Landesbeauftragte
für Datenschutz
und Akteneinsicht

Tätigkeitsbericht
Datenschutz 2025

Tätigkeitsbericht Datenschutz

der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht

zum 31. Dezember 2025

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 2025 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: Institut für Physik und Astronomie
Universität Potsdam
Foto: Detlev Kozian,
BLK2 Architekten PartG mbB

Druck: Landesvermessung und Geobasisinformation
Brandenburg

Vorwort

Liebe Leserinnen und Leser,

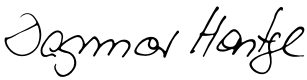
mit dem vorliegenden Tätigkeitsbericht möchte ich Sie wieder über wichtige datenschutzrechtliche Themen sowie ausgewählte Beratungs- und Beschwerdefälle informieren, mit denen sich meine Behörde im Berichtsjahr befasst hat.

Bereits das dritte Jahr in Folge war die Künstliche Intelligenz (KI) wesentlicher Schwerpunkt der Arbeit meiner Behörde. Kein anderes Themenfeld entwickelt sich mit einer vergleichbaren Dynamik. Nicht nur in Unternehmen, sondern auch in der öffentlichen Verwaltung werden die Projekte immer konkreter. So unterstützen KI-Systeme die Verwaltung bereits beim ersten Bürgerkontakt über das Internet. Auch prüfen Behörden die Vollständigkeit eingereichter Unterlagen in unterschiedlichen Antragsverfahren teilweise schon mithilfe Künstlicher Intelligenz. Schließlich stellen Schulen den Schülerinnen und Schülern erstmals einen Chatbot als Lernunterstützung zur Seite. In der Einführungsphase dieser Projekte bemühe ich mich mit meinen Mitarbeiterinnen und Mitarbeitern darum, insbesondere mit Hinweisen und Beratungsangeboten für Verantwortliche auf die Einhaltung des Datenschutzes hinzuwirken. Eine von Anfang an möglichst kooperative Projektbegleitung ist gegenwärtig aus meiner Sicht für alle Beteiligten hilfreicher als die spätere Einleitung formaler Aufsichtsverfahren.

Festzustellen ist im Übrigen, dass nicht nur Unternehmen und Behörden zunehmend von Künstlicher Intelligenz Gebrauch machen, sondern auch Menschen, die sich über Datenschutzverstöße dieser Stellen bei meiner Behörde beschweren. Mithilfe sogenannter großer Sprachmodelle formulieren sie ihre Anliegen und scheuen sich offenbar nicht, den jeweiligen Programmen teilweise sehr sensible – eigene wie fremde – persönliche Sachverhalte anzuvertrauen. Sie berücksichtigen dabei vermutlich nicht, dass die Daten in das Training der Modelle einfließen und möglicherweise anschließend wieder extrahiert werden können. Es bedarf in diesem Kontext eines tieferen Verständnisses für die Funktionsweise der Künstlichen Intelligenz und eines größeren Bewusstseins für den Umgang mit personenbezogenen Daten.

Die Arbeit meiner Behörde beschränkte sich im Berichtsjahr natürlich nicht nur auf die Künstliche Intelligenz. Auch die Videoüberwachung beschäftigte meine Mitarbeiterinnen und Mitarbeiter weiterhin in hohem Maß; erneut war eine Zunahme der Fallzahlen im Vergleich zum Vorjahr zu beobachten. Neben unzähligen Beratungen musste meine Behörde auch wieder Sanktionen ergreifen, um z. B. unzulässige Kameras abzuschalten oder den Betrieb auf ein zulässiges Maß zu reduzieren. Weiterhin habe ich zahlreiche Projekte zur Digitalisierung von Verwaltungsleistungen begleitet und Städte bzw. Gemeinden zu Fragen des Datenschutzes u. a. im Zusammenhang mit den Kommunalparlamenten beraten.

Erkennbar wird die Bedeutung des Datenschutzes aber nicht nur durch die großen, aufwendigen Beratungen und Beschwerdeverfahren. Vielmehr zeigt sich gerade an den vermeintlich „kleinen“ Fällen, wie omnipräsent Datenschutzfragen in unserem Alltag sind. Deshalb berichte ich wieder über ganz unterschiedliche Lebensbereiche – sei es über den Umgang mit Mieterdaten, den Verkauf eines Gebrauchtwagens oder den Erwerb einer „Mystery Box“. Ihnen, liebe Leserinnen und Leser, wünsche ich eine interessante und angenehme Lektüre.



Dagmar Hartge

Bericht nach Artikel 59 Datenschutz-Grundverordnung

I Schwerpunkt: Künstliche Intelligenz

Am 1. August 2024 trat die europäische Verordnung über Künstliche Intelligenz (KI-Verordnung, KI-VO) in Kraft, die weltweit erste, umfassende gesetzliche Regulierung dieser Technologie.[1] Die Vorschriften werden schrittweise wirksam. Seit dem 2. Februar 2025 gelten die Kapitel I und II der Verordnung. Dort verpflichtet der europäische Gesetzgeber Anbieterinnen bzw. Anbieter und Betreiberinnen bzw. Betreiber von KI-Systemen beispielsweise zu Maßnahmen, damit ihr Personal beim Betrieb und bei der Nutzung von KI-Systemen über ausreichende KI-Kompetenz verfügt (Artikel 4 KI-VO). Darüber hinaus bestimmt er verbotene Praktiken im KI-Bereich (Artikel 5 KI-VO). Seit dem 2. August 2025 ist eine Reihe zusätzlicher Regelungen wirksam. Hierzu zählen insbesondere die Festlegungen von Kapitel V der Verordnung zu KI-Modellen mit allgemeinem Verwendungszweck, einschließlich solcher Modelle, die ein systemisches Risiko aufweisen (Artikel 51 ff. KI-VO).

Gemäß Artikel 2 Absatz 7 KI-VO bleiben datenschutzrechtliche Vorschriften der Europäischen Union, insbesondere die Datenschutz-Grundverordnung, unberührt, soweit mit Künstlicher Intelligenz personenbezogene Daten verarbeitet werden. Insofern hat unsere Behörde im Berichtszeitraum ihre diesbezüglichen Aktivitäten der vergangenen Jahre bei der datenschutzrechtlichen Beratung und Aufsicht weitergeführt und ausgebaut. Flankiert wurde dies von einer innerbehördlichen Initiative, um den eigenen Mitarbeiterinnen und Mitarbeitern die notwendigen Kenntnisse zu KI-Systemen, ihren Chancen und Risiken zu vermitteln.

1 Tätigkeitsbericht Datenschutz 2024, A I 1.

1 Einführung eines KI-Assistenztools in der Landesverwaltung

In der brandenburgischen Landesverwaltung bestehen große Erwartungen bezüglich des Einsatzes von Künstlicher Intelligenz. Ein wichtiges Element zur Entlastung der Beschäftigten, zur Beschleunigung von Verfahrensabläufen und zur Erhöhung der Effizienz der Verwaltungstätigkeit wird dabei in der Einführung eines sogenannten KI-Assistenztools gesehen. Dieses Werkzeug soll es beispielsweise ermöglichen, Texte mithilfe von KI zu erstellen, sie zu korrigieren oder stilistisch zu verbessern sowie wesentliche Inhalte aus umfangreichen Texten zu extrahieren und zusammenzufassen. Die Einführung des Systems ist Teil der KI-Landesstrategie.[2]

Im Berichtszeitraum hat eine Arbeitsgruppe des Beratungsgremiums der IT-Beauftragten der Ressorts (RIO-Ausschuss) das Thema erörtert sowie eine Markterkundung und Bewertung bereits verfügbarer KI-Assistenztools vorgenommen. Ziel war es, Grundlagen für eine Entscheidung des Digital-Lenkungskreises der Landesregierung über die Einführung eines solchen Werkzeugs zu schaffen.

Positiv festzuhalten ist zunächst, dass in der Landesverwaltung für die genannten Zwecke keine der frei im Internet zugänglichen KI-Plattformen eingesetzt werden soll. Die damit verbundenen Risiken – auch aus datenschutzrechtlicher Sicht – wären wohl nicht beherrschbar. Vielmehr ist beabsichtigt, ein geschlossenes und abgeschottetes KI-System als Assistenzwerkzeug entweder selbst im Land zu betreiben oder bei einem externen Dienstleister im Auftrag betreiben zu lassen. Die Arbeitsgruppe präferiert den Einsatz von europäischen großen Sprachmodellen (Large Language Models, LLMs). Perspektivisch sollen auch eine Optimierung der KI-Ausgaben (Fine Tuning) sowie das Training und die Nutzung eigener Wissensdatenbanken auf Basis existierender Verwaltungsdaten (Retrieval Augmented Generation, RAG) ermöglicht werden.

2 Tätigkeitsbericht Datenschutz 2024, A I 1.

Da die Verarbeitung personenbezogener Daten mit dem geplanten KI-Assistenztool nicht ausgeschlossen wurde, gehen wir gegenwärtig davon aus, dass der Betrieb bzw. die Nutzung auch datenschutzrechtliche sowie technisch-organisatorische Belange berührt. Die Anforderungen der Datenschutz-Grundverordnung (DS-GVO) und des Brandenburgischen Datenschutzgesetzes (BbgDSG) sind insofern einzuhalten. Wir haben deshalb die Gelegenheit ergriffen, zu den Ergebnissen der oben erwähnten Arbeitsgruppe umfassend Stellung zu nehmen. Insbesondere stellten wir fest:

- Zurzeit ist unklar, auf welche datenschutzrechtliche Rechtsgrundlage die Verarbeitung personenbezogener Daten im geplanten KI-Assistenzsystem gestützt werden soll. Dies betrifft insbesondere diejenigen Personen, die keine Nutzerinnen bzw. Nutzer des Werkzeugs sind. Eine spezielle Vorschrift im Landesrecht, die eine solche Verarbeitung gestattet, existiert aktuell nicht. Einen Rückgriff auf die Generalklausel von § 5 BbgDSG, wonach die Verarbeitung erlaubt ist, wenn sie zur Erfüllung der Aufgaben der Verwaltung erforderlich ist, sehen wir kritisch. Eine Erforderlichkeit (im juristischen Sinne) ist bislang nicht nachgewiesen.

Allzweckmittel KI?

- Fraglich ist auch, wie den datenschutzrechtlichen Grundsätzen der Datenminimierung und der Zweckbindung im geplanten KI-Assistenzsystem Rechnung getragen wird. Aus unserer Sicht ist die Verarbeitung personenbezogener Daten (z. B. von Bürgerinnen und Bürgern), die in ein KI-System hochgeladen werden, im vorliegenden Kontext wohl grundsätzlich nicht auf das für die jeweiligen Verarbeitungszwecke notwendige Maß beschränkt. Sie wäre damit unzulässig (jedenfalls solange es keine entsprechende rechtliche Grundlage gibt). Gleiches gilt, wenn das System perspektivisch mit personenbezogenen Daten trainiert und weiterentwickelt wird, da in diesem Fall die Daten zu anderen als den ursprünglich verfolgten Zwecken verarbeitet werden.

