang mit der Bezahlkarte für Geflüchtete zu berichten.

Wir möchten auch in Zukunft mit den behördlichen Datenschutzbeauftragten im Gespräch bleiben und einen offenen Austausch darüber führen, wo der Datenschutz die Beteiligten vor Herausforderungen stellt und wie er in der Praxis rechtskonform und effektiv umgesetzt werden kann.

---

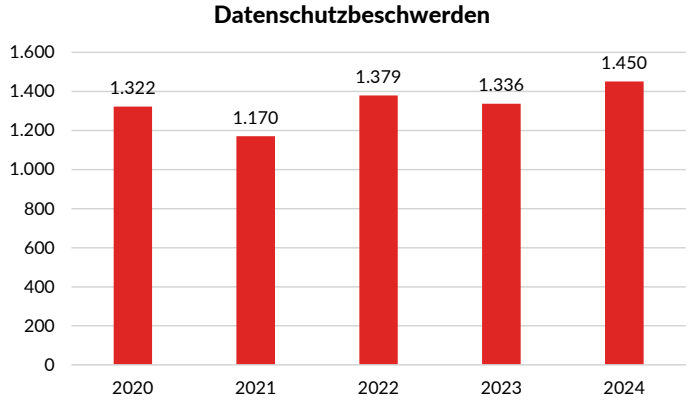
23 Siehe A I, A V 5.1.

Wir danken dem Ministerium des Innern und für Kommunales, das uns erneut einen Sitzungsraum für die Veranstaltung in Potsdam zur Verfügung gestellt hat.

VI Zahlen und Fakten

1 Beschwerden

Im Berichtszeitraum gingen bei der Landesbeauftragten 1.450 schriftliche Beschwerden gemäß Artikel 77 Datenschutz-Grundverordnung ein. Damit hat sich die Anzahl gegenüber dem Vorjahr leicht erhöht und bleibt insgesamt weiter auf hohem Niveau. Die Beschwerden wurden von Personen eingereicht, die der Ansicht waren, dass die Verarbeitung ihrer personenbezogenen Daten sie in ihren Rechten verletzt und gegen das Datenschutzrecht verstößt.



2 Beratungen

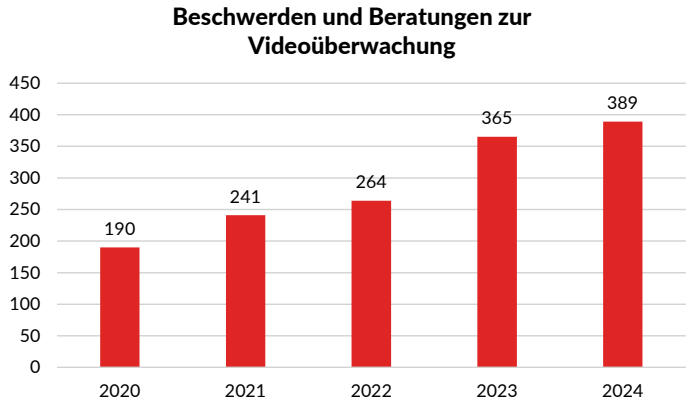
Neben der Bearbeitung von Beschwerden berät die Landesbeauftragte auch zu Datenschutzfragen. Im Berichtsjahr unterstützte sie betroffene Personen, Verantwortliche im öffentlichen und nicht öffentlichen Bereich sowie die Landesregierung bei Rechtsetzungsverfahren in insgesamt 467 Fällen durch schriftliche Stellungnahmen, Hinweise und Anmerkungen, was einen sehr deutlichen Anstieg ge-

genüber dem Vorjahr mit 324 Fällen bedeutet. Hinzu kommt eine Vielzahl telefonischer Beratungen, die nicht statistisch erfasst werden.

3 Videoüberwachung: Beschwerden und Beratungen

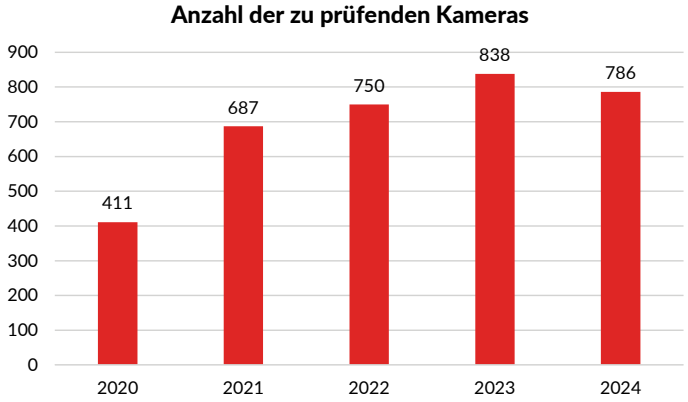
Vielfach wenden sich Bürgerinnen und Bürger an uns, weil sie in ihrem direkten Wohnumfeld mit dem Einsatz von Videokameras konfrontiert werden. Wir nehmen solche Beschwerden zum Anlass, ein Verwaltungsverfahren einzuleiten und den Sachverhalt zu ermitteln. Ergeben sich dabei Anhaltspunkte, dass neben dem eigenen Grundstück auch der Bürgersteig, die Straße oder ein Nachbargrundstück von der Videoüberwachung erfasst werden, haken wir bei den Verantwortlichen nach. In den meisten Fällen geben diese zwar nachvollziehbare Gründe für das Installieren einer Kamera an, wie z. B. die Sicherung des eigenen Grundstücks oder Gebäudes. Die Berechtigung für eine solche Videoüberwachung endet jedoch in der Regel an den eigenen Grundstücksgrenzen. Halten sie diese Grenzen nicht ein, klären wir die Verantwortlichen über die datenschutzrechtliche Zulässigkeit der Videoüberwachung auf.

Im Berichtsjahr erreichten uns 330 Beschwerden (nach 322 Beschwerden im Vorjahr). Darüber hinaus führten wir 59 Beratungen durch (nach 43 Beratungen im Vorjahr). Die Anzahl der Beschwerden und Beratungen ist somit erneut gestiegen und bewegt sich weiterhin auf einem hohen Niveau.



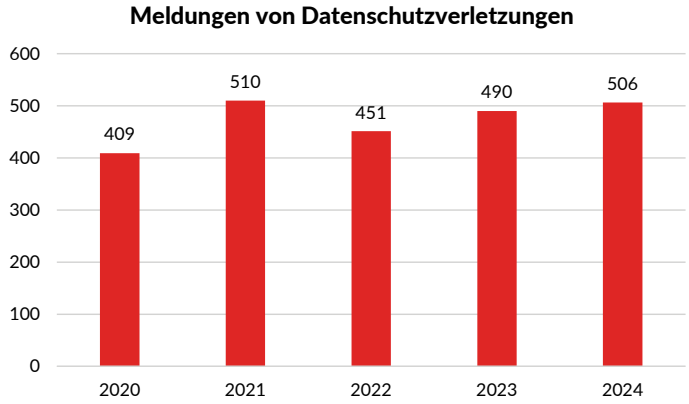
Einen umfangreichen Teil unserer Prüf- und Kontrolltätigkeit stellten außerdem komplexe Sachverhalte dar, in denen beispielsweise ganze Gewerbegebiete und Hotelanlagen mit Kameras ausgerüstet waren. Teilweise wurde auch in Pflegeeinrichtungen umfassend gefilmt – von den Pausenräumen der Mitarbeiterinnen und Mitarbeiter bis hin zu den Betten der Bewohnerinnen und Bewohner. Üblicherweise wird in solchen Fällen eine Vielzahl von Kameras eingesetzt. Die datenschutzrechtliche Bewertung erfordert immer eine Prüfung jeder einzelnen Kamera. Dabei sind u. a. die Besonderheiten des jeweiligen Falls sowie frühere Vorkommnisse, die als Grund für die Videoüberwachung angegeben werden, zu berücksichtigen.

Im Berichtszeitraum hatten wir insgesamt 786 Kameras zu überprüfen.



4 Meldungen von Datenschutzverletzungen

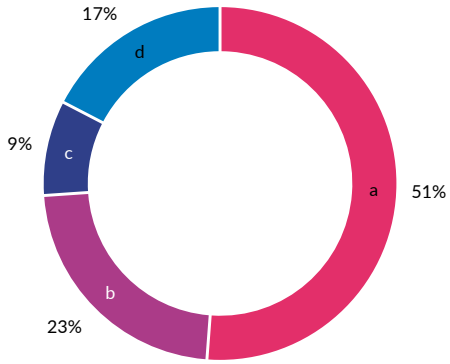
Artikel 33 Datenschutz-Grundverordnung verpflichtet den Verantwortlichen, eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, an die zuständige Datenschutzaufsichtsbehörde zu melden. Die Meldepflicht entfällt nur, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Hat die Verletzung des Schutzes personenbezogener Daten hingegen voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, muss der Verantwortliche zusätzlich zur Meldung bei der Aufsichtsbehörde auch die betroffenen Personen unverzüglich über die Verletzung informieren.



Im Berichtszeitraum erhielt die Landesbeauftragte insgesamt 506 Meldungen von Datenschutzverletzungen. Das bedeutet eine – wenn auch geringfügige – Steigerung gegenüber dem Vorjahr, in welchem 490 Meldungen eingingen. Die Datenschutzverletzungen passierten sowohl im öffentlichen (274 Meldungen) als auch im nicht öffentlichen Bereich (232 Meldungen). Beachtlich ist, dass sich die Zahl der Meldungen durch öffentliche Stellen wiederum überproportional – um ca. 20 % – erhöhte, während die Zahl der Meldungen

durch nicht öffentliche Stellen um ca. 10 % sank. Allerdings geben diese Zahlen nur Auskunft über die Meldungen und nicht über die tatsächliche Zahl der Datenschutzverletzungen.

Art der Datenschutzverletzung



a Fehler beim Versand von Unterlagen
b Hackerangriffe, Viren, Phishing und erpresserische Verschlüsselung
c Diebstahl oder Verlust
d Sonstige Vorfälle

Ungefähr die Hälfte aller Meldungen betraf den Fehlversand von Unterlagen (insgesamt 259 Fälle). Hiervon umfasst sind sowohl Fehlkuvertierungen von Briefpost, versehentlicher E-Mail-Versand an einen offenen Verteilerkreis, Namensverwechslungen oder die Beifügung von Unterlagen unbeteiligter Dritter.

Deutlich gestiegen im Vergleich zum Vorjahr ist hingegen die Anzahl der gemeldeten Datenschutzverletzungen, die auf technischen Mängeln beruhten und insofern Virenbefall, Phishing, Hackerangriffe, unberechtigte Zugriffe Dritter und erpresserische Verschlüsselungen von Datensätzen ermöglichten. Sie erhöhte sich von 83 auf 115. Der Anteil solcher Datenschutzverletzungen stieg damit von 17 % auf 23 %.

Ein Abhandenkommen physischer Datenträger, etwa durch Diebstähle aus Räumen des Verantwortlichen oder durch Verlust auf dem Postweg, wurde der Landesbeauftragten in 44 Fällen gemeldet.

Eine bunte Mischung aus 88 Datenschutzverletzungen fällt in die Kategorie „Sonstiges“. Hier finden sich so unterschiedliche Fälle wie die Übersendung von ärztlichen Befunden via WhatsApp, die Veröffentlichung von Videomitschnitten aus Schulstunden oder der ungewollte Versand von Wahlbenachrichtigungen an Personen, die noch nicht das Alter erreicht hatten, um überhaupt wählen zu dürfen.

Von den meisten gemeldeten Datenschutzverletzungen waren auch im Berichtsjahr jeweils nur wenige Personen betroffen. Dies ist vermutlich, ebenso wie im Vorjahr, mit der großen Menge an fehlversandter Briefpost zu erklären. Hohe Betroffenenzahlen von über 1.000 ergaben sich dagegen etwa bei erfolgreichen Hackerangriffen, in deren Verlauf Datenbestände verschlüsselt und so dem Zugriff der eigentlich Befugten entzogen wurden, oder auch bei der unbeabsichtigten Verwendung eines umfangreichen offenen E-Mail-Verteilers. Der Anteil solcher Fälle machte weniger als 10 % der Meldungen aus.

5 Abhilfemaßnahmen

5.1 Warnungen, Verwarnungen, Anweisungen und Anordnungen

Gemäß Artikel 58 Absatz 2 Datenschutz-Grundverordnung sind die Aufsichtsbehörden befugt, gegen Verantwortliche vorzugehen, die entweder bereits gegen datenschutzrechtliche Vorschriften verstoßen haben oder die unmittelbar davorstehen, datenschutzrechtliche Bestimmungen nicht einzuhalten. Die Befugnisse umfassen u. a. die Möglichkeit, Warnungen, Verwarnungen, Anweisungen und Anordnungen auszusprechen. Insbesondere das Instrument der Warnung hat präventiven Charakter, da diese Maßnahme bereits im Vorfeld eines möglichen Datenschutzverstoßes genutzt werden kann. In diesem Fall ist der Rechtsverstoß noch nicht passiert, würde aber verwirklicht, wenn der Verantwortliche sein Handeln unverändert fortführt. Im Gegensatz dazu rügt eine Verwarnung einen zurückliegenden Datenschutzverstoß. Mit einer Anweisung oder Anordnung werden Verantwortliche zu einem konkreten Tun oder Unterlassen verpflichtet.

Eine Abhilfemaßnahme fasst dabei häufig mehrere Einzelfälle oder Verstöße zusammen. So kann beispielsweise bei einem großflächigen Areal mit einer hohen Anzahl von Kameraüberwachungseinrichtungen eine Vielzahl unterschiedlich zu bewertender Überwachungsszenarien vorliegen. Hier könnte jeweils gegen jede einzelne Kameranutzung eine gesonderte Anordnung ausgesprochen werden. Erfolgt jedoch die Bewertung des Betriebs mehrerer Kameras in einer Maßnahme, muss trotzdem jede für sich geprüft und rechtlich beurteilt werden. Die bloße Zahl der Maßnahmen spiegelt daher nur teilweise die tatsächlich vorgefundenen Umstände wider.

Die Landesbeauftragte sprach im Berichtszeitraum eine Warnung, 22 Verwarnungen und 4 Anordnungen aus, wobei sich 3 Verwarnungen und eine Anordnung gegen öffentliche Stellen richteten. Hinzu kommen die im folgenden Abschnitt behandelten Bußgeldverfahren.

5.2 Geldbußen

Im Berichtszeitraum wurden der Bußgeldstelle der Landesbeauftragten 45 Sachverhalte wegen Verstößen gegen datenschutzrechtliche Vorgaben zur Kenntnis gegeben. Die Verfahren wurden zu einem großen Teil, nämlich in 39 Fällen, von den zuständigen Polizeibehörden oder Staatsanwaltschaften an die Bußgeldstelle weitergeleitet. Insgesamt 4 Sachverhalte haben aufsichtsbehördlich tätige Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten oder andere Aufsichtsbehörden mangels eigener Zuständigkeit an die Bußgeldstelle abgegeben. In einem weiteren Fall wurde ein Ordnungswidrigkeitenverfahren von Amts wegen eingeleitet, in einem anderen zeigte eine Privatperson eine Ordnungswidrigkeit an.

Die Bußgeldstelle schloss im Berichtszeitraum 49 Verfahren ab, die sich sowohl gegen nicht öffentliche Stellen als auch gegen Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen richteten. Etwas weniger als ein Viertel der abgeschlossenen Verfahren war im Vorjahr eröffnet worden.

In 5 Fällen verhängte die Landesbeauftragte wegen der festgestellten datenschutzrechtlichen Verstöße ein Bußgeld. Die Gesamtsumme der festgesetzten Bußgelder betrug knapp 33.500 Euro. In den übrigen Fällen wurde entweder kein Ordnungswidrigkeitenverfahren eingeleitet, das Verfahren eingestellt oder dieses mangels Zuständigkeit an die entsprechende Verfolgungsbehörde abgegeben.

6 Europäische Verfahren

Kapitel VII der Datenschutz-Grundverordnung (DS-GVO) sieht vor, dass bei grenzüberschreitender Datenverarbeitung eine europaweite Zusammenarbeit der Datenschutzaufsichtsbehörden erfolgen muss. Eine solche grenzüberschreitende Verarbeitung liegt z. B. dann vor, wenn der Verantwortliche personenbezogene Daten von betroffenen Personen aus mehreren Mitgliedstaaten verarbeitet oder verarbeiten lässt. Um die Zusammenarbeit der EU-Behörden zu erleichtern, erfolgt der gegenseitige Austausch elektronisch über das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission.

Im Berichtszeitraum erhielt die Landesbeauftragte insgesamt 1.968 einzelne Benachrichtigungen aus dem Binnenmarkt-Informationssystem, hinsichtlich derer sie das Ergreifen von Maßnahmen zu prüfen hatte.

Von allen eingegangenen Benachrichtigungen prüften wir gemäß Artikel 56 DS-GVO in 885 Fällen, die von anderen europäischen Aufsichtsbehörden gemeldet wurden, ob eine Zuständigkeit der Landesbeauftragten als federführende oder betroffene Aufsichtsbehörde in Betracht kommt und entsprechend Verfahrensschritte ergriffen werden müssen. Diese Zahl hat sich gegenüber dem Vorjahr um ca. ein Drittel erhöht. In 18 Fällen – 50 % mehr als im Vorjahr – initiierten wir aufgrund eingegangener Beschwerden selbst ein Verfahren gemäß Artikel 56 DS-GVO. Die Federführung orientiert sich dabei an der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen in der EU. Eine Betroffenheit ist demgegenüber dann gegebenen, wenn die gemeldete Verarbeitungstätigkeit durch die jeweiligen Unternehmen erhebliche Auswirkungen auf Bürgerinnen und Bürger im Land Brandenburg haben könnte oder die verantwortliche Stelle eine Niederlassung im Zuständigkeitsbereich der Landesbeauftragten hat.