- Unklar ist weiter, wie die Anforderungen zur Wahrung der Rechte betroffener Personen in dem geplanten KI-Assistenzsystem erfüllt werden. Dies bezieht sich sowohl auf die Transparenz der Verarbeitung und die Aufklärung betroffener Personen über die Verarbeitung ihrer Daten als auch auf die Rechte dieser Perso-

nen auf Auskunft, Berichtigung, Löschung sowie Einschränkung der Verarbeitung. Hierbei ist zu beachten, dass die Landesverwaltung nur sehr begrenzt Einfluss auf die Datenverarbeitung im gewählten KI-Sprachmodell nehmen kann und darüber hinaus von den Informationen abhängig ist, die die Anbieterin bzw. der Anbieter des jeweiligen Modells bereitstellt. Zur Frage der Löschung oder Berichtigung personenbezogener Daten im KI-System findet sich in den Ergebnissen der Arbeitsgruppe keine Antwort.

- Den Unterlagen können wir auch nicht entnehmen, welche großen Sprachmodelle konkret eingesetzt werden sollen und wer über den Einsatz aufgrund welcher Kriterien entscheidet. Zwar unterstützen wir die Absicht, „möglichst ein europäisches Sprachmodell mit Optimierungen auf die deutsche Verwaltungssprache“ zu verwenden. Allerdings bedarf es einer schlüssigeren Begründung als die pauschale Aussage, dass dadurch die Qualität der Antworten verbessert und die Voreingenommenheit (Bias) reduziert wird. Ebenso ist es kein Automatismus, dass „KI-Assistenzsysteme, die für die Verwaltung entwickelt wurden [...] wesentliche Anforderungen an IT-Sicherheit und Datenschutz grundsätzlich mit sich bringen“ – so war es jedenfalls im Abschlussbericht zu lesen.

- Wir können darüber hinaus gegenwärtig auch nicht erkennen, welche konkreten technischen und organisatorischen Maßnahmen für das KI-Assistenzsystem umgesetzt werden sollen. Die Vorgaben der Datenschutz-Grundverordnung verlangen, dass der Verantwortliche (hier: die Behörden der Landesverwaltung) bereits bei der Konzipierung von Verarbeitungen personenbezogener Daten derartige Maßnahmen vorsieht.

- Wir sind der Auffassung, dass für das geplante System wegen der Neuartigkeit der Technologie, des Umfangs an personenbezogenen Daten sowie der möglichen Risiken für die Rechte und Freiheiten betroffener Personen eine Datenschutz-Folgenabschätzung durchzuführen ist. Dies gilt umso mehr, weil spezifische Angriffe auf KI-Systeme (z. B. Data Poisoning, Prompt Injection) sowie spezifische Risiken (wie Verzerrungen, Diskriminierung, Halluzinationen) betrachtet werden müssen. Uns ist gegenwärtig nicht bekannt, wie dieser Anforderung im vorliegenden Fall entsprochen werden soll.

Aus der Aufzählung ist ersichtlich, dass wir im Hinblick auf die Einführung des KI-Assistenztools in der Landesverwaltung gegenwärtig erhebliche Defizite insbesondere bei der Einhaltung der datenschutzrechtlichen Grundsätze von Artikel 5 DS-GVO sehen. Gleichwohl hat der RIO-Ausschuss sich mit überwiegender Mehrheit für die Einführung ausgesprochen. Der Digital-Lenkungskreis der Landesregierung entschied, eine Arbeitsgruppe mit der Vorbereitung einer entsprechenden Ausschreibung zu beauftragen. Ziel sollte die Einführung des Werkzeuges im Jahr 2026 sein. Das Ministerium der Justiz und für Digitalisierung sagte zu, unsere Stellungnahme im weiteren Verlauf des Projekts zu berücksichtigen.

Kurz vor Redaktionsschluss dieses Berichts erreichte uns die Information über die Entscheidung des Ministeriums, zunächst das KI-Assistenzsystem LLMoin für die Landesverwaltung bereitzustellen, um mehr Zeit für die Ausschreibung und Produktentscheidung zu gewinnen und den Beschäftigten die Möglichkeit zu bieten, Erfahrungen mit einem derartigen Werkzeug zu sammeln. LLMoin wird von der Anstalt öffentlichen Rechts Dataport angeboten und ist bereits in mehreren Bundesländern im Einsatz.

2 Einsatz des Chatbots „telli“ an Schulen

Bereits vor zwei Jahren hatten wir uns mit dem Einsatz von Künstlicher Intelligenz (KI) in Schulen befasst und darüber berichtet.[3] Konkreter Anlass war die Herausgabe eines „Handlungsleitfadens zur Nutzung von textgenerierenden KI-Anwendungen an Schulen im Land Brandenburg“ durch das Ministerium für Bildung, Jugend und Sport. Wichtig war uns zu diesem Zeitpunkt insbesondere, dass die KI nicht ungeregelt verwendet wird. Weiterhin sollten Schülerinnen und Schüler nach unserer Auffassung für einen sachgerechten und kritischen Umgang mit KI-Anwendungen sensibilisiert werden und gleichzeitig lernen, wie hierbei das Recht auf informationelle Selbstbestimmung gewahrt werden kann. Schon damals war absehbar, dass die Bedeutung des Themas zunehmen wird.

Insofern begrüßten wir die Initiative des Bildungsministeriums, gemeinsam mit dem Institut für Film und Bild in Wissenschaft und Unterricht (FWU) an der Bereitstellung eines Chatbots für den schulischen Einsatz zu arbeiten. Das Ergebnis ist „telli“ – ein elektronisches Dialogsystem, welches ein natürliches Gegenüber imitiert. Diese KI-Anwendung wurde im Berichtszeitraum in mehreren brandenburgischen Schulen pilotiert und ist seit dem Schuljahr 2025/26 flächendeckend im Land einsetzbar. Bei „telli“ handelt es sich um ein länderübergreifendes Projekt – viele weitere Bundesländer planen, ihren Schulen das System für Lehr- und Lernzwecke anzubieten.

Gegenwärtig können brandenburgische Lehrkräfte über das Schulportal auf „telli“ zugreifen und den Chatbot sowohl für die Vorbereitung als auch direkt im Unterricht einsetzen. Insbesondere können sie verschiedene Lernszenarien erstellen und dabei die spezifischen Bedürfnisse der Schülerinnen und Schüler sowie besondere Rahmenbedingungen flexibel berücksichtigen. Über einen Link bzw. einen QR-Code teilen sie anschließend im Unterricht die erstellten Szenarien. Für das Fach Geschichte ist es beim Thema „Industrielle Revolution“ beispielsweise möglich, während der Unterrichtsvorbereitung spezielle Dialogpartnerinnen und -partner (etwa Personen

3 Tätigkeitsbericht Datenschutz 2023, A I 1.3.

der Zeitgeschichte oder fiktive Charaktere) vorzusehen. Schülerinnen und Schüler können anschließend im Unterricht etwas über die Lebensumstände im 18. und 19. Jahrhundert lernen, indem sie KI-generierte Dialoge mit den fiktiven Personen führen. Da sich die Lernszenarien in verschiedenen Fächern stark unterscheiden können, sind in „telli“ mehrere große Sprachmodelle (Large Language Modells, LLMs) mit unterschiedlichen Stärken integriert.

Aus datenschutzrechtlicher Sicht sind die einzelnen Schulen für die Nutzung von „telli“ jeweils selbst verantwortlich. Das FWU betreibt die KI-Plattform im Rahmen einer Auftragsverarbeitung für die Schulen. Dort bindet sie wiederum verschiedene Unterauftragsverarbeiter ein, welche die Sprachmodelle anbieten. Somit agiert das FWU gewissermaßen als Schnittstelle und Vermittler zwischen den Schulen und den Angeboten.

Von der Pilotierung und der geplanten Einführung des Chatbots „telli“ in Brandenburg erfuhren wir zunächst nur aus der Presse. Insofern konnten wir das Projekt erst zu einem relativ späten Zeitpunkt datenschutzrechtlich begleiten und auf die Einhaltung der Anforderungen der Datenschutz-Grundverordnung (DS-GVO) hinwirken. Wir hätten uns eine frühzeitige Einbindung durch das Ministerium oder (im Kontext der Arbeitsgremien der Datenschutzkonferenz) durch die FWU gewünscht, um die Schulen als datenschutzrechtlich Verantwortliche bestmöglich bei einem rechtssicheren Einsatz des KI-Systems zu unterstützen und bei der Umsetzung datenschutzrechtlicher Vorgaben zu entlasten. Sie müssen beispielsweise eine tragfähige Rechtsgrundlage für die Verarbeitung personenbezogener Daten in „telli“ benennen, den Nutzerinnen und Nutzern die gesetzlich vorgeschriebenen Informationen gemäß Artikel 13 DS-GVO bereitstellen, Vereinbarungen zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO abschließen, eine Datenschutz-Folgenabschätzung gemäß Artikel 35 DS-GVO durchführen sowie ihrer Nachweis- und Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DS-GVO nachkommen. Die Abstimmung entsprechender Muster erleichtert in der Regel das Vorgehen und hilft, die Qualität der Ergebnisse zu sichern.

Eine der wichtigsten Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten ist diejenige nach der Rechtmäßigkeit der Verarbeitung. Grundsätzlich dürfen Schulen gemäß § 65 Absatz 2 Brandenburgisches Schulgesetz personenbezogene Daten verarbeiten, soweit dies zur Erfüllung ihres Erziehungs- und Bildungsauftrags

erforderlich ist. Diese Regelung gilt auch für digitale Lehr- und Lernmittel. Bei der Prüfung der Erforderlichkeit sind jedoch die unterschiedlichen Verarbeitungsvorgänge einer KI-gestützten Anwendung einzeln zu beleuchten. Im Allgemeinen lassen sich grob drei verschiedene Kontexte unterscheiden: Erstens können personenbezogene Daten für nicht KI-spezifische Komponenten bzw. Funktionen des Systems verarbeitet werden. Hierzu gehören z. B. die technische Bereitstellung des Dienstes, die Nutzerverwaltung und die Möglichkeit der Speicherung von Inhalten. Diese Verarbeitung kann bei „telli“ im Grunde genommen auf die genannte Vorschrift des Brandenburgischen Schulgesetzes gestützt werden. Zweitens können aber die Anfragen an das KI-System (die sogenannten Prompts) sowie die generierten Antworten personenbezogene Daten enthalten. Und drittens ist es denkbar, dass das KI-Modell auf Grundlage der Nutzereingaben weiter trainiert bzw. feinjustiert wird. Nach unserer Auffassung ist eine Verarbeitung personenbezogener Daten im zweiten und im dritten Kontext bei „telli“ für die Erfüllung des Erziehungs- und Bildungsauftrags nicht erforderlich. Dies hat das FWU insofern berücksichtigt, als dass das KI-Training und die Verarbeitung für eigene Zwecke durch die Unterauftragsverarbeiter vertraglich ausgeschlossen sein sollen. Sowohl das FWU als auch das brandenburgische Bildungsministerium haben darüber hinaus klargestellt, dass Eingaben mit Personenbezug in „telli“ unerwünscht sind. Das Ministerium hat hierzu ein entsprechendes Verbot in die Nutzungsbedingungen des Chatbots aufgenommen. Zusätzlich werden die Lehrkräfte sowie die Schülerinnen und Schüler diesbezüglich belehrt und sensibilisiert. Über die Wirksamkeit dieser Maßgaben wird noch zu diskutieren sein. Auch ob ergänzende technische Maßnahmen umzusetzen sind, um die unerwünschte Verarbeitung personenbezogener Daten (etwa auch in den Ausgaben von „telli“) tatsächlich auszuschließen, konnte im Berichtszeitraum noch nicht abschließend erörtert werden.

Spannender Unterricht mit KI

Im Hinblick auf die Transparenzanforderungen und Informationspflichten bei der Nutzung von „telli“ ist es für die Schulen als datenschutzrechtlich Verantwortliche essenziell zu wissen, welche personenbezogenen Daten im System wie verarbeitet werden. Dies erfordert zunächst eine Unterstützung durch das FWU als Auftragsverarbeiter sowie durch die Anbieterinnen und Anbieter der Sprachmodelle als Unterauftragsverarbeiter; sie sollten entsprechend aussagekräftige Unterlagen zuliefern. Datenschutzinformationen gemäß

Artikel 13 DS-GVO sollten aus unserer Sicht zentral vorbereitet und den Schulen bereitgestellt werden, damit diese sie ggf. anpassen und an die betroffenen Personen weiterleiten können. Das FWU hat diese Aufgabe übernommen und eine existierende Version nach datenschutzrechtlichen Hinweisen bereits überarbeitet. Gegenüber dem Bildungsministerium haben wir zudem angeregt, die Personalvertretung der Lehrkräfte frühzeitig einzubeziehen und Eltern ergänzende Informationen zu „telli“ bereitzustellen.

Gemäß Artikel 35 Absatz 1 DS-GVO muss eine Datenschutz-Folgenabschätzung durchgeführt werden, wenn die Datenverarbeitung voraussichtlich hohe Risiken für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. Beim Einsatz von KI-Systemen an Schulen kann grundsätzlich davon ausgegangen werden, dass ein hohes Risiko vorliegt und eine Datenschutz-Folgenabschätzung somit erforderlich ist. Diese Einschätzung berücksichtigt, dass Kinder zu den besonders schutzbedürftigen Betroffenen zählen und Künstliche Intelligenz eine neue Technologie darstellt. Für „telli“ wurde zwar eine Datenschutz-Folgenabschätzung durch das FWU erstellt, jedoch war für uns problematisch, dass viele Risiken nicht ausreichend Berücksichtigung fanden. So wurde beispielsweise das Risiko, dass Prompts (entgegen der Nutzungsbedingungen) personenbezogene Daten enthalten können, gar nicht erst erörtert. Auch weiteren, KI-spezifischen Risiken wurde keine Beachtung geschenkt. Zu nennen sind beispielsweise sogenannte Prompt Injections, bei denen Sprachmodelle gezielt dazu veranlasst werden, ungewollte Inhalte (wie etwa Trainingsdaten) offenzulegen. Da die Datenschutz-Folgenabschätzung Verantwortlichen und Auftragsverarbeitern auch als Basis für die Umsetzung technischer und organisatorischer Maßnahmen zur Risikominimierung dient, zahlt sich gerade hier ein sorgfältiges, strukturiertes und gründliches Vorgehen aus. Insofern begrüßen wir die Zusage des FWU, die Datenschutz-Folgenabschätzung zu überarbeiten.

Wegen des geplanten Einsatzes von „telli“ in mehreren Bundesländern hat sich in der Zwischenzeit ein Arbeitsgremium der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gebildet, das zu einigen der o. g. Themen eine inhaltliche Abstimmung mit dem FWU und den Bildungsministerien anstrebt. Nach unserer Einschätzung weisen diese bisherigen Erörterungen in die richtige Richtung. Insgesamt stellen wir fest, dass sich Brandenburg nach einem holprigen Start aktuell auf dem richtigen Weg

befindet. Positiv hervorzuheben ist auch, dass das FWU die Datenschutzaufsichtsbehörden bereits über das nächste KI-Projekt im Schulbereich informiert und die Einbindung zugesagt hat. Um den Schulen zukünftig Rechtssicherheit bei der Nutzung von Künstlicher Intelligenz zu bieten, empfehlen wir darüber hinaus, die schulrechtlichen Vorschriften des Landes rechtzeitig zu überprüfen und ggf. anzupassen.

3 Nutzung von KI im Wohngeldverfahren

Die Wohngeldstelle der Landeshauptstadt Potsdam testet seit dem Frühjahr des Berichtszeitraums ein Programm, das mithilfe Künstlicher Intelligenz (KI) die Bearbeitung von Wohngeldanträgen beschleunigen soll. Dafür wird die speziell für den Wohngeldbereich entwickelte Software eines jungen bayerischen Unternehmens eingesetzt. Sie soll die von Antragstellerinnen und Antragstellern eingereichten Unterlagen automatisiert digital erfassen, die Antragsdaten extrahieren sowie diese auf Vollständigkeit und Plausibilität prüfen. Zusätzlich soll ein fachspezifischer Chatbot Beschäftigten rechtliche Fragen zu ihrer Tätigkeit rund um das Wohngeldgesetz und die zugehörigen Umsetzungsbestimmungen beantworten. Das Pilotprojekt wird gemeinsam mit der Digitalagentur Brandenburg durchgeführt und vom Ministerium für Infrastruktur und Landesplanung des Landes Brandenburg unterstützt. Perspektivisch ist die Anwendung in allen brandenburgischen Wohngeldstellen geplant.

Nachdem wir durch Medienberichte auf das Projekt aufmerksam geworden waren, nahmen wir im Rahmen eines Beratungsverfahrens Kontakt mit den Verantwortlichen auf und baten um einen Austausch. Unser Ziel war zunächst, das System und insbesondere die genutzten KI-Komponenten kennenzulernen sowie Erfahrungen und Herausforderungen im Projekt zu ermitteln. Darüber hinaus wollten wir feststellen, welche technischen und organisatorischen Maßnahmen umgesetzt wurden bzw. noch umgesetzt werden sollen, um die Risiken für betroffene Personen bei der Verarbeitung ihrer besonders schutzbedürftigen Sozialdaten mittels KI zu beherrschen. Wegen des zuletzt genannten Aspekts und der geplanten Ausweitung auf weitere Wohngeldstellen im Land halten wir eine Projektbegleitung durch unsere Dienststelle für besonders wichtig.

Die Zusammenarbeit mit den Verantwortlichen und der Digitalagentur war durchweg konstruktiv und von großer Offenheit geprägt. Bei einem ersten Vor-Ort-Termin wurden die Funktionsweise des Systems und getroffene Schutzmaßnahmen ausführlich erläutert. Bereits im Vorfeld hatten wir Unterlagen zur Dokumentation des Verfahrens erhalten. Zum Zeitpunkt der Erstellung dieses Berichtes war ein zweites Treffen in Vorbereitung, um die Diskussion zu den technischen und organisatorischen Maßnahmen zu vertiefen. Fest-

zuhalten ist, dass die Maßnahmen aufgrund unserer Fragen und Hinweise in der Auftaktberatung bereits überarbeitet wurden. Beide Seiten haben großes Interesse, den Dialog fortzuführen.

Im Fokus der bisherigen Erörterungen standen diverse Fragen und Herausforderungen, die in vielen ähnlich gelagerten Projekten ebenfalls relevant sein dürften. So ist es beim Einsatz neuer Technologien und der Verarbeitung sensibler Daten für eine Vielzahl betroffener Personen unerlässlich, dass Verantwortliche das Instrument der Datenschutz-Folgenabschätzung gemäß Artikel 35 Datenschutz-Grundverordnung (DS-GVO) nutzen, um systematisch die möglichen Risiken der Datenverarbeitung zu erkennen und diese durch geeignete und angemessene Maßnahmen hinreichend zu minimieren. Im konkreten Fall stehen sie dabei vor der Schwierigkeit, dass es zum Einsatz von Künstlicher Intelligenz im Allgemeinen und großen Sprachmodellen (Large Language Models, LLMs) im Besonderen bisher kaum etablierte Standards für die Gewährleistung von Datenschutz und Informationssicherheit gibt. Insofern ist spezielle Sorgfalt z. B. auf die Identifikation möglicher Gefährdungen, ihre Bewertung hinsichtlich Eintrittswahrscheinlichkeit und Schadenshöhe, die Beachtung KI-spezifischer Angriffsszenarien und Fehlfunktionen, die Bestimmung von Schutzmaßnahmen, die Einschätzung ihrer Eignung und Wirksamkeit sowie die Ermittlung des verbleibenden Restrisikos der Verarbeitung zu legen. Ausgangspunkt der Untersuchungen muss wie bei jeder Datenschutz-Folgenabschätzung eine exakte und umfassende Beschreibung der Datenverarbeitungsprozesse, der konkreten Datenkategorien und Datenflüsse sowie der Prozessschritte, der beteiligten IT-Systemkomponenten und -schnittstellen sein. Für das Wohngeldverfahren haben wir den Verantwortlichen entsprechende Hinweise gegeben.

Qualität von Anträgen mit KI erhöhen

Zu den KI-spezifischen Risiken gehören Halluzinationen, Voreingenommenheit (Bias), Diskriminierung oder sonstige Fehlfunktionen der KI. Sollten sich diese Risiken in Verwaltungsverfahren zur Gewährung von Sozialleistungen auf Entscheidungen der Behörde auswirken, können daraus gravierende Folgen für die betroffenen Personen resultieren. Vor der Nutzung eines Systems mit KI-Komponenten muss daher u. a. klar geregelt sein, welche konkreten Nachprüfungen die Beschäftigten der Behörde bei Ausgaben der KI vorzunehmen haben und wie mit Fehlern umzugehen ist. Falls auf die Verpflichtung zur umfassenden manuellen Nachprüfung von KI-Aus-

gaben explizit verzichtet wird, ist genau darzulegen, welche Risiken dadurch entstehen und wie diese beherrscht werden. Dabei kann z. B. die Transparenz ein wichtiger Aspekt sein: Erhält eine Antragstellerin oder ein Antragsteller ein Schreiben der Behörde, das auf der Basis von KI-generierten und nicht vollständig durch Menschen überprüften Informationen erstellt wurde, muss dies in jedem Fall deutlich gekennzeichnet sein.

Weiter ist sicherzustellen, dass Antragstellerinnen und Antragsteller nicht einer ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung unterworfen werden, die ihnen gegenüber rechtliche Wirkung entfaltet – es sei denn, es besteht eine gesetzlich geregelte Ausnahme und es gibt keinen Ermessensspielraum der Behörde. Insofern gilt, dass die Künstliche Intelligenz allein keine tatsächliche Entscheidung für oder gegen die Gewährung z. B. von Sozialleistungen bzw. über deren Höhe treffen darf. Verantwortliche sollten jedoch schon bei vorbereitenden und unterstützenden Verarbeitungen durch KI große Vorsicht walten lassen und eine menschliche Nachkontrolle vorsehen. Beim vorliegenden KI-unterstützten Wohngeldverfahren ist positiv hervorzuheben, dass sich die Verarbeitung mittels eines Sprachmodells auf den Aspekt der Erkennung und Klassifizierung von eingereichten Unterlagen beschränkt. Alle weiteren Verarbeitungsschritte, wie z. B. die Plausibilitätsprüfung oder die Generierung von Textentwürfen für Schreiben zur Nachforderung von Unterlagen finden auf Basis definierter, nachvollziehbarer Regeln ohne KI-Einfluss statt.