Eine Federführung der Landesbeauftragten haben wir in 2 Fällen festgestellt. Bei 54 Fällen ergab sich eine Betroffenheit unserer Dienststelle. In den übrigen Fällen haben wir nach Prüfung der vorliegenden Informationen entschieden, uns nicht an dem weiteren Verfahren zu beteiligen, da die Verantwortlichen keine Niederlas-

sung in Brandenburg hatten und keine erheblichen Auswirkungen auf Brandenburgerinnen und Brandenburger festzustellen waren.

In 987 Fällen beteiligten wir uns an Verfahren der Zusammenarbeit und Kohärenz, etwa im Rahmen gegenseitiger Amtshilfe, bei der Vorbereitung einer Stellungnahme des Europäischen Datenschutzausschusses oder durch Prüfung, ob die Landesbeauftragte einen Einspruch gegen die Entscheidung einer federführenden Aufsichtsbehörde einlegen möchte.

Einen besonderen Schwerpunkt bildete dabei das gegenseitige Amtshilfeverfahren zwischen der Nationalen Kommission für den Datenschutz (CNPD) des Großherzogtums Luxemburg und der Landesbeauftragten. Diese erfolgte zur Bearbeitung von Beschwerden, die gegen das Unternehmen PayPal (Europe) S.à r.l. & Cie, S.C.A. (PayPal) gerichtet waren. PayPal hat seinen europäischen Hauptsitz in Luxemburg, weshalb die CNPD für datenschutzrechtliche Fragestellungen und Beschwerden, die PayPal-Dienste in Europa betreffen, die federführende Aufsichtsbehörde ist. In Brandenburg verfügt das Unternehmen über eine unselbstständige Zweigniederlassung, sodass wir die sachnächste Aufsichtsbehörde innerhalb Deutschlands gemäß § 19 Absatz 2 Satz 1 Bundesdatenschutzgesetz sind. Beschwerden gegen PayPal werden deswegen von anderen deutschen Aufsichtsbehörden weitergereicht und bei uns zentralisiert. Sie werden dann im Rahmen der gegenseitigen Amtshilfe an die CNPD übermittelt und im engen Austausch bearbeitet.

Im Berichtsjahr gingen 40 Beschwerden und weitere Anfragen bei der Landesbeauftragten ein; wir haben sie zum Teil selbst bearbeitet, zum Teil an die CNPD weitergeleitet. Im Vergleich zum Vorjahr hat die Zahl der Beschwerden gegen PayPal damit geringfügig abgenommen. In 19 Verfahren haben wir gegenseitige Amtshilfe gemäß Artikel 61 DS-GVO geleistet – jedem Verfahren lagen bis zu 5 Beschwerden zugrunde.

7 Förmliche Begleitung von Rechtsetzungsvorhaben

Aus den zahlreichen Beratungen ist die Begleitung rechtsetzender Maßnahmen durch die Landesbeauftragte besonders hervorzuheben. Insgesamt nahmen wir im Berichtszeitraum 28 Mal zu Gesetzen, Verordnungen, Satzungen oder Verwaltungsvorschriften Stellung.

Die rechtliche Grundlage zur Beteiligung der Landesbeauftragten folgt aus § 18 Absatz 5 Satz 1 Brandenburgisches Datenschutzgesetz. Danach ist die Landesbeauftragte vor dem Erlass von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, zu hören. Auch die Datenschutz-Grundverordnung überträgt in Artikel 57 Absatz 1 Buchstabe c den Aufsichtsbehörden eine Beratungsfunktion bei rechtsetzenden Maßnahmen.

Bericht nach § 37 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz

1 Speicherung dienstlicher Daten auf privater Festplatte – Beanstandung

Bei der Polizei verarbeitete personenbezogene Daten unterliegen in der Regel einem besonderen Schutzbedarf. Dies gilt sowohl für die Daten von Tatverdächtigen, Täterinnen und Tätern, Zeuginnen und Zeugen sowie Opfern als auch für die Daten der Polizistinnen und Polizisten selbst. Deswegen sind die technischen und organisatorischen Maßnahmen, die die Polizei zur Absicherung der Datenverarbeitung ergreifen muss, an das bestehende erhöhte Risiko für die Rechte und Freiheiten der betroffenen Personen anzupassen. Außerdem ist es unabdingbar, dass alle Bediensteten der Polizei in besonderem Maß im Hinblick auf den Datenschutz und die Informationssicherheit sensibilisiert sind. Um diesen Anforderungen Rechnung zu tragen, arbeitet die Polizei Brandenburg in einem fortlaufenden Prozess an einem Sicherheitskonzept auf Basis des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und setzt entsprechende Maßnahmen um. Weiterhin existieren Richtlinien und Anweisungen für die Mitarbeiterinnen und Mitarbeiter, die klare Vorgaben hinsichtlich des Umgangs mit der Informationstechnik enthalten. Dazu gehört auch, dass der Einsatz privater externer Speichermedien bei der dienstlichen Datenverarbeitung verboten ist.

Dennoch kam es im Berichtszeitraum im Bereich des Polizeipräsidiums zu einem gravierenden Vorfall, der die Wirksamkeit der ergriffenen Maßnahmen erheblich in Frage stellte. Ein Bediensteter in leitender Position hatte eine private USB-Festplatte, die u. a. Filme, private Daten, nicht lizenzierte Software und Schadprogramme enthielt, an einen Dienstrechner angeschlossen und dienstliche Daten im Umfang von ca. 8 Gigabyte auf die Festplatte kopiert. Die übertragenen Daten enthielten umfangreiche Informationen hochsensibler Art, u. a. zu Straftaten, Tatverdächtigen, Opfern sowie Zeuginnen und Zeugen, aber auch zu Beschäftigten der entsprechenden Polizeidienststelle, z. B. dienstliche Beurteilungen und Gesundheitsdaten. Der Beamte verfügte zwar über eine USB-Freigabe – die USB-Schnittstellen an seinem Dienstrechner waren somit für ihn

entsperrt – jedoch verstieß er gegen das oben genannte Verbot.[24] Dass er ein privates Speichermedium anschloss, fiel nur deshalb auf, weil die Schadsoftware auf der Festplatte einen Alarm des Antivirenprogramms auslöste und dieser an das IT-Sicherheitsmanagementteam weitergeleitet wurde.

Im Verlauf der Sachverhaltsermittlung zeigte sich, dass zwar in der Standardeinstellung der Dienstrechner für alle Polizeibediensteten die USB-Schnittstellen für die Benutzung mit Speichermedien gesperrt waren – wie vom BSI verlangt. Jedoch gab es Ausnahmen für eine erhebliche Menge von Einzelpersonen, die sich im Laufe der Jahre angehäuft hatten und in vielen Fällen nicht mehr nachvollziehbar waren. Hierzu gehörte der leitende Beamte.

Schnittstellen überwachen, Datenabflüsse verhindern

Unbestritten ist es in bestimmten Fällen aus dienstlichen Gründen erforderlich, dass Bedienstete über die USB-Schnittstelle auf externe Speichermedien zugreifen können müssen. Allerdings sind diese Bedarfe restriktiv zu prüfen, zu dokumentieren und regelmäßig zu kontrollieren. Darüber hinaus ist es zwingend notwendig, dass nur dienstliche Geräte eingesetzt werden können; alle nicht registrierten Speichermedien sind technisch zu blockieren. Inzwischen hat die Polizei Brandenburg beide Maßnahmen umgesetzt. Der vorliegende Vorfall hätte allerdings verhindert werden können, wenn die Maßnahmen auch in der Vergangenheit bereits implementiert worden wären, so wie der Stand der Technik es bereits seit langem vorgibt und entsprechende IT-Sicherheitsprodukte es ermöglichen.

Im Rahmen der nachträglichen forensischen Untersuchung konnte die Polizei nicht mit absoluter Sicherheit ausschließen, dass die auf die private Festplatte kopierten Daten Unbefugten zur Kenntnis gelangten. So hätte es beispielsweise zu einer Datenübermittlung an Dritte kommen können, wenn der Beamte die Festplatte mit den darauf gespeicherten dienstlichen Daten an den heimischen Computer angeschlossen und eine Schadsoftware die Daten weitergeleitet hätte oder durch Familienmitglieder darauf zugegriffen worden wäre. Die bei der Polizei verarbeiteten sensiblen personenbezoge-

24 Siehe A II 8.2.

nen Daten waren durch sein Handeln insoweit einem erheblichen Risiko ausgesetzt.

Weiter ist auch fraglich, inwieweit die bisher im Polizeipräsidium ergriffenen Sensibilisierungsmaßnahmen ausreichen, wenn es zu einem derart eklatanten Verstoß – insbesondere durch eine Führungsperson – gegen die existierenden internen Richtlinien und Vorgaben kommt. Die Polizei sollte sich darüber Gedanken machen, welche Möglichkeiten sie nutzen kann, um die Beschäftigten in Sachen Datenschutz und Informationssicherheit effektiver als bisher zu schulen.