Im Hinblick auf den oben erwähnten Chatbot, der Beschäftigten der Wohngeldstelle Fragen zum Wohngeldgesetz und Umsetzungsvorschriften beantworten soll, war für uns wichtig zu klären, ob hierbei die Verarbeitung personenbezogener Daten aus der Antragstellung zwingend notwendig ist. Dies verneinten die Verantwortlichen. Generell sollte aus unserer Sicht auch bei vergleichbaren KI-basierten Assistenzsystemen die Ein- und Ausgabe personenbezogener Daten von Betroffenen mithilfe von Dienstanweisungen und technischen Filterkomponenten verhindert sowie die Einhaltung der Festlegungen ggf. mit angemessenen, stichprobenartigen Protokollauswertungen überprüft werden.[4]

4 Siehe A I 1 und A I 4.

Auch der Informationssicherheit kommt beim Einsatz von KI-Systemen eine große Bedeutung zu. Insbesondere bei der Verarbeitung hoch schutzbedürftiger personenbezogener Daten durch Externe im Rahmen einer Auftragsverarbeitung ist zu beachten, dass die Auftraggeberin bzw. der Auftraggeber die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der dort durchgeführten Datenverarbeitung tatsächlich kontrollieren können muss. Dafür sind ein umfassendes Informationssicherheitskonzept sowie die Festlegung von Kontrollmechanismen, die auch die besonderen Risiken von KI-Systemen berücksichtigen, unerlässlich.

Ein aus unserer Sicht noch offener Punkt, den öffentliche Stellen vor Nutzung eines KI-Systems zur Verarbeitung personenbezogener Daten klären müssen, ist die Rechtsgrundlage, auf deren Basis die Verarbeitung erfolgt. Gemäß Artikel 5 Absatz 1 Buchstabe a DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben sowie in einer für betroffene Personen nachvollziehbaren Weise verarbeitet werden. Öffentliche Stellen können sich dabei gegenüber Bürgerinnen und Bürgern bei der Erfüllung ihrer Aufgaben nicht auf ein berechtigtes Interesse nach Artikel 6 Absatz 1 Buchstabe f DS-GVO stützen. Wenn der Einsatz von KI für die Erfüllung einer Verwaltungsaufgabe nicht zwingend erforderlich ist, braucht es nach unserer Auffassung daher eine explizite Erlaubnisnorm.

Wir werden zu den genannten Fragen im weiteren Verlauf der Beratung mit der Wohngeldstelle Potsdam, der Digitalagentur Brandenburg sowie dem Ministerium für Infrastruktur und Landesplanung gemeinsam nach datenschutzkonformen Lösungen suchen.

4 Einführung einer KI-Assistenz in der Verwaltung des Landkreises Uckermark

Der Landkreis Uckermark möchte allen Beschäftigten der Kreisverwaltung eine KI-Assistenz namens „Uckermark-GPT“ bereitstellen. Er soll der Unterstützung und Optimierung interner Arbeitsabläufe durch Textgenerierung, Recherche und Dokumentenauswertung dienen. Neben der Absicht, die Mitarbeiterinnen und Mitarbeiter bei ihrer Arbeit zu unterstützen, besteht das Ziel auch darin, die unerlaubte individuelle Nutzung von nicht datenschutzkonformen, internetbasierten KI-Plattformen in der Verwaltung einzudämmen.

Nachdem wir durch die öffentliche Berichterstattung auf dieses Projekt aufmerksam wurden, nahmen wir mit den Verantwortlichen Kontakt auf, um sie im weiteren Prozess zu beraten und zu begleiten. Zum einen wollten wir wissen, wie bei der geplanten KI-Assistenz die Verarbeitung personenbezogener Daten geregelt ist und welche technischen und organisatorischen Maßnahmen in dieser Hinsicht getroffen werden. Weiterhin war unser Ziel, angesichts der rasanten Entwicklungen im Bereich Künstliche Intelligenz konkrete Einsatzbeispiele im Land Brandenburg kennenzulernen, uns mit den Verantwortlichen über die Herausforderungen aus datenschutzrechtlicher und technischer Sicht auszutauschen und erste Ideen für zukünftige Prüfkriterien und -prozesse zu entwickeln. Die Erörterung fiel in eine Zeit, als parallel die Einführung eines KI-Assistenzwerkzeugs in der Landesverwaltung diskutiert wurde.[5]

Die Zusammenarbeit mit der Kreisverwaltung gestaltete sich äußerst konstruktiv. Nachdem wir im Vorhinein die ausführliche Dokumentation für das Projekt einsehen konnten, fand im Herbst des Berichtszeitraums ein gemeinsames Treffen per Videokonferenz statt. Dabei wurden sowohl der Stand des Projekts erläutert (zu diesem Zeitpunkt im Probebetrieb mit etwa 50 Beschäftigten) als auch viele konkrete Fragen zu technischen und organisatorischen Maßnahmen besprochen. Weiterhin spielte die Einbindung des Zweckverbandes

5 Siehe A I 1.

Digitale Kommunen Brandenburg (DIKOM) als Dienstleister und Auftragsverarbeiter eine wichtige Rolle.

Die Erkenntnisse aus der Begleitung des Projekts zeigen einige Aspekte auf, die für die datenschutzgerechte Umsetzung von KI-Vorhaben wie dem hier beschriebenen generell hilfreich sein können. Besonders hervorzuheben ist die Entscheidung des Landkreises, von Anfang an die Eingabe personenbezogener Daten in das KI-System auszuschließen, da dies für die vorgesehenen Anwendungsfälle nicht notwendig ist. Dadurch lassen sich nicht nur Risiken wie der Abfluss personenbezogener Daten vermeiden, die trotz vertraglicher Regelungen mit dem Auftragsverarbeiter sowie technisch-organisatorischer Maßnahmen nie ganz ausgeschlossen werden können. Ebenso erübrigt sich so die Beantwortung der noch nicht abschließend geklärten Frage nach einer Rechtsgrundlage in der brandenburgischen Verwaltung für die Verarbeitung personenbezogener Daten mithilfe großer Sprachmodelle (Large Language Models, LLMs). Einen wichtigen Beitrag zur Sensibilisierung der Beschäftigten, bei der Nutzung der KI keine personenbezogenen Daten einzugeben, leistet eine klare Dienstanweisung, die sehr konkret erlaubte und verbotene Einsatzszenarien sowie Pflichten der Beschäftigten beim Einsatz des Werkzeugs auflistet. Darüber hinaus müssen alle Nutzerinnen und Nutzer vor der Verwendung ein Schulungsmodul absolvieren, das bei der Herstellung der erforderlichen KI-Kompetenz hilft. Und letztlich erinnert das System bei der Nutzung an die Vorgabe, auf personenbezogene Daten zu verzichten.

Gleichwohl ist es aus unserer Sicht angemessen, zusätzlich zu den beschriebenen dienstlichen Vorschriften und Standardvorkehrungen wie Nutzerauthentisierung, Regelung von Zugriffsrechten und Verschlüsselung des Datentransports weitere technische und organisatorische Maßnahmen umzusetzen, um Verstöße zu erkennen bzw. diesen vorzubeugen – zumindest, wenn ein großer Personenkreis Zugriff auf das System hat. Insbesondere haben wir empfohlen, sowohl für die Eingaben der Nutzerinnen und Nutzer als auch für die Ausgaben des KI-Systems einen Filter vorzusehen, der die Verarbeitung personenbezogener Daten durch das KI-System verhindert, indem diese Daten erkannt und aus der Ein- bzw. Ausgabe gelöscht werden.

Außerdem kann eine klar dokumentierte Protokollierung sinnvoll sein, um die Wirksamkeit der vorgenommenen Maßnahmen zu be-

werten. Hierbei ist allerdings immer sorgsam zwischen der Kontrolle einer rechtmäßigen Verarbeitung und dem Beschäftigtendatenschutz abzuwägen. Ein guter Ansatz, der sich in anderem Kontext auch praktisch bewährt hat, ist die im Rahmen der Beratung mit dem Landkreis entwickelte Überlegung, anonyme Stichproben der Eingaben zu sammeln und regelmäßig auszuwerten. Dadurch lässt sich überprüfen, ob die ergriffenen Maßnahmen ausreichen und wirksam sind, ohne in die Persönlichkeitsrechte der Beschäftigten einzugreifen.

Wir werden das Projekt und insbesondere den Übergang in den Regelbetrieb weiter begleiten.

5 Einsatz von KI beim Betreiber eines großen Online-Marktplatzes

Ein in Brandenburg ansässiges, international tätiges Unternehmen, das einen großen Marktplatz im Internet betreibt, informierte uns im Berichtszeitraum über den geplanten Einsatz von Künstlicher Intelligenz (KI). Erklärtes Ziel war, den Online-Handel auf der Plattform intelligenter und effizienter zu gestalten. Potenziell von KI unterstützte Prozesse sollten u. a. die leichtere Erstellung von (Verkaufs-)Angeboten, die Zusammenfassung von Produktrezensionen, die Bereitstellung einer individuelleren und persönlicheren Nutzererfahrung, die Verbesserung des Kundenservices durch Einsatz eines Chatbots, die Analyse von Interaktionen mit dem Kundendienst zur Qualitätsverbesserung, die Betrugserkennung und Compliance-Prüfung sowie die Datenanalyse für Markforschungszwecke sein. Das Unternehmen wollte hierbei sowohl eigene KI-Modelle und -Systeme trainieren bzw. entwickeln als auch solche von Dritten einsetzen. Es passte die im Internet verfügbare Datenschutzerklärung entsprechend an. Weiterhin wurden die Kundinnen und Kunden per E-Mail allgemein über den geplanten KI-Einsatz und den beabsichtigten Startzeitpunkt informiert. Die Nachricht endete mit dem Satz „Sie brauchen nichts weiter zu tun."

Die Ankündigung führte zu einer Reihe von Beschwerden bei uns. Nutzerinnen und Nutzer zweifelten u. a. die Rechtmäßigkeit des Vorhabens an und monierten insbesondere, dass sie keinen Einfluss auf die Nutzung ihrer personenbezogenen Daten für Zwecke der Entwicklung und des Trainings von KI hätten. Sie gingen davon aus, dass das Unternehmen zuvor eine Einwilligung einholen oder eine Möglichkeit vorsehen müsste, der entsprechenden Datenverarbeitung zu widersprechen.

Der zuletzt genannte Punkt konnte schnell geklärt werden: Das Unternehmen hatte sehr wohl in der geänderten Datenschutzerklärung im Abschnitt zu den KI-Planungen auf die Rechte betroffener Personen aufmerksam gemacht – nämlich durch einen Verweis auf eine andere Stelle des Textes. Um der Nutzung der personenbezogenen Daten für Zwecke der Entwicklung und des Trainings von KI-Modellen bzw. -Systemen zu widersprechen, war im eigenen Nutzerkonto lediglich eine entsprechende Einstellung zu aktivieren. Unsere Be-

schwerdeführerinnen und Beschwerdeführer hatten dies offenbar missverstanden.

Gleichwohl hatten wir erheblichen Diskussionsbedarf und führten seit der ersten Information über den geplanten KI-Einsatz mehrere Beratungen mit dem Unternehmen durch. In einer offenen, vertrauensvollen und konstruktiven Atmosphäre wurden dabei insbesondere folgende Punkte erörtert:

- Nicht alle Prozesse, die durch Künstliche Intelligenz unterstützt werden sollen, bedürfen auch personenbezogener Daten. Das Unternehmen war bereits selbst davon ausgegangen, den Personenbezug nur dann aufrechtzuerhalten, wenn er wirklich erforderlich ist. Ansonsten wollte es (insbesondere für das KI-Training) anonymisierte Daten nutzen. Weiter sagte es zu, selbstverständlich die Widersprüche der Nutzerinnen und Nutzer bei der Entwicklung und dem Training der KI-Komponenten zu beachten, soweit dem nicht gesetzliche Regelungen entgegenstehen.

- Das Unternehmen stützt die Datenverarbeitung durch KI bzw. für Trainings- und Entwicklungszwecke auf Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO). Die Verarbeitung ist nach dieser Vorschrift zulässig, wenn sie zur Wahrung berechtigter Interessen des Unternehmens erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten betroffener Personen, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Zu den in diesem Kontext zu beachtenden Anforderungen hatte sich der Europäische Datenschutzausschuss bereits Ende 2024 in einer entsprechenden Stellungnahme geäußert.[6] Wir machten das Unternehmen in den Beratungen darauf aufmerksam, dass aus unserer Sicht für jede der beabsichtigten Verarbeitungen eine entsprechende Interessenabwägung durchzuführen ist, und forderten Nach-

6 Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, angenommen am 17. Dezember 2024. Siehe auch Tätigkeitsbericht Datenschutz 2024, A I 3.

besserungen, da eine solche bislang lediglich pauschal und nicht auf den jeweiligen Kontext bezogen durchgeführt wurde.

- Kritisch sahen wir auch die o. g. Änderungen in der Datenschutzerklärung. Das Unternehmen argumentierte, mit der umfangreichen Fortschreibung und der Aufnahme möglichst vieler Anwendungsfälle von KI weit in die Zukunft geplant zu haben und somit häufige Änderungen des Textes (die in verschiedenen Sprachen vorzunehmen und stets rechtssicher zu formulieren sind) vermeiden zu können. Aus unserer Sicht waren jedoch die datenschutzrechtlichen Transparenzanforderungen von Artikel 13 DS-GVO nicht vollständig erfüllt, da Nutzerinnen und Nutzer nicht erkennen konnten, an welchen Stellen und in welcher Form KI tatsächlich im Einsatz war. Insbesondere bemängelten wir z. B., dass Verarbeitungen lediglich exemplarisch aufgezählt wurden, Verarbeitungszwecke im KI-Kontext unvollständig benannt, nur unzureichende Aussagen zu genutzten KI-Modellen sowie summarische Angaben zu möglichen Datenübermittlungen an Dritte für das KI-Training enthalten waren. Wir regten an, nachzubessern und z. B. durch eine mehrstufige Information an Nutzerinnen und Nutzer sowohl allgemeine (1. Stufe) als auch detaillierte Angaben (2. Stufe) zu den konkret durch Künstliche Intelligenz unterstützten Prozessen bereitzustellen. Die Informationen auf der zweiten Stufe könnten dann flexibel ergänzt bzw. angepasst werden, etwa wenn KI in weiteren Anwendungsszenarien genutzt werden soll oder sich Rahmenbedingungen des bisherigen KI-Einsatzes ändern.

- Zur Vorbereitung der Beratungen übersandte uns das Unternehmen auch den Entwurf einer Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO. Auch hier waren die Betrachtungen nach unserer Ansicht zu allgemein und pauschal, weil sie sich nicht auf den konkreten Verarbeitungskontext der jeweiligen KI-Nutzung bzw. der Entwicklung und des Trainings von KI-Modellen und –Systemen bezogen (s. o. zur Interessenabwägung). Gleichwohl ist positiv hervorzuheben, dass auch KI-spezifische Risiken und entsprechende technische und organisatorische Gegenmaßnahmen zur Wahrung der Rechte und Freiheiten betroffener Personen Eingang in die Betrachtungen fanden.

- Detailliert legte uns das Unternehmen dar, welche allgemeinen und spezifischen technischen und organisatorischen Maßnah-

men nach Artikel 32 DS-GVO bereits umgesetzt oder noch geplant waren, um die spezifischen Risiken durch den Einsatz von Künstlicher Intelligenz oder im Zuge der Entwicklung von KI-Systemen bzw. des Trainings von KI-Modellen zu beherrschen und zu minimieren. Im Mittelpunkt stand dabei das Training von eigenen Sprachmodellen für generative KI. Dieses erfolgt ausschließlich in abgeschlossenen Umgebungen im Rechenzentrum des Unternehmens. Soweit große Sprachmodelle von anderen Firmen genutzt werden, fließen keine Daten an diese zurück. Das Unternehmen hat selbst kein Interesse daran, dass personenbezogene Daten Teil des Sprachmodells werden, und deshalb Prozesse zur Aufbereitung der Trainingsdaten etabliert, um den Personenbezug frühzeitig auszuschließen. Daten von Nutzerinnen und Nutzern, die der Verwendung widersprochen haben, werden ohnehin nicht für Zwecke des KI-Trainings genutzt. Im Anschluss an einen mehrstufigen Trainingsprozess folgen Validierungen der Ergebnisse (insbesondere hinsichtlich der Reproduzierbarkeit personenbezogener Daten aus dem Modell) sowie umfassende Prüfungen zur Wirksamkeit der technischen Datenschutzmaßnahmen.

KI-Training: Nur rechtmäßig!

Das Unternehmen sagte zu, mit der Nutzung personenbezogener Daten für Zwecke des Trainings von KI-Modellen erst zu beginnen, wenn die offenen Fragen geklärt sind. Es arbeitet daran, die erkannten Defizite bei der Erfüllung der datenschutzrechtlichen Anforderungen zu beseitigen. Diesen Prozess werden wir weiter kritisch und konstruktiv begleiten.

6 Mitwirkung an Orientierungshilfen der Datenschutzkonferenz zu KI

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) strebt an, Verantwortliche und Auftragsverarbeiter durch Publikationen beim datenschutzkonformen Entwickeln, Betreiben und Nutzen von Modellen und Systemen der Künstlichen Intelligenz (KI) zu unterstützen. Bereits im vorherigen Berichtszeitraum veröffentlichte sie die Orientierungshilfe „Künstliche Intelligenz und Datenschutz“. Mit diesem Dokument erhalten Verantwortliche insbesondere Hinweise und Hilfestellungen für die Konzeption des Einsatzes, die Implementierung und die Nutzung von KI-Anwendungen unter Beachtung der datenschutzrechtlichen Vorgaben.[7]

Im Berichtszeitraum finalisierte eine Arbeitsgruppe der Konferenz, in der auch unsere Behörde mitwirkte, eine weitere Publikation. Sie wurde im Juni 2025 als „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ verabschiedet.

Aufsicht bietet Orientierung

Grundlage dieser Orientierungshilfe war ein entsprechendes Positionspapier der Datenschutzkonferenz aus dem Jahr 2019. Die genannte Arbeitsgruppe schrieb das Papier fort und berücksichtigte dabei aktuelle technische und rechtliche Entwicklungen. Insbesondere hat sie den seinerzeit gewählten Ansatz übernommen, die Phasen des Lebenszyklus eines KI-Systems zu untersuchen und anhand der Gewährleistungsziele des Standard-Datenschutzmodells (Transparenz, Datenminimierung, Nichtverkettung, Intervenierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit) technische und organisatorische Maßnahmen zur Wahrung des Datenschutzes zu beschreiben. Zudem teilte sie die Betrachtungen auf die vier Lebenszyklusphasen Design (inkl. Datenauswahl und -sammlung), Entwicklung (inkl. Datenaufbereitung, Training und Validierung), Einführung (im Sinne der

7 Tätigkeitsbericht Datenschutz 2024, A I 2.

Softwareverteilung inkl. Updates) sowie Betrieb und Monitoring des KI-Systems auf.

Die Arbeitsgruppe hatte auch die verwendeten Begrifflichkeiten zu aktualisieren und mit der am 2. August 2024 in Kraft getretenen europäischen Verordnung über Künstliche Intelligenz (KI-Verordnung) in Einklang zu bringen. Darüber hinaus floss die „Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen“ des Europäischen Datenschutzausschusses (EDSA) in die Orientierungshilfe ein.[8]

Aufgrund des Umfangs und der Komplexität des Themas musste der Fokus der Orientierungshilfe eingeschränkt werden, insbesondere um den Umfang des Dokuments in einem handhabbaren Rahmen zu halten. So wurden beispielsweise technische und organisatorische Maßnahmen, die für klassische IT-Systeme gelten, nicht explizit aufgeführt, da diese implizit auch bei KI-Systemen umzusetzen sind. Weiterhin waren datenschutzrechtliche Fragen, die sich aus der Sammlung großer Datenmengen für das Training von KI-Modellen ergeben (z. B. beim Crawling und Scraping), nicht Teil der Betrachtungen. Diese werden auch in anderen Dokumenten thematisiert, u. a. in der erwähnten Stellungnahme des EDSA. Des Weiteren lag der Schwerpunkt der Ausführungen auf Empfehlungen für Herstellerinnen und Hersteller, die KI-Modelle oder -Systeme für eigene Zwecke entwickeln und einsetzen. Die Einbindung von KI-Modellen oder -Systemen, die durch andere entwickelt wurden, stand nicht im Fokus. Gleichwohl sind viele der in der Orientierungshilfe beschriebenen Maßnahmen auch auf diesen Fall anwendbar.

Im Oktober 2025 veröffentlichte die Datenschutzkonferenz zudem die Orientierungshilfe „Datenschutzrechtliche Besonderheiten generativer KI-Systeme mit RAG-Methode“. Auch an deren Erstellung waren wir beteiligt.

Retrieval Augmented Generation (RAG) ist eine Technologie, mit der KI-Systeme um zusätzliche Komponenten ergänzt werden, die kontextspezifische Inhalte z. B. aus unternehmens- oder behörden-

8 Tätigkeitsbericht Datenschutz 2024, A I 3.

internen Wissensquellen (den so genannten Referenzdokumenten) bereitstellen. RAG-(Sub-)Systeme können unabhängig von einem großen Sprachmodell (Large Language Model, LLM) entwickelt und betrieben werden. Letzteres bleibt jedoch wichtig für die Erzeugung der textlichen Antwort auf Anfragen von Nutzerinnen und Nutzern und bezieht dabei insbesondere die spezifischen, zuvor besonders aufbereiteten Wissensquellen der Institution ein. Dies eröffnet Verantwortlichen auch die Möglichkeit, eine größere Kontrolle über die Verarbeitung personenbezogener Daten im KI-Gesamtsystem auszuüben und Risiken für die betroffenen Personen zu verringern.

Insbesondere kann die Nutzung von RAG im Hinblick auf die Bereitstellung kontextbezogener und überprüfbarer Inhalte positive Effekte auf die Richtigkeit und Nachvollziehbarkeit der Ausgaben eines KI-Systems mit sich bringen. Weiterhin lassen sich in einem durch RAG ergänzten System die Vertraulichkeit und Integrität bei der Verarbeitung von zusätzlich eingebundenen personenbezogenen Daten verbessern. Das genutzte Sprachmodell kann in der Regel kleiner sein und lokal vorgehalten werden; es benötigt weniger umfangreiche Trainingsdaten. Die Extraktion personenbezogener Daten aus dem KI-System kann vom Verantwortlichen besser kontrolliert und ggf. unterbunden werden. Gleiches gilt für die Nutzung dieser Daten zum Training und zur Weiterentwicklung des Modells.