Darüber hinaus haben sich im Rahmen des Vorfalls auch Mängel im Datenschutzmanagement gezeigt. Nach den gesetzlichen Vorgaben sind Datenschutzverletzungen möglichst innerhalb von 72 Stunden nach Bekanntwerden bei der Landesbeauftragten anzuzeigen. Sollten zu diesem Zeitpunkt noch nicht alle Tatsachen ermittelt worden sein, so genügt eine vorläufige Meldung. Deren Vervollständigung kann schrittweise erfolgen, so wie die Sachverhaltsuntersuchung es ermöglicht. Im vorliegenden Fall erreichte uns die erforderliche Meldung jedoch mit einer Verspätung von über sieben Monaten. Die vorgetragene Begründung konnte die Verzögerung nicht rechtfertigen. Auch die von uns nachgefragten weitergehenden Informationen wurden durch das Polizeipräsidium nur schleppend übermittelt, sodass sich die Sachverhaltsermittlung lange hinzog. Es ist daher unabdingbar, das dortige Datenschutzmanagement zu verbessern, um eine rechtzeitige Meldung von Datenschutzverletzungen – auch in Fällen von Abwesenheit der verantwortlichen Personen – und eine fristgerechte Zusammenarbeit mit der Landesbeauftragten sicherzustellen.

Im Ergebnis hat die Landesbeauftragte Verstöße des Polizeipräsidiums Brandenburg gegen § 17 Absätze 1 und 2, § 29 Absatz 1 und Absatz 3 Satz 2 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) sowie gegen § 64 Absatz 1, § 65 Absätze 1 und 4 Bundesdatenschutzgesetz festgestellt und diese wegen der Schwere und Bedeutung des Vorfalls gemäß § 36 Absatz 1 Nummer 2 BbgPJMDSG beanstandet. Diese Maßnahme bezog sich auf die Verarbeitung von personenbezogenen Daten durch die Polizei u. a. für Zwecke der Strafverfolgung. Soweit in Bezug auf andere Datenverarbeitungen der Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) eröffnet war, haben

wir von einer Verwarnung wegen der Verstöße gegen Artikel 24 Absatz 1, Artikel 25 Absatz 1, Artikel 32 Absatz 1, Artikel 33 Absatz 1 und Artikel 33 Absatz 4 DS-GVO nach Ausübung unseres Ermessens abgesehen.

2 Einsatz des Gesichtserkennungssystems PerIS in Brandenburg

Durch Medienberichte wurden wir Mitte des Berichtszeitraums darauf aufmerksam, dass in den Ländern Baden-Württemberg, Berlin, Brandenburg, Niedersachsen und Nordrhein-Westfalen eine durch die Polizei in Sachsen bereits seit Jahren verwendete mobile Observationstechnik eingesetzt wurde, mit deren Hilfe verdeckt nach Personen und Fahrzeugen gefahndet werden kann. Die Gesichtserkennungssoftware sei in Fahrzeugen verbaut und ermögliche den automatisierten biometrischen Abgleich mit gespeicherten Gesichtsbildern aus polizeilichen Datenbanken in Echtzeit sowie eine spätere Auswertung der Aufzeichnungen. Das Personen-Identifikations-System sei unter der Bezeichnung PerIS bekannt. Es komme u. a. im Land Brandenburg im Rahmen der Amtshilfe durch den Freistaat Sachsen zum Einsatz. Ein konkreter Hinweis auf die Nutzung in Brandenburg ergab sich aus der Antwort des Sächsischen Staatsministeriums des Innern auf eine parlamentarische Anfrage[25], welches eine Amtshilfe mit Observationstechnik und Bilddatenabgleich auf der Grundlage der Strafprozessordnung im Bereich der Eigentumskriminalität bestätigte.

Wir haben daraufhin unverzüglich eine Anfrage zur konkreten Nutzung durch die brandenburgischen Ermittlungsbehörden an die Polizei Brandenburg gerichtet, die letztlich erst nach vier Monaten beantwortet wurde. Darin teilte das Polizeipräsidium mit, dass das Landeskriminalamt in zwei Ermittlungsverfahren der Staatsanwaltschaft Frankfurt (Oder) auf das Verfahren PerIS im Rahmen strafprozessualer Observationsmaßnahmen zurückgegriffen hat. Es handelte sich um Ermittlungen zu schwerer grenzüberschreitender Eigentumskriminalität. Die Erhebung der Bilddaten wurde dabei von der Staatsanwaltschaft auf die Rechtsgrundlage der längerfristigen Observation unter Verwendung bestimmter technischer Mittel (§ 163f Absätze 1, 2 und 3 Satz 1 i. V. m. § 100h Absatz 1 Nummer 2 Strafprozessordnung – StPO) und der Datenabgleich auf die sogenannte

25 Antwort des Staatsministers vom 24. Mai 2024 auf eine Kleine Anfrage, Landtags-Drucksache 7/16308.

Rasterfahndung (§§ 98a Absatz 1 Nummern 5, 6, 98b Absatz 1 StPO) gestützt. In beiden Fällen wurden die beantragten Maßnahmen richterlich angeordnet.

Wir haben das Verfahren PerIS selbst noch nicht näher untersucht, können jedoch auf Erkenntnisse zurückgreifen, die der Sächsische Datenschutzbeauftragte nach einem Einsatz des Gesichtserkennungsverfahrens durch sächsische Polizeibeamte bei einem Fußballspiel 2021 und im Rahmen einer nachfolgenden Vorführung des Programms durch die Polizeidirektion Dresden gewonnen hat. Diese Informationen wurden bereits in seinem Tätigkeitsbericht für das Jahr 2021 veröffentlicht.[26] Danach können die verwendeten Bilddaten sowohl aus fest installierten Kameras in aufgestellten Kamerasäulen als auch aus Kameras stammen, die in sogenannten PerIS-Mobilen eingebaut wurden. Zusammengefasst ist die Software in der Lage, in den erhobenen Bild- oder Videodaten automatisiert nach Gesichts- und Körperbildern zu suchen und auf der Grundlage biometrischer Daten vorhandene Gesichtsmuster bzw. -merkmale zu bestimmen (Gesichtsdetektion), die zum Zweck der Gesichtsidentifikation in nachfolgenden Abgleichen verwendet werden können. Auf diese Weise werden alle in den Rohbildern vorhandenen Gesichter erfasst. Diese bzw. die aus den markanten Merkmalen erstellten Templates werden in einer Referenzdatenbank abgelegt. In einem zweiten Schritt nimmt die Software einen Abgleich mit den von Ermittlerinnen und Ermittlern bereitgestellten Gesichtsbildern vor. Eine Beamtin oder ein Beamter verifiziert anschließend die Treffer bzw. löscht diese bei fehlerhaft festgestellten Ähnlichkeiten in der separaten Trefferdatei. Ein biometrischer Bildabgleich kann sowohl in Echtzeit erfolgen als auch mit zeitlicher Verzögerung von wenigen Minuten bis mehreren Tagen nach der Aufnahme, also retrograd. Ergibt der Abgleich keinen Treffer, werden Bilder in dem Verfahren – anders als bei der in Brandenburg auch eingesetzten automatisierten Kennzeichenfahndung – nicht unverzüglich automatisiert gelöscht. Die Löschung erfolgt je nach Delikt entweder automatisch nach voreingestellten Fristen oder händisch nach der Feststellung, dass das Bild für das Verfahren nicht benötigt wird.

26 https://www.datenschutz.sachsen.de

Biometrische Gesichtserkennung betrifft – insbesondere, wenn sie großflächig im öffentlichen Raum eingesetzt wird – eine Vielzahl von Unbeteiligten. Denn alle von der Kamera erfassten Gesichter werden dem biometrischen Abgleich unterzogen, unabhängig davon, ob die betroffenen Personen in strafrechtlich relevante Handlungen verwickelt sind oder sich rein zufällig an dem Ort der Erfassung aufhalten. Anders als bei der herkömmlichen Videoüberwachung wird jedoch nicht nur beobachtet. Vielmehr werden Personen während oder nach der Überwachung auch identifiziert. Anhand der gespeicherten Templates ist es möglich, dauerhaft zu kontrollieren, wo sich konkrete Personen zu welchem Zeitpunkt aufhalten und wohin sie sich bewegen. Vor dem Abgleich werden nach bisherigen Erkenntnissen auch keine Bilddaten ausgewählt oder ausgefiltert, um die Zahl an Betroffenen zu reduzieren. Die Maßnahme stellt wegen ihrer Streubreite einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar.

Da unsere konkrete Sachverhaltsermittlung in den brandenburgischen Ermittlungsverfahren noch nicht abgeschlossen ist, können wir zu den Details der richterlichen Anordnungen und dem erhobenen Bildmaterial noch keine Aussagen treffen. Darüber hinaus sind wir nicht für die Kontrolle von Gerichten zuständig, sodass uns in beiden Fällen eine datenschutzrechtliche Bewertung der Entscheidungen verwehrt ist. Wir sind jedoch der Auffassung, dass weder die Datenerhebung noch der nachfolgende biometrische Gesichtsabgleich auf die von der Staatsanwaltschaft herangezogenen Rechtsgrundlagen der Strafprozessordnung gestützt werden kann.