Allerdings bleiben einige datenschutzrechtliche Herausforderungen im Kontext der Nutzung von Künstlicher Intelligenz – insbesondere von großen Sprachmodellen – auch beim Einsatz von RAG bestehen. Dies betrifft beispielsweise die datenschutzrechtliche Beurteilung des KI-Trainings, die Einhaltung der Grundsätze der Zweckbindung und der Datensparsamkeit oder die Gewährleistung der Transparenz und der Rechte betroffener Personen. Die damit zusammenhängenden Fragen sind von den Verantwortlichen jeweils im Einzelfall zu beantworten.

7 Gesetzentwurf des Bundes zur Umsetzung der KI-Verordnung

Im Rahmen der Umsetzung der Verordnung über Künstliche Intelligenz (KI-Verordnung, KI-VO) hatten die Mitgliedstaaten der Europäischen Union u. a. bis zum 2. August 2025 zuständige Behörden für die Marktüberwachung zu benennen. Die Bundesregierung hat dazu im September 2025 einen Referentenentwurf für ein Gesetz zur Durchführung der KI-Verordnung[9] vorgelegt, wonach die Bundesnetzagentur (mit sektorspezifischen Ausnahmen) zentrale Marktüberwachungsbehörde werden soll. Zum Zeitpunkt des Redaktionsschlusses dieses Berichts lief zu diesem Entwurf die Länder- und Verbändeanhörung.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat zum Entwurf des Gesetzes Stellung genommen.[10] Wesentliche Kritikpunkte sind die Gefahr von Doppelzuständigkeiten im Kontext von Hochrisiko-KI-Systemen im Sicherheitsbereich, die Missachtung der grundgesetzlichen, föderalen Zuständigkeitsordnung, unklare Regelungen zur Zusammenarbeit zwischen Marktüberwachungs- und Datenschutzaufsichtsbehörden sowie die fehlende Möglichkeit, sogenannte Reallabore auch jenseits der Bundesnetzagentur zu unterhalten.

Artikel 74 Absatz 8 KI-VO sieht vor, dass die Mitgliedstaaten die Marktüberwachung über Hochrisiko-KI-Systeme gemäß Anhang III Nummern 1, 6, 7 und 8 KI-VO (z. B. bei Strafverfolgung, Wahlen, Grenzkontrollen, Rechtspflege) bestimmten Behörden zuweisen. Namentlich sind das die Datenschutzaufsichtsbehörden nach Datenschutz-Grundverordnung oder Richtlinie (EU) 2016/680 (JI-Richt-

9 Referentenentwurf des Bundesministeriums für Digitales und Staatsmodernisierung für ein Gesetz zur Durchführung der KI-Verordnung (Bearbeitungsstand: 11. September 2025).

10 Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 10. Oktober 2025 zum Entwurf eines Gesetzes zur Durchführung der Verordnung über künstliche Intelligenz (KI-VO).

linie) oder Behörden, die denselben Bedingungen unterliegen, wie sie in den Artikeln 41 bis 44 JI-Richtlinie festgelegt sind. Hier wollte der Verordnungsgeber gerade ermöglichen, die nach der Datenschutz-Grundverordnung und der JI-Richtlinie bereits bestehenden Zuständigkeiten in grundrechtssensiblen Bereichen auch für die Überwachung der KI-Verordnung zu nutzen. Der Referentenentwurf sieht jedoch vor, bei der Bundesnetzagentur eine Unabhängige KI-Marktüberwachungskammer (UKIM) einzurichten. Sie soll auch den Einsatz von Hochrisiko-KI-Systemen von Landesbehörden beaufsichtigen. Dies stellt einen Verstoß gegen die grundgesetzliche Zuständigkeitsordnung dar (vgl. Artikel 30 Grundgesetz) und schafft Doppelstrukturen. Denn die Datenschutzaufsichtsbehörden bleiben – unabhängig von einer gesetzlichen Regelung zur Umsetzung der KI-Verordnung – zuständig für die Verarbeitung personenbezogener Daten in Hochrisiko-KI-Systemen der Landesbehörden. Das gilt auch für die in Anhang III Nummern 1, 6, 7 und 8 KI-VO aufgeführten Bereiche.

Setzt etwa die Polizei Brandenburg ein für eigene Zwecke entwickeltes KI-System zur biometrischen Fernidentifizierung ein (vgl. Anhang III Nummer 1 Buchstabe a KI-VO), wäre nach dem Referentenentwurf die UKIM als Marktüberwachungsbehörde gemäß Artikel 74 Absatz 8 KI-VO zur Bewertung des Hochrisiko-KI-Systems zuständig, während die Landesbeauftragte gemäß § 18 Absatz 1 Satz 1 Brandenburgisches Datenschutzgesetz (BbgDSG) i. V. m. Artikel 41 Absatz 1 JI-Richtlinie zuständige Aufsichtsbehörde zur Überwachung der Verarbeitung personenbezogener Daten ist. Der Entwurf bezieht sich dabei hinsichtlich der Gesetzgebungskompetenz des Bundes auf das Recht der Wirtschaft gemäß Artikel 74 Nummer 11 Grundgesetz, während das Beispiel zeigt, dass hier eindeutig eine ausschließliche Gesetzgebungs- und Verwaltungskompetenz der Länder besteht. Ähnliches würde z. B. auch für Hochrisiko-KI-Systeme im Bereich der allgemeinen und beruflichen Bildung gelten (Anhang III Nummer 3 KI-VO).

Im Hinblick auf die Zusammenarbeit zwischen den Marktüberwachungsbehörden (insbesondere der Bundesnetzagentur) und den Datenschutzaufsichtsbehörden bleibt der Referentenentwurf vage. Nach Auffassung der Datenschutzkonferenz muss sich die noch zu treffende Regelung an den Aufgaben und Befugnissen der Datenschutzaufsichtsbehörden orientieren. Ihnen obliegt die Bewertung und Entscheidung zur Vereinbarkeit der Verarbeitung personenbezo-

gener Daten in KI-Systemen mit dem Datenschutzrecht. Diese müssen für Marktüberwachungsbehörden wie die Bundesnetzagentur bindend sein.

Dem Referentenentwurf fehlt darüber hinaus eine Klarstellung, dass auch die Datenschutzaufsichtsbehörden KI-Reallabore i. S. v. Artikel 57 und 58 KI-VO mit datenschutzrechtlichem Fokus einrichten und betreiben können. KI-Reallabore bieten eine kontrollierte Umgebung, um Innovation zu fördern und die Entwicklung, das Training, das Testen und die Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem produktiven Einsatz nach einem mit der zuständigen Behörde vereinbarten Reallabor-Plan zu erleichtern.

Artikel 57 Absatz 2 KI-VO regelt ausdrücklich, dass KI-Reallabore auch auf regionaler und lokaler Ebene möglich sind. Der Referentenentwurf sieht jedoch vor, dass KI-Reallabore bei der Bundesnetzagentur und ggf. bei sektorspezifischen Marktüberwachungsbehörden eingerichtet werden. Dies umfasst aber gerade nicht die Datenschutzaufsichtsbehörden.

8 Behördeninterne Fortbildungen zum Thema Künstliche Intelligenz

Seit dem 2. Februar 2025 sind die Kapitel I und II der europäischen Verordnung über Künstliche Intelligenz (KI-Verordnung, KI-VO) gültig. Zu den ab diesem Zeitpunkt anzuwendenden Vorschriften gehört Artikel 4 KI-VO. Darin werden Anbieterinnen und Anbieter sowie Betreiberinnen und Betreiber von KI-Systemen zu Maßnahmen verpflichtet, die sicherstellen, dass ihr Personal beim Betrieb und bei der Nutzung von KI-Systemen über ein ausreichendes Maß an KI-Kompetenz verfügt. Damit sind u. a. Kenntnisse und Fähigkeiten der Beschäftigten gemeint, um KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von Künstlicher Intelligenz bewusst zu sein.

Aus unserer Sicht ist es zwingend erforderlich, die entsprechende Kompetenz auch auf Seiten der Datenschutzaufsichtsbehörde aufzubauen. Nur unter dieser Voraussetzung ist es möglich, öffentliche und nicht öffentliche Stellen, die KI-Modelle bzw. KI-Systeme entwickeln oder einsetzen und hierbei personenbezogene Daten verarbeiten, sachkundig zu beraten, ihre Projekte zu begleiten und eine fundierte datenschutzrechtliche bzw. technische Bewertung vorzunehmen. Aus diesem Grund haben wir im Berichtszeitraum mehrere interne Fortbildungen zu KI-Themen eigenverantwortlich organisiert und durchgeführt. Zielgruppe waren unsere eigenen Mitarbeiterinnen und Mitarbeiter.

Für einen Einstieg in das Gebiet Künstliche Intelligenz wurde zunächst allen Beschäftigten – unabhängig von ihrer Tätigkeit in der Dienststelle – eine Grundlagenschulung angeboten. Ziel dieser Schulung war eine verständliche Einführung in das Thema und die Darstellung relevanter Zusammenhänge. Neben der notwendigen Klärung von Fachbegriffen (wie Künstliche Intelligenz, Maschinelles Lernen, Künstliche Neuronale Netze) wurden insbesondere die Funktionsweise großer Sprachmodelle und Aspekte generativer KI vermittelt. Auch gesellschaftliche Auswirkungen des KI-Einsatzes waren Teil der Erörterung. Weiterführende Hinweise zu Literatur, zu Online-Kursen und zu KI-Werkzeugen erlauben es Beschäftigten, sich bei Bedarf individuell weiter in die Materie zu vertiefen. Diese Grundlagenschulung wurde mehrfach durchgeführt; eine Wiederho-

lung ist geplant, um auch neue Beschäftigte der Dienststelle auf den gleichen Wissensstand zu bringen.

Darüber hinaus erhielten Fachreferentinnen und -referenten spezifische interne Fortbildungen. Im Mittelpunkt standen dabei die Anforderungen der KI-Verordnung und ihre Wechselwirkungen mit datenschutzrechtlichen Regelungen. Thematisiert wurden insbesondere die aus der Datenschutz-Grundverordnung anzuwendenden Rechtsgrundlagen für die Nutzung von KI-Systemen und das Training von KI-Modellen. Für die Schulungsteilnehmerinnen und -teilnehmer war in diesem Kontext wichtig, die Zusammenhänge anhand ausgewählter Fallkonstellationen zu diskutieren. Sie konnten auch konkrete Beispiele einbringen, die sich aus der zunehmenden Anzahl von Beschwerden mit KI-Bezug, die betroffene Personen bei uns einlegen, ergaben.

Ebenfalls seit Februar 2025 gelten die Regelungen zu verbotenen Praktiken im KI-Bereich, die in Artikel 5 KI-VO festgeschrieben sind. Hierzu gehört das Verbot der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken – mit gewissen Ausnahmen, die ebenfalls Artikel 5 KI-VO beschreibt. Vor dem Hintergrund unserer datenschutzrechtlichen Aufsichtszuständigkeit nach § 18 Absatz 1 Brandenburgisches Datenschutzgesetz i. V. m. der Richtlinie (EU) 2016/680 (JI-Richtlinie) über Behörden, Einrichtungen und sonstigen öffentlichen Stellen im Bereich der Strafverfolgung haben die zuständigen Referentinnen und Referenten eine interne Schulung erhalten, in der die entsprechenden Vorschriften der KI-Verordnung im Überblick dargestellt und die Auswirkungen auf die datenschutzbehördliche Aufsichtstätigkeit diskutiert wurden.

Das Format der internen Fortbildungen hat sich bewährt. Wir werden entsprechende Veranstaltungen auch in Zukunft durchführen. Bereits jetzt ist geplant, Schulungen anzubieten, die auf den im Berichtsjahr veröffentlichten Orientierungshilfen der Datenschutzkonferenz[11] zu technischen und organisatorischen Maßnahmen bei der Planung und beim Einsatz von KI-Systemen sowie zu KI-Systemen mit RAG-Komponente (Retrieval Augmented Generation) aufbauen.

---

11 Siehe A I 6.

In Vorbereitung befindet sich weiterhin eine tiefergehende Erörterung zu technischen Details großer Sprachmodelle.

II Datenschutzverstöße: Maßnahmen und Sanktionen

1 Anforderung eines Gehaltsnachweises im Mietverhältnis

Nach einem Eigentümerwechsel forderte die neue Vermieterin ihre Mieterin dazu auf, einen aktuellen Gehaltsnachweis vorzulegen, obwohl das Vertragsverhältnis ohne Störungen verlaufen war. Die Betroffene kam dieser Forderung nicht nach und beschwerte sich bei uns.

Die Vermieterin erläuterte im Rahmen unserer Anhörung die Hintergründe und die Rechtsgrundlage, die es aus ihrer Sicht erlaubt, das aktuelle Nettoeinkommen der Mieterin zu erfahren. So habe die vormalige Eigentümerin der Wohnung den Mietvertrag mit der Beschwerdeführerin unter Berücksichtigung ihres befristeten Arbeitsvertrags geschlossen, der mit der Mieterakte übergeben worden war. Da der Arbeitsvertrag jedoch ausgelaufen war, hatte die neue Eigentümerin keine Kenntnis der aktuellen Bonität.

Datenschutzrechtlich gilt der Grundsatz des Verbots mit Erlaubnisvorbehalt. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn sie eine der in Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) genannten Voraussetzungen erfüllt. Diese lagen jedoch hier nicht vor:

Eine Einwilligung beispielsweise kam nicht in Betracht. Sie muss stets freiwillig abgegeben werden. Wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, ist die Freiwilligkeit regelmäßig zu bezweifeln. Im vorliegenden Fall existierte sie ohnehin nicht. Die Mieterbonität bei einem laufenden Mietvertragsverhältnis erneut zu überprüfen, ist auch weder zur Durchführung des Vertragsverhältnisses noch zur Erfüllung einer rechtlichen Verpflichtung oder zum Schutz lebenswichtiger Interessen erforderlich.

Es lag auch kein überwiegendes berechtigtes Interesse an einer Bonitätsüberprüfung im laufenden Mietvertragsverhältnis vor, sodass der Erlaubnistatbestand des Artikel 6 Absatz 1 Buchstabe f DS-GVO im Hinblick auf die Anforderung eines aktuellen Gehaltsnachweises nicht erfüllt war. Ein Mietverhältnis wird als längerfristiges Dauerschuldverhältnis regelmäßig im Vertrauen darauf begründet, dass beide Parteien für die Dauer des Vertrags imstande sind, ihren vertraglichen Verpflichtungen nachzukommen. Deshalb ist vor Vertragsschluss die Erfragung der Höhe des Nettoeinkommens und desjenigen Betrags, der nach Abzug der laufenden monatlichen Belastungen für die Tilgung des Mietzinses zur Verfügung steht, regelmäßig zulässig. Der Nachweis kann z. B. durch eine Lohn- oder Gehaltsabrechnung, einen Kontoauszug oder einen Einkommensteuerbescheid in Kopie – jeweils unter Schwärzung der nicht erforderlichen Angaben – erfolgen.

Einmaliger Nachweis genügt meist

Zum Zeitpunkt der Mietvertragsanbahnung hatte die Mieterin diesen Nachweis durch die Vorlage ihres befristeten Arbeitsvertrages erbracht. Die damalige Eigentümerin hatte ihn auch anerkannt und für ausreichend erachtet – sie entschied sich für die Betroffene als zukünftige Mieterin.

Durch den Eigentümerwechsel änderte sich am bestehenden Mietverhältnis – bis auf eine Vertragspartei – nichts. Die Mieterin leistete die Mietzahlungen regelmäßig und ohne Störungen. Es bestand kein Anlass, ihre Zahlungsfähigkeit nach dem Eigentumswechsel zu überprüfen. Mieterinnen und Mieter sind während des laufenden Mietverhältnisses auch nicht verpflichtet, ihre Vermieterinnen oder ihre Vermieter über Einkommensänderungen zu informieren.

Eine Rechtsgrundlage für die Forderung eines Gehaltsnachweises bestand somit nicht. Die Landesbeauftragte hat gegenüber der Vermieterin eine Warnung gemäß Artikel 58 Absatz 2 Buchstabe a DS-GVO ausgesprochen, weil die beabsichtigte Datenverarbeitung gegen die Datenschutz-Grundverordnung verstoßen würde.

2 Übermittlung von Mieterdaten an den sozialpsychiatrischen Dienst

Eine Wohnungsgenossenschaft hatte Schwierigkeiten mit einem Mieter und erhoffte sich Unterstützung vom sozialpsychiatrischen Dienst der Stadtverwaltung am Wohnort. Zu diesem Zweck übermittelte sie dessen Daten dorthin. Der Betroffene konnte nicht nachvollziehen, welche konkreten Informationen zu seiner Person von der Wohnungsgenossenschaft an die Stadt übermittelt worden waren, und beschwerte sich bei uns.

In ihrer Stellungnahme erläuterte die Genossenschaft die Hintergründe der Kontaktaufnahme mit dem sozialpsychiatrischen Dienst. Übermittelt wurden Name und Anschrift des Beschwerdeführers sowie der Hinweis, dass das Mietverhältnis durch Beschimpfungen und Bedrohungen gegenüber der Reinigungsfirma sowie der Hausverwaltung nachhaltig gestört sei. Weiter argumentierte der Verantwortliche, dass eine konstruktive Beteiligung des Mieters zur Verbesserung der Kommunikation und der Herstellung des Hausfriedens ebenso wenig zu erwarten gewesen sei wie die Einwilligung zur Datenübermittlung. Stattdessen wurde die Übermittlung auf Artikel 6 Absatz 1 Buchstabe b und f Datenschutz-Grundverordnung (DS-GVO) gestützt. Sie sei zur Durchführung des Mietverhältnisses und zur Wahrung berechtigter Interessen der Wohnungsgenossenschaft erforderlich gewesen, damit der sozialpsychiatrische Dienst den Mieter ansprechen und ihm ein Beratungsangebot zur Konfliktbeseitigung unterbreiten könne. Die schutzwürdigen Interessen des Mieters hätten angesichts der mitgeteilten Daten nicht überwogen.

Die Übermittlung der personenbezogenen Daten an den sozialpsychiatrischen Dienst ließ sich nach unserer Einschätzung auf keinen der Erlaubnistatbestände nach Artikel 6 Absatz 1 DS-GVO stützen. Eine Einwilligung nach Artikel 6 Absatz 1 Buchstabe a DS-GVO wurde von dem Mieter nicht eingeholt. Die Datenübermittlung war auch nicht für die Durchführung des Mietvertrags nach Artikel 6 Absatz 1 Buchstabe b DS-GVO erforderlich. Den Vortrag der Genossenschaft hielten wir nicht für ausreichend. Ebenso wenig konnte sich die Genossenschaft auf Artikel 6 Absatz 1 Buchstabe f DS-GVO berufen.

Voraussetzung der letztgenannten Vorschrift ist, 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.

Ein Interesse ist berechtigt, wenn es schutzwürdig und objektiv begründbar ist. Ein schutzwürdiges Interesse der Genossenschaft mussten wir verneinen. Außerdem lag keine Störung des Hausfriedens im Sinne des § 569 Absatz 2 Bürgerliches Gesetzbuch vor, da andere Mieterinnen und Mieter von dem Streit nicht betroffen waren. Insofern hatten wir Zweifel, dass ein berechtigtes Interesse an der Datenübermittlung bestand.

Konflikte datensparsam lösen

Selbst bei Vorliegen dieser Voraussetzung hätte die konkrete Datenverarbeitung zur Wahrung der berechtigten Interessen der Genossenschaft auch tatsächlich erforderlich sein müssen. Voraussetzung hierfür wäre gewesen, dass kein milderes, gleich effektives Mittel zur Verfügung gestanden hätte, um die beabsichtigten Zwecke zu erreichen – eine bloße Zweckdienlichkeit genügt nicht. Um weniger in die Rechte des Betroffenen einzugreifen, hätte der Verantwortliche diesen zunächst schlicht über das Beratungsangebot des sozialpsychiatrischen Dienstes informieren können. Die Datenverarbeitung war somit nicht erforderlich. Im Ergebnis waren die Voraussetzungen für die Übermittlung der Mieterdaten an den sozialpsychiatrischen Dienst der Stadtverwaltung auch auf der Grundlage von Artikel 6 Absatz 1 Buchstabe f DS-GVO nicht erfüllt.

Wegen dieses datenschutzrechtlichen Verstoßes haben wir den Verantwortlichen gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO verwarnt.

3 Übermittlung von Mietdaten an den Arbeitgeber

Eine Vermieterin stand mit ihrer Mieterin im Streit um die Nutzung eines Nebengelasses. Dieses sollte entweder geräumt oder zusätzlich gemietet werden. Weil keine Reaktion erfolgte, erwog sie, einen Dienstleister mit der Räumung zu beauftragen. Dieser war gleichzeitig Arbeitgeber der Mieterin. Zur Bekräftigung ihrer Forderung übermittelte die Vermieterin auch Daten aus dem Mietverhältnis an das Unternehmen und regte an, in einem Mitarbeitergespräch eine Klärung herbeizuführen. Die Mieterin sah keine Notwendigkeit für die Datenübermittlung und beschwerte sich bei uns.

Die Vermieterin führte in ihrer Stellungnahme aus, dass sie keine Daten übermittelt hätte, die der Arbeitgeber nicht ohnehin bereits kannte. Außerdem hätte die Mieterin genügend Zeit gehabt, das Nebengelass zu mieten oder zu räumen. Sie konnte keine Verletzung der Persönlichkeitsrechte erkennen und verwies auf den Schutz ihrer Eigentumsrechte.

Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Die Datenschutz-Grundverordnung (DS-GVO) folgt dem Prinzip des Verbots mit Erlaubnisvorbehalt. Das bedeutet, dass jegliche Verarbeitung – wozu auch die Übermittlung zählt – verboten ist, es sei denn, es liegt eine der in Artikel 6 Absatz 1 DS-GVO genannten Rechtsgrundlagen vor. Auch der Umstand, dass der Empfängerin oder dem Empfänger die Daten bereits bekannt sind, ändert nichts an dieser Anforderung. Die Datenschutz-Grundverordnung schützt das Recht der betroffenen Person auf Kontrolle darüber, wer wann welche ihrer Daten verarbeitet, und sorgt nicht nur für die Vertraulichkeit der Daten beim Verantwortlichen selbst.