Biometrische Daten zur Identifizierung einer natürlichen Person (insbesondere Gesichtsbilder) gehören zu den personenbezogenen Daten besonderer Kategorien nach § 2 Nummer 14 Buchstabe c und Nummer 16 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG), § 500 StPO i. V. m. § 46 Nummern 12 und 14 Buchstabe c Bundesdatenschutzgesetz (BDSG). Bei Verarbeitung dieser Daten ist die Eingriffsintensität in das Persönlichkeitsrecht regelmäßig hoch, weshalb höhere Anforderungen an die Rechtfertigung des Eingriffs zu stellen sind. Der Gesetzgeber hat festgelegt, dass die Verarbeitung dieser Daten zu polizeilichen Zwecken nur erfolgen darf, wenn dies gesetzlich vorgesehen und für die Aufgabenerfüllung unerlässlich (präventive Verarbeitung, § 9 Absatz 1 BbgPJMDSG) bzw. unbedingt erforderlich ist (repressive Verarbeitung, § 48 Absatz 1 BDSG). Für die Verarbeitung

von biometrischen Gesichtsdaten bedarf es daher eindeutiger spezifischer Rechtsgrundlagen.

Die Beobachtungsbefugnis des § 100h i. V. m. § 163f Absatz 2 Satz 1 StPO erlaubt zwar eine längerfristige Observation auch dann, wenn die Erfassung Dritter nicht zu vermeiden ist. Es ist jedoch der hier dargestellten Maßnahme immanent, dass je nach zeitlicher Dauer der Anordnungen hunderte oder tausende Gesichter Unbeteiligter erfasst werden. Dies geht über die gesetzliche Abwägung, dass gezielte Observationen unvermeidlich auch Unbeteiligte betreffen können, weit hinaus. Noch gravierender ist der Eingriff, wenn alle durch die Kameras erfassten Gesichter nachfolgend einem biometrischen automatisierten Gesichtsabgleich unterzogen werden. Die hierfür herangezogene Rasterfahndung nach § 98a Absatz 1 Satz 1 StPO setzt gerade darauf, dass nur jene Daten von Personen, die bestimmte, auf die Täterin bzw. den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, in den maschinellen Abgleich einbezogen werden. Dies ist hier nicht der Fall. Das Verfahren PerIS speichert von jeder Person Bildaufnahmen und erstellt biometrische Abgleichsdaten, die bei einem retrograden Abgleich zudem nicht unmittelbar weiterverarbeitet oder gelöscht werden. Wird der Datenbestand – hier das Bildmaterial – nicht in zeitlicher und örtlicher Hinsicht reduziert bzw. nach potenziell infrage kommenden Verdächtigen gefiltert, sondern unterschiedslos dem Abgleich unterzogen, sehen wir die Verarbeitung nicht mehr als verhältnismäßig an.

Obacht bei der Beobachtung

Dass die Staatsanwaltschaft Frankfurt (Oder) auf die genannten strafprozessualen Normen für die PerIS-Gesichtsbilderhebung und -analyse zurückgreift, deren Bilddaten während des Anordnungszeitraums aus dauerhaft im öffentlichen Raum aufzeichnenden Kameras stammen, und einen (retrograden) Abgleich ohne sofortige automatisierte Löschung vorsieht, erstaunt uns. Denn zumindest hinsichtlich der massenhaften Daueraufzeichnung und des Abgleichs von Kfz-Kennzeichendaten durch das polizeiliche automatische Kennzeichenlesesystem KESY in Brandenburg bestehen einschlägige Erfahrungen mit der Rechtsgrundlage des § 100h StPO. Die darauf gestützte nahezu unbegrenzte Erfassung und Speicherung von Kfz-Kennzeichen von Unbeteiligten im sogenannten Aufzeichnungsmodus haben wir bereits im Jahr 2019 als unverhältnismäßig

angesehen und entsprechend kritisiert.[27] Zwischenzeitlich wurde diese Maßnahme eingestellt. Auch der Bundesgesetzgeber hat, indem er im Jahr 2021 mit § 163g StPO eine strafprozessuale spezifische Befugnis für den automatisierten Kfz-Kennzeichenabgleich im öffentlichen Verkehrsraum schuf[28], auf die Problematik reagiert, dass bestehende Rechtsgrundlagen den Einsatz von automatischen Kennzeichenlesesystemen nur unzureichend rechtfertigen. Zugleich wurden enge Begrenzungen für den automatisierten Abgleich geschaffen, der unverzüglich nach der Datenerhebung erfolgen muss. Es ist naheliegend, dass die bezüglich des Kennzeichenabgleichs geltenden Bedenken erst recht für den Abgleich von Personen bzw. Gesichtsbildern gelten.

Wir haben deshalb unsere Kritik gegenüber der Polizei und Staatsanwaltschaft Frankfurt (Oder) geäußert und um eine Erläuterung der Rechtsgrundlagen in den konkreten Fällen gebeten. Da zwischenzeitlich jedoch Sicherheitsbehörden in mehreren Ländern biometrische Gesichtserkennungssysteme einsetzen, sah die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder es als sachdienlich an, mit einer Entschließung[29] über die datenschutzrechtlichen Gefahren im Zusammenhang mit diesem Eingriff zu informieren. Darüber hinaus wies die Konferenz auf die Vorgaben der europäischen KI-Verordnung[30] hin. Darin hat der europäische Gesetzgeber bestimmte Anwendungen ausgeschlossen und für andere Anwendungen enge Grenzen bestimmt. Sofern nach der KI-Verordnung und dem Verfassungsrecht Regelungsspielraum für

27 Tätigkeitsbericht Datenschutz 2019, B 3.

28 Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 17. März 2021, Bundestags-Drucksache 19/27654, S. 84.

29 Entschließung „Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden“ vom 20. September 2024.

30 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024).

den nationalen Gesetzgeber verbleibt und er den entsprechenden Einsatz als zwingend erforderlich betrachtet, muss er spezifische, verhältnismäßige Rechtsgrundlagen für den Einsatz von Gesichtserkennungssystemen schaffen. Hierin sind in Abhängigkeit von der Eingriffsintensität hinreichende Eingriffsschwellen, ausreichende Anforderungen an den Rechtsgüterschutz und zusätzliche Schutzmechanismen festzulegen.

3 Daten aus Bußgeldverfahren an die polnische Polizei

Im Berichtszeitraum hatte die polnische Polizei die Bußgeldstelle eines Landkreises gebeten, ihr Informationen und Bildmaterial aus einem Ordnungswidrigkeitenverfahren zu übersenden, da sie diese Angaben für eine dort anhängige Anzeige benötigte. Der Landkreis bat uns um Unterstützung bei der Bestimmung der anwendbaren Rechtsgrundlagen.

Die nationalen Übermittlungsgrundlagen der §§ 46 und 49b Ordnungswidrigkeitengesetz (OWiG) i. V. m. § 474 Absatz 1 Strafprozessordnung (StPO) waren nur indirekt anwendbar. Aufgrund des grenzüberschreitenden Bezugs ergab sich dies aus dem Gesetz über die internationale Rechtshilfe in Strafsachen (IRG).

Dieses Gesetz regelt den Rechtshilfeverkehr mit dem Ausland in strafrechtlichen Angelegenheiten, wobei Ordnungswidrigkeiten von diesem Begriff mit umfasst sind. Die eigentlich beim Bund liegende Befugnis, über ausländische Rechtshilfeersuchen zu entscheiden, kann auf Landesregierungen und von dort auf Landesbehörden übertragen werden. Diese Übertragungsbefugnisse wurden genutzt, sodass die örtlich zuständige Staatsanwaltschaft im Land Brandenburg über eingehende Ersuchen um sonstige Rechtshilfe entscheidet. Da die im Ordnungswidrigkeitenverfahren zuständige Verfolgungsbehörde im Bußgeldverfahren dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten hat, war der Landkreis in seiner Eigenschaft als Ordnungswidrigkeitenstelle vom Anwendungsbereich des Gesetzes erfasst.

Die Zulässigkeit der sonstigen Rechtshilfe ist allgemein in § 59 IRG geregelt. Nach § 59 Absatz 3 IRG darf die Rechtshilfe nur geleistet werden, wenn die Voraussetzungen vorliegen, unter denen deutsche Gerichte oder Behörden einander in entsprechenden Fällen Rechtshilfe leisten könnten. Nach nationalem Recht ist der Landkreis berechtigt, der deutschen Polizei auf Ersuchen nach § 161 Absatz 1 StPO Auskünfte aus dem Ordnungswidrigkeitenverfahren nach §§ 46 und 49b OWiG i. V. m. § 474 Absatz 1 StPO zu übermitteln und somit Rechtshilfe zu leisten.

Die Vorschrift zur internationalen Übermittlung personenbezogener Daten bei sonstigen Rechtshilfeersuchen ist § 77d IRG. Da es sich bei Polen um einen Mitgliedstaat der Europäischen Union handelt, sind nach § 97b IRG nur bestimmte Vorgaben des § 77d IRG einschlägig. Aus ihnen folgt, dass personenbezogene Daten im Regelfall an öffentliche Stellen anderer Staaten übermittelt werden dürfen, wenn dies für die Verfolgung von Straftaten oder von Ordnungswidrigkeiten erforderlich ist. Die Normen der Strafprozessordnung und des Ordnungswidrigkeitengesetzes gelten nach § 77 Absatz 1 IRG entsprechend.

Ausweislich der Gesetzesbegründung zum Gesetz über die internationale Rechtshilfe in Strafsachen ist § 77d IRG nicht als Befugnisnorm zu verstehen. Vielmehr muss sich die Befugnis zur Datennutzung und auch die Reichweite der Befugnis aus den einschlägigen rechtshilferechtlichen Vorschriften ergeben, beispielsweise aus § 59 Absätze 1 und 3 IRG. Dies war vorliegend gegeben, da prinzipiell innerstaatliche Rechtshilfe nach §§ 46 und 49b OWiG i. V. m. § 474 Absatz 1 StPO geleistet werden darf. Die polnische Polizei benötigte die Daten für die Verfolgung der dort anhängigen Strafanzeige, insofern war die Datenübermittlung auch erforderlich. Der Landkreis hatte die Daten bereits zur Durchführung des eigenen Bußgeldverfahrens erhoben. Insofern durfte er aufgrund der obigen Normen diese in erforderlichem Umfang an die polnische Polizei übermitteln.

4 Übermittlung eines Lichtbilds auf Verlangen der Staatsanwaltschaft

Im Berichtszeitraum wurde die Frage an uns herangetragen, auf welche Rechtsgrundlagen sich das Zusammenspiel aus Anfordern von personenbezogenen Daten durch die Staatsanwaltschaft und Übermitteln solcher Daten durch eine Verwaltungsbehörde stützt. Konkret begehrte eine Staatsanwaltschaft von einer kommunalen Führerscheinstelle die Übersendung eines Lichtbilds, da sie dieses in einem Ermittlungsverfahren gegen die abgebildete Person benötigte.

Die Staatsanwaltschaft vertrat die Auffassung, dass die Führerscheinstelle verpflichtet sei, ihr das Lichtbild allein auf Grundlage von § 161 Strafprozessordnung (StPO) zu übermitteln. Die Führerscheinstelle war der Ansicht, dass sie dafür eine eigene Rechtsgrundlage benötige, die aber nicht gegeben sei. § 161 StPO regelt, dass die Staatsanwaltschaft zur Aufklärung des Sachverhalts befugt ist, von allen Behörden Auskunft zu verlangen. Im vorliegenden Fall hatte die Führerscheinstelle das Lichtbild sogar rechtswidrig gespeichert. Deshalb durfte sie es im Ergebnis nicht übersenden.

Bei der Übersendung des Lichtbilds handelt es sich um eine Zweckänderung, da das Lichtbild ursprünglich nicht zu dem Zweck gespeichert wurde, es an die Staatsanwaltschaft zu übermitteln. Die für die Führerscheinstelle grundsätzlich anzuwendende zweckändernde Übermittlungsvorschrift ist Artikel 6 Absatz 1 Buchstabe c oder e, Absatz 3 Buchstabe b, Absatz 4 Datenschutz-Grundverordnung (DS-GVO) i. V. m. §§ 5 und 6 Absatz 1 Nummer 3 Brandenburgisches Datenschutzgesetz (BbgDSG) i. V. m. Artikel 35 Grundgesetz. § 6 Absatz 1 Nummer 3 BbgDSG legen wir dahingehend aus, dass er auch bei Ersuchen der Staatsanwaltschaft gilt.

Da die Führerscheinstelle das Lichtbild zum Zeitpunkt des Auskunftsverlangens der Staatsanwaltschaft unzulässig gespeichert hatte, konnte sie sich aber nicht auf die obige Zweckänderungsvorschrift berufen. Denn ein einmal rechtswidrig verarbeitetes personenbezogenes Datum kann nicht durch eine weitere Verarbeitung rechtmäßig werden.

Selbst die von uns nicht geteilte Annahme, dass allein aus § 161 StPO die rechtliche Pflicht zur Übermittlung personenbezogener Daten resultiere, ohne dass es einer zweckändernden Übermittlungsnorm bedürfe oder dass § 161 StPO selbst die zweckändernde Übermittlungsnorm sei, hätte die Rechtswidrigkeit der Übermittlung nicht heilen können. Denn das Rechtmäßigkeitsprinzip würde umgangen, wenn aufgrund des § 161 StPO eine Übermittlung rechtswidrig gespeicherter Daten möglich wäre, die gleichzeitig nach Datenschutzrecht untersagt ist.

Insofern teilten wir die Auffassung der Führerscheinstelle.

5 Zahlen und Fakten

Im Berichtszeitraum befasste sich die Landesbeauftragte mit insgesamt 37 Beschwerden von Bürgerinnen und Bürgern über die Tätigkeit der Polizei und Staatsanwaltschaften. Diese betrafen auch Verfahren aus früheren Berichtszeiträumen. Inhaltlich handelte es sich im Wesentlichen um Fragen zum Umgang mit personenbezogenen Daten durch die Polizei im Rahmen der Wahrnehmung von Betroffenenrechten. In knapp 30 Fällen berieten wir sowohl Verantwortliche als auch Rat suchende Bürgerinnen und Bürger schriftlich zu datenschutzrechtlichen Fragestellungen. Zusätzlich berieten wir in einer Vielzahl von Fällen telefonisch, ohne dies statistisch zu erfassen.

Wir begleiteten im Berichtszeitraum ein polizeirechtliches Gesetzesvorhaben mittels Stellungnahmen und Beratungen und standen dabei im Austausch mit dem zuständigen Referat im Ministerium des Innern und für Kommunales.

Die verantwortlichen Stellen der Polizei erstatteten der Landesbeauftragten 17 Meldungen über Verletzungen der Sicherheit personenbezogener Daten gemäß § 29 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz bzw. § 65 Bundesdatenschutzgesetz. Diese beziehen sich fast ausschließlich auf Vorfälle bei der Verarbeitung von Daten zu gefahrenabwehrrechtlichen oder repressiven Zwecken.

Im Einzelnen erhielten wir 8 Meldungen vom Zentraldienst der Polizei, 8 Meldungen vom Polizeipräsidium und eine Meldung von der Hochschule der Polizei. Die Meldungen des Zentraldienstes der Polizei standen alle im Zusammenhang mit der Bearbeitung von Verwarnungsverfahren durch die Zentrale Bußgeldstelle der Polizei. Mehrfach wurden aufgrund von Mängeln im Kuvertierungsprozess Dokumente an nicht berechtigte Personen fehlversandt. Ein Fall betraf eine Abfrage im Fahreignungsregister, ein weiterer die unzulängliche Bildnachbearbeitung eines Blitzerfotos. Die Meldungen aus dem Polizeipräsidium bezogen sich sowohl auf technische Störungen, z. B. die ungewollt erweiterte Aufzeichnung von Funksprüchen, als auch auf den fehlerhaften unbeabsichtigten wie auch vorsätzlich rechtswidrigen Umgang mit Daten oder IT-Technik durch Polizeibedienstete.

In einem Fall sprachen wir eine Beanstandung gegenüber der Polizei aus, in der es um die verzögerte Meldung einer Verletzung der Sicherheit personenbezogener Daten ging.[31] Nach den gesetzlichen Vorgaben hat der Verantwortliche die Meldung unverzüglich nach Bekanntwerden, möglichst innerhalb von 72 Stunden, an uns zu übermitteln. Erfolgt die Meldung zu einem späteren Zeitpunkt, muss sie eine Begründung für die Verzögerung enthalten. Sofern die Sachverhaltsaufklärung noch andauert, ist zunächst eine Vorabmeldung zu erstatten, die zu einem späteren Zeitpunkt ergänzt wird.

Wir registrieren alle Meldungen und bewerten insbesondere die von der Polizei vorgenommenen Abhilfemaßnahmen. Wenn die Ursachen der Datenschutzverletzung nicht umgehend beseitigt werden können, wir den Vorfall als gravierend einstufen oder erkennbar weiterer Ermittlungsbedarf besteht, werden wir gegenüber dem Verantwortlichen aufsichtsrechtlich tätig. Dies war neben der oben erwähnten Beanstandung noch in zwei Fällen erforderlich: Einer betraf eine Störung im internen Polizeinetz, der andere einen auch in den Medien aufgegriffenen Vorfall bei der Nutzung eines Netzwerkspeichers im Landeskriminalamt.

31 Siehe B 1.

Die Dienststelle

1 Öffentlichkeitsarbeit

Jedes Jahr führt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz), zu deren Mitgliedern die Landesbeauftragte zählt, eine zentrale Veranstaltung anlässlich des Europäischen Datenschutztags durch. Im Berichtsjahr stand diese unter der Überschrift „Digitale Transformation – die Datenschutz-Zukunft gestalten“. Renommierte Expertinnen und Experten aus Deutschland und der EU hielten Vorträge zu Themen wie dem Europäischen Gesundheitsdatenraum oder Privacy-Enhancing Technologies und deren Auswirkungen auf die Arbeit von Datenschutzaufsichtsbehörden. Ausgerichtet wurde die Veranstaltung von der Landesbeauftragten für Datenschutz Schleswig-Holstein als Vorjahresvorsitzenden der Datenschutzkonferenz in Berlin.

Am 1. Juni 2024 veranstaltete der Landtag Brandenburg erneut einen Tag der offenen Tür. Interessierte Bürgerinnen und Bürger hatten dabei wieder Gelegenheit, das Parlamentsgebäude zu erkunden und Einblicke in die Arbeit nicht nur der Abgeordneten und Landtagsbeschäftigten, sondern auch der Mitarbeiterinnen und Mitarbeiter verschiedener Landesbehörden und -einrichtungen zu gewinnen. Wie schon in der Vergangenheit war die Landesbeauftragte auch dieses Mal wieder mit einem Informationsstand vertreten. Als Schwerpunkt wählten wir erneut das Thema „Videoüberwachung in der Nachbarschaft“, da nachbarliche Videokameras in der täglichen Bearbeitung von Beschwerdefällen weiterhin als häufiger Beschwerdegrund auftreten. Weil der 1. Juni als Internationaler Kindertag dem Einsatz für die Bedürfnisse und Rechte von Kindern gewidmet ist, lag ein spezieller Fokus der Veranstaltung auf dem jüngeren Publikum. Auch das Standangebot der Landesbeauftragten war in besonderer Weise auf Kinder zugeschnitten: Die zentrale Komponente bildete ein buntes Klemmbaustein-Modell einer typischen Wohnsiedlung mit besonders anschaulichen, durch reale Fälle inspirierten Szenen unzulässiger Videoüberwachung. Diese Form spielerischer Interaktion diente als Auftakt für ein Gespräch, das die Kinder über die Frage nach dem Grund der Unzulässigkeit an den Begriff des Privaten heranführte und die Erwachsenen für die Erfordernisse und Grenzen datenschutzkonformer Videoüberwachung sensibilisierte. Als vertiefende Lektüre erhielten die Kinder zum Abschluss je nach

Alter eines von zwei Bilderbüchern des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die in kindgerechter Weise grundlegendes Wissen zum Thema Datenschutz vermitteln; den Erwachsenen bot das von der Landesbeauftragten herausgegebene Faltblatt „Videoüberwachung in der Nachbarschaft“ Hinweise für einen datenschutzgerechten Betrieb von Videokameras.

Die Landesbeauftragte hält für diejenigen, die sich über Datenschutzrecht informieren möchten, vielfältiges Informationsmaterial in gedruckter und digitaler Form bereit. So stellt sie beispielsweise zentrale Rechtstexte als Druckbroschüren bereit. Unter den Gesetzen, die so zur Verfügung gestellt werden, sind das Brandenburgische Datenschutzgesetz und das Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz. Beide Broschüren gingen infolge reger Nachfrage im Berichtsjahr schließlich zur Neige, sodass ein erneuter Druck erforderlich wurde. Während im Fall der Broschüre Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz nur geringfügige redaktionelle Änderungen nötig waren, bedurfte die Broschüre Brandenburgisches Datenschutzgesetz auch einer inhaltlichen Anpassung, da das Gesetz zwischenzeitlich leicht geändert worden war. Die Broschüren wurden schließlich als 2., korrigierte bzw. 9., aktualisierte Auflage neu herausgegeben.

Das Engagement der Landesbeauftragten zur Aufklärung über und Sensibilisierung für Datenschutz umfasst neben der Herausgabe entsprechender Informationsmaterialien und der Unterstützung von Veranstaltungen wie Tagen der offenen Tür auch den persönlichen Auftritt als Rednerin bei Fachtagungen und Expertenkonferenzen. Im Berichtsjahr referierte die Landesbeauftragte beispielsweise auf dem Datenschutzkongress 2024, einer Veranstaltung des Handelsblatts, über „KI aus Perspektive einer Aufsichtsbehörde“. In ihrem Vortrag sprach sie über die Anforderungen an Verantwortliche, die Einbindung von Auftragsverarbeitern, Dokumentationspflichten, Betroffenenrechte und Sanktionen und schloss mit dem Fazit, dass die Erfahrung aus der Umsetzung der Datenschutz-Grundverordnung öffentlichen wie nicht öffentlichen Stellen bei der Umsetzung der KI-Verordnung als nützliche Orientierung dienen kann.

Der Gerichtshof der Europäischen Union entscheidet über grundlegende Fragen zur Auslegung der Datenschutz-Grundverordnung. Seinen Urteilen kommt für die Datenschutzpraxis daher eine hohe

Bedeutung zu. Vor diesem Hintergrund führt die Landesbeauftragte auf einer Schwerpunktseite ihres Internetangebots eine Liste ausgewählter Entscheidungen des Gerichtshofs, die ständig fortgeschrieben wird. Auch im Berichtsjahr haben wir diese Liste wieder um einige richtungsweisende Urteile erweitert. Diese betrafen die Verhängung von Bußgeldern gegen juristische Personen, automatisierte Bonitätsberechnungen, Informationen zu Restschuldbefreiungen in Datenbanken privater Wirtschaftsauskunfteien, Schadenersatz bei Cyberangriffen, die Datenverarbeitung in parlamentarischen Untersuchungsausschüssen, die Versteigerung personenbezogener Daten für Werbezwecke, die Vorratsspeicherung von IP-Adressen zur Bekämpfung von Straftaten und die Datenverarbeitung zu Werbezwecken durch soziale Netzwerke.

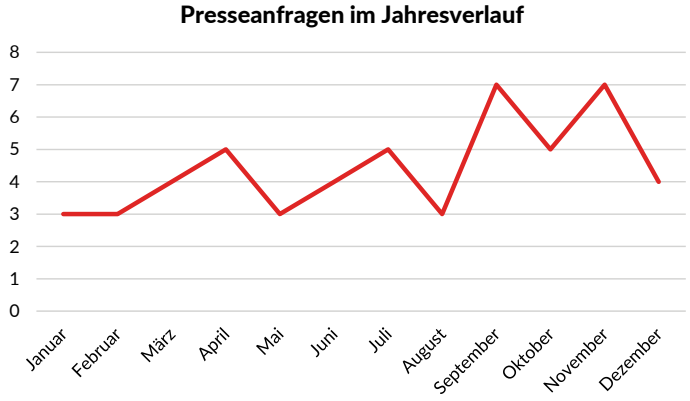
In Orientierungshilfen und Anwendungshinweisen gibt die Datenschutzkonferenz Antworten auf wichtige Fragen zu Auslegung und Umsetzung datenschutzrechtlicher Vorschriften. Als Konferenzmitglied wirkt die Landesbeauftragte an der Erarbeitung solcher Papiere mit. Im Berichtsjahr wuchs das Angebot abermals: Neu hinzu kamen eine Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ mit Kriterien für eine datenschutzkonforme Nutzung von Anwendungen Künstlicher Intelligenz, eine Orientierungshilfe „Datenverarbeitung im Zusammenhang mit funkbasierten Zählern“, die sich mit Fragen rund um die Rechtmäßigkeit funkgesteuerter Erhebung und Übermittlung von Verbrauchsdaten befasst, und eine Orientierungshilfe „Ausgewählte Fragestellungen des neuen Onlinezugangsgesetzes“, die erläutert, welche datenschutzrelevanten Neuregelungen das Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung vom 19. Juli 2024 mit sich bringt. Zudem wurden drei existierende Papiere überarbeitet und mit neuer Versionsnummer veröffentlicht, nämlich die Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressierten als Version 1.0, die Orientierungshilfe für Anbieterinnen und Anbieter digitaler Dienste als Version 1.2 und das den Anwendungshinweisen zugeordnete Papier „Das Standard-Datenschutzmodell“ als Version 3.1. Alle genannten Dokumente sind im Internetangebot der Landesbeauftragten abrufbar.

Einheitlichkeit in der Anwendung der EU-Datenschutzvorschriften ist eines der wesentlichen Ziele des Europäischen Datenschutzausschusses. Zu diesem Zweck gibt er u. a. sogenannte Leitlinien heraus. Üblicherweise erscheinen diese zunächst in englischer Sprache und

werden nach ihrer Veröffentlichung in andere Sprachen der Europäischen Union übersetzt. Die Landesbeauftragte hält ausgewählte Leitlinien auf ihrer Internetseite bereit und ist bestrebt, deren deutsche Übersetzung zur Verfügung zu stellen, sobald sie vorliegt. Grund zur Aktualisierung dieses Angebots gab im Berichtsjahr die Verfügbarkeit einiger neuer Übersetzungen, etwa im Falle der „Leitlinien 04/2022 für die Berechnung von Geldbußen im Sinne der DS-GVO“ oder der „Leitlinien 05/2022 über den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung“.

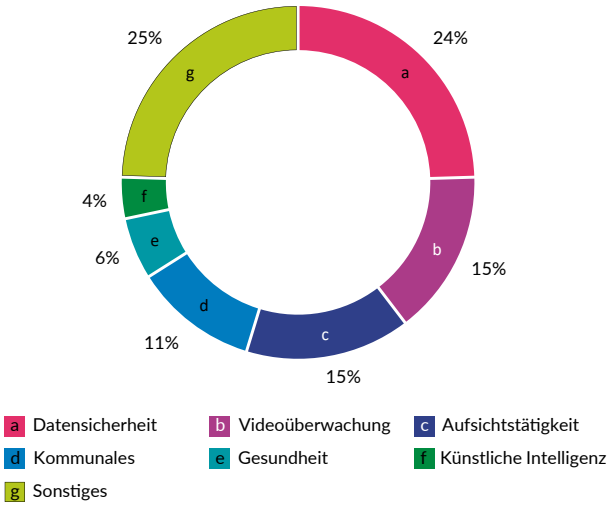
2 Pressearbeit

Im Berichtszeitraum haben wir 53 Medienanfragen zum Datenschutz erhalten. Das war ca. ein Viertel weniger als im Vorjahr. Im monatlichen Vergleich erreichten uns die meisten Anfragen im Herbst.



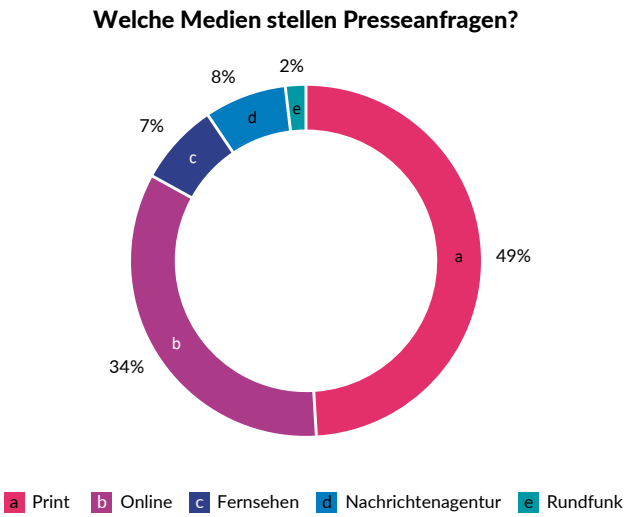
Die thematischen Schwerpunkte der Presseanfragen variierten stark. Am häufigsten bezogen sie sich auf Datensicherheit im weiteren Sinne. Dazu gehören – im Sinne dieser Statistik – auch Fragen zum Datenschutz im Internet sowie zu bekanntgewordenen Datenschutzverletzungen („Datenpannen“). Mit einem größeren Abstand folgte die Videoüberwachung. Diesem Schlagwort haben wir auch zwei Anfragen zugeordnet, die sich auf die Verarbeitung durch Fotografie oder Sprachaufzeichnungen richteten. Die klassische Datenverarbeitung durch kommunale Verwaltungen war ein dritter wesentlicher Schwerpunkt.

Schwerpunkte der Presseanfragen



Lässt man jene Fragen, die keinen Verantwortlichen unmittelbar betrafen, unberücksichtigt, haben sich 57 % der Presseanfragen auf die Datenverarbeitung durch Unternehmen gerichtet. 38 % bezogen sich auf öffentliche Stellen und lediglich 5 % auf Privatpersonen.

Anfragen, die in einer Online-Berichterstattung münden sollen, stellen inzwischen ein Drittel der an die Landesbeauftragte gerichteten Presseanfragen. Anliegen von Journalistinnen und Journalisten, die in Print-Medien berichten, machten etwa die Hälfte der gesamten Anfragen aus. Sowohl Online- als auch Print-Medien haben ihren Anteil damit im Vergleich zum Vorjahr erheblich gesteigert. Für Anfragen von Nachrichtenagenturen und Fernsehsendern hingegen war im Vergleich zum Vorjahr ein Rückgang zu verzeichnen. Die Abgrenzung zwischen den einzelnen Arten der Medien bleibt allerdings weiterhin schwer, da viele ihre Berichterstattung inzwischen in unterschiedlicher Form anbieten.



Nachdem das Interesse an einem großen europäischen Verfahren mit brandenburgischem Bezug bereits vor Beginn des Berichtszeitraums abgeebbt war, verringerte sich auch wieder die Zahl der Anfragen von internationalen Medien, und zwar von 12 % im Vorjahr auf nunmehr 4 %. Anfragen von Medien aus den Ländern Brandenburg oder Berlin legten geringfügig auf 56 % zu. In ähnlicher Weise nahmen Anfragen von Journalistinnen und Journalisten aus anderen Bundesländern oder von überregional tätigen Medien auf 40 % zu.

3 Personal und Organisation der Dienststelle

Im Berichtsjahr war die Personalsituation weiter sehr angespannt. Zwar verfügt die Dienststelle über 44 planmäßige Stellen, jedoch waren im Berichtsjahr Abgänge von 7 Mitarbeiterinnen und Mitarbeiter zu verzeichnen. Diese betrafen alle Bereiche der Dienststelle. Es gelang zwar, 5 Stellen nachzubesetzen, allerdings nur mit erheblichem Verwaltungsaufwand für die Durchführung zahlreicher, zum Teil erfolgloser Bewerbungsverfahren – z. B. bedurfte es für eine Stelle 9 Ausschreibungen. Zudem waren aufgrund von Kündigungsfristen seitens der Bewerberinnen und Bewerber oftmals mehrere Monate an Vakanz zu überbrücken. Eine besondere Herausforderung bedeutete in diesem Kontext die Nichtbesetzung einzelner Führungspositionen.

Die vielen unbesetzten Stellen, die es zu vertreten galt, führten erneut zu einer sehr hohen Belastung der anderen Mitarbeiterinnen und Mitarbeiter. Hinzu kam wieder ein hoher Krankenstand mit teils langen Ausfallzeiten, wie er auch bei anderen Behörden und Unternehmen festzustellen war. Die Kompensation gelang auch mit großen Anstrengungen nur teilweise. Für Beschwerde führende Personen bedeutete dies, dass sie oftmals viel Geduld für die Bearbeitung ihrer Anliegen aufbringen mussten. Dies ist angesichts der gesetzlich z. B. in der Datenschutz-Grundverordnung geregelten Fristen für die Beschwerdebearbeitung nicht zufriedenstellend.

An dieser Stelle möchte ich mich wie bereits in den Jahren zuvor bei allen Beschäftigten meiner Dienststelle für die geleistete Mehrarbeit und die großen Bemühungen, trotz aller Probleme so bürgerfreundlich wie möglich zu arbeiten, herzlich bedanken.

Leider ist nicht zu erwarten, dass sich die Personalsituation in den kommenden Jahren wesentlich verbessern wird. Dies liegt zum einen an der hohen Fluktuation an Beschäftigten, die auch andere Branchen trifft. Darüber hinaus wird auch diese Dienststelle das Ausscheiden der geburtenstarken Jahrgänge aus dem Erwerbsleben zu verkraften haben. Bereits jetzt plane und beginne ich Maßnahmen zum Transfer von Wissen, zur Übergabe von Funktionen und zur Aufrechterhaltung der ordnungsgemäßen Aufgabenerfüllung.

Die angespannte Raumsituation meiner Behörde konnte auch im Berichtszeitraum nicht gelöst werden. Zwar ist die Sanierung von einigen Räumen eines Nachbargebäudes auf der Liegenschaft in Planung, eine Umsetzung zum Ende des Berichtszeitraums allerdings noch nicht absehbar. Das Gebäude ist mit Fahrstühlen ausgestattet und rollstuhlgeeignet.

Erfreulich war, dass der Brandenburgische Landesbetrieb für Liegenschaften und Bauen im Berichtsjahr bereits Verbesserungen mit Blick auf die Behindertenfreundlichkeit der drei bestehenden Häuser meiner Dienststelle vorgenommen hat. So wurden vor allen Hauseingängen Geländer angebracht und in einem Haus eine spezielle Sanitäreinrichtung verbaut. Leider bleibt das grundsätzliche Problem der Barrierefreiheit nach wie vor bestehen; insbesondere kann keines der drei Häuser mit einem Rollstuhl genutzt werden.

Die Liegenschaft wird weiterhin regelmäßig von Wildschweinrotten aufgesucht. Nicht nur werden die Grünflächen dabei oftmals umgegraben, sondern auch die Mülltonnen immer wieder umgeworfen. Ihr Inhalt verteilt sich großflächig auf der Liegenschaft und dem angrenzenden Bürgersteig. Mittlerweile sind die Tiere auch tagsüber aktiv. Die Bachen säugen ihre Frischlinge inzwischen sogar ganz ungerührt während der Mittagszeit in der Toreinfahrt.

Bedauerlich ist, dass in der Umgebung der Dienststelle mehrere Möglichkeiten der auswärtigen Mittagsversorgung weggefallen sind. Sowohl die Kantine des benachbarten Julius Kühn-Instituts als auch jene im zu Fuß erreichbaren Europarc Dreilinden schlossen. Auch dies ist für den Behördenstandort Kleinmachnow nicht unbedingt attraktivitätssteigernd.

Kontakt

Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Telefax: 033203 356-49
E-Mail: Poststelle@LDA.Brandenburg.de

www.LDA.Brandenburg.de