Im vorliegenden Fall wurde weder eine Einwilligung der Mieterin gemäß Artikel 6 Absatz 1 Buchstabe a DS-GVO in die Übermittlung eingeholt noch war Letztere für die Durchführung des Mietvertrags gemäß Artikel 6 Absatz 1 Buchstabe b DS-GVO erforderlich. Die in Rede stehende Datenverarbeitung war auch nicht nach Artikel 6 Absatz 1 Buchstabe f DS-GVO zulässig. Aus der Sachverhaltsdarstellung ergab sich weder ein persönliches, berechtigtes Interesse der Vermieterin, die Daten aus dem Mietverhältnis zu übermitteln,

noch ein berechtigtes Interesse des Arbeitgebers an der Kenntnis der Daten.

Darüber hinaus ist mit der Datenübermittlung eine Änderung der Verarbeitungszwecke verbunden. Diese kann auch nicht auf Artikel 6 Absatz 4 DS-GVO i. V. m. § 24 Bundesdatenschutzgesetz (BDSG) gestützt werden. § 24 Absatz 1 Nummer 2 BDSG lässt eine Zweckänderung zu, wenn sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Im vorliegenden Fall war weder die Erforderlichkeit gegeben noch wäre die Interessenabwägung zugunsten der Vermieterin ausgegangen.

Wegen dieses Verstoßes wurde die Vermieterin gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO verwarnt.

4 Verlust sämtlicher Daten bei einer Arztpraxis

Im Berichtszeitraum schlossen wir einen im Vorjahr eröffneten Vorgang ab. Er zeigt, dass eine Datensicherung allein kein Garant dafür ist, die Verfügbarkeit der verarbeiteten personenbezogenen Daten auf Dauer sicherzustellen. Dies verlangt jedoch Artikel 32 Absatz 1 Datenschutz-Grundverordnung (DS-GVO).

Ausgangspunkt war die Meldung einer Arztpraxis über eine Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 DS-GVO. Daraus ging hervor, dass die IT-Systeme der Praxis Opfer einer Schadsoftware geworden waren, konkret wurden sie durch eine sogenannte Ransomware befallen. Angriffe mit Ransomware gehören zu den häufigsten Cyberangriffen. Durch die Ausnutzung einer Sicherheitslücke oder durch eine menschliche Fehlhandlung gelangt die Schadsoftware auf das Zielsystem. Ihre Funktion besteht darin, Daten zu verschlüsseln, sodass sie im Ergebnis nicht mehr nutzbar sind. Anschließend soll der Verantwortliche ein „Lösegeld“ zahlen, um einen Schlüssel zur Entschlüsselung der Daten zu erhalten. In der Regel wird empfohlen, nicht zu zahlen, da die Lieferung des Schlüssels nicht garantiert ist. In einem solchen Fall hilft eine in angemessenen Abständen erstellte Sicherheitskopie, die Verfügbarkeit der Daten wiederherzustellen und den IT-Betrieb fortzusetzen. In der Regel sind die Unterschiede zwischen den aus der Kopie zurückgespielten Daten und ihrer letzten Version gering und können mit vertretbarem Aufwand kompensiert werden.

Der Meldung entnahmen wir, dass ca. 75 Gigabyte an medizinischen und administrativen Daten zu über 8.000 Patientinnen und Patienten von dem Vorfall betroffen waren. Ein Abfluss der Daten im Rahmen des Angriffs konnte durch einen IT-Dienstleister ausgeschlossen werden. Weiter wurde mitgeteilt, dass Versuche zur Entschlüsselung und Wiederherstellung der Daten aus der Sicherheitskopie gescheitert waren.

Dies verwunderte uns, da eine Datensicherung eigentlich genau zu diesem Zweck erstellt wird und – ein korrektes Verfahren vorausgesetzt – der Rückgriff auf die gesicherten Daten keine sonderlich komplexe Aufgabe ist. Im Rahmen einer Anhörung wollten wir Ge-

naueres erfahren. Dabei stellte sich heraus, dass in der Arztpraxis zwar eine Datensicherung nach der 3-2-1-Regel durchgeführt werden sollte, deren Umsetzung jedoch mangelhaft war. Die genannte Regel entspricht grundsätzlich dem Stand der Technik. Sie besagt, dass drei Kopien der zu sichernden Daten auf mindestens zwei unterschiedlichen Speichermedien (z. B. Festplatte, SSD, CD, DVD, Sicherungsband) liegen, wobei eine der Kopien räumlich getrennt an einem anderen Standort aufzubewahren ist.

Im konkreten Fall gab es zwar mehrere Festplatten, die als Sicherungsmedium dienten. Sie waren jedoch zum Zeitpunkt des Angriffs alle parallel am IT-System mit den zu sichernden Daten angeschlossen. Da die Ransomware auf sie zugreifen konnte, wurden die dort gespeicherten Daten mitverschlüsselt. Im Ergebnis gab es also keine unverschlüsselte Kopie der Daten mehr, die hätte zurückgespielt werden können. Alle Daten waren unwiederbringlich verloren.

Aufgrund der fehlerhaften Umsetzung der Datensicherung in der Arztpraxis wurde weder die Verfügbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten sichergestellt noch gelang es, die Verfügbarkeit der Daten nach dem Zwischenfall rasch wiederherzustellen. Somit lag ein Verstoß gegen Artikel 32 Absatz 1 Buchstabe b und c DS-GVO vor. Wegen dieses Verstoßes verwarnten wir die Praxis gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO. Darüber hinaus gaben wir einige Hinweise für eine Anpassung und Verbesserung der Datensicherungsmaßnahmen vor Ort.

5 Online-Recruiting kann gegen Datenschutz verstoßen

Durch Beschwerden fiel uns auf, dass spezialisierte Agenturen zur Personalvermittlung zunehmend Daten von Internetnutzerinnen und -nutzern verwenden, um ihnen offene Stellen anzubieten. Im vorliegenden Fall hatte sich der Verantwortliche auf die Vermittlung von Fachkräften aus dem IT-Bereich u. a. an Tech-Unternehmen fokussiert. Hierzu legte er ein eigenes Profil auf einer Plattform an, die Institutionen und Einzelpersonen die Möglichkeit bietet, sich über eigene Softwareprojekte auszutauschen und gemeinsam daran zu arbeiten. Auch der Beschwerdeführer hatte ein Profil auf der Plattform, das seinen Namen und seine private E-Mail-Adresse enthielt. Der Verantwortliche sandte ihm innerhalb von drei Tagen zwei unerwünschte E-Mails mit spezifischen Stellenangeboten. Zwischen beiden bestand kein vorheriger Kontakt. Nach einem erfolglosen Auskunftsersuchen gemäß Artikel 15 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) reichte der Betroffene eine Beschwerde bei uns ein. Darin zweifelte er auch die Rechtmäßigkeit der erhaltenen Werbe-E-Mails an.

In seiner Stellungnahme führte der Verantwortliche aus, dass das Auskunftsersuchen einen fremdsprachigen, im Ausland tätigen Beschäftigten erreicht hatte, der das Ersuchen nicht intern an die zuständige Stelle weiterleitete. Deswegen war eine Antwort auf das Auskunftsersuchen ausgeblieben. Das Profil des Betroffenen auf der Online-Plattform habe mit einer Suchanfrage eines Kunden des Verantwortlichen übereingestimmt, sodass der Betroffene für das Vermittlungsangebot ausgewählt und kontaktiert worden war. Hierbei ging der Verantwortliche davon aus, dass es sich bei dieser Kontaktaufnahme nicht um Werbung handelte. Außerdem vertrat er den Standpunkt, dass der Betroffene durch die Angabe seiner E-Mail-Adresse auf der Plattform des Online-Dienstes eindeutig zum Ausdruck gebracht habe, mit Kontaktaufnahmen zur Geschäftsanbahnung einverstanden zu sein. Er ging weiter davon aus, das Zusenden der E-Mails auf eine Einwilligung in die Datenverarbeitung oder eine Wahrnehmung berechtigter Interessen als Rechtsgrundlage stützen zu können.

Wir stellten fest, dass der Verantwortliche bei dem hier beschriebenen Online-Recruiting gegen Artikel 6 Absatz 1 DS-GVO verstoßen hat, indem er den Namen und die E-Mail-Adresse des Betroffenen ohne Rechtsgrundlage zu Werbezwecken verwendete. Der Begriff Werbung umfasst 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.[12] Er ist weit zu verstehen. Im vorliegenden Fall lag weder eine Einwilligung der betroffenen Person nach Artikel 6 Absatz 1 Buchstabe a DS-GVO vor noch wäre die nach Artikel 6 Absatz 1 Buchstabe f DS-GVO vorzunehmende Abwägung der Interessen zugunsten des Verantwortlichen ausgegangen.

Personalakquise mit Hürden

Eine Einwilligung ist nach Artikel 4 Nummer 11 DS-GVO 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. Entgegen der Ansicht des Verantwortlichen stellte allein der Umstand, dass der Nutzer auf der Webseite des Online-Dienstes ein Profil angelegt hatte, keine explizite Erlaubnis für die Kontaktaufnahme dar. Im vorliegenden Fall war zudem davon auszugehen, dass der Betroffene die Plattform zum Austausch mit anderen Nutzerinnen und Nutzern ausschließlich privat nutzte. In diesem Kontext musste er nicht erwarten, Ziel von Werbung Dritter zu werden. Seine Interessen haben damit Vorrang vor denen des Unternehmens, Werbung zu versenden.

Darüber hinaus lag ein Verstoß gegen die gesetzlichen Vorgaben für die Ausübung der Betroffenenrechte nach Artikel 12 Absatz 1 und 3 DS-GVO vor. Das Auskunftsersuchen wurde nicht innerhalb der einmonatigen Frist des Artikels 12 Absatz 3 Satz 1 DS-GVO beantwortet. Außerdem hatte der Verantwortliche es versäumt, die Erfüllung der Betroffenenrechte organisatorisch sicherzustellen. So hätte

12 Richtlinie 2006/114/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über irreführende und vergleichende Werbung (ABl. L 376 vom 27.12.2006, S. 21).

er dafür sorgen müssen, dass der Auskunftsantrag an die zuständige Kontaktstelle innerhalb des Unternehmens weitergeleitet und fristgemäß bearbeitet wird. Einen entsprechenden Hinweis, an wen Anfragen zu den Betroffenenrechten zu richten sind, hatte der Verantwortliche weder in den Werbe-E-Mails noch in den Bestimmungen zum Datenschutz auf seiner Internetpräsenz aufgeführt.

Auch lag ein Verstoß gegen Artikel 14 Absatz 3 Buchstabe b DS-GVO vor, da der Verantwortliche seinen Informationspflichten nach Artikel 14 Absatz 1 und 2 DS-GVO gegenüber dem Betroffenen nicht spätestens zum Zeitpunkt der ersten Kontaktaufnahme nachgekommen war. Der Verantwortliche hatte den Namen und die private E-Mail-Adresse des Betroffenen nämlich dem Nutzerprofil auf der Plattform entnommen. Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so muss der Verantwortliche der betroffenen Person die in Artikel 14 Absatz 1 und 2 DS-GVO normierten Informationen mitteilen. Hierzu gehören etwa Informationen über die Verarbeitungszwecke sowie die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten. Die Werbe-E-Mails des Verantwortlichen entbehrten jeglicher Angabe hierzu.

Wegen der festgestellten Verstöße verwarnte die Landesbeauftragte den Verantwortlichen gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO.

6 Videoüberwachung in einem Barbershop

Um Vandalismus vorzubeugen und die Kassenvorgänge am Tresen zu kontrollieren, filmte der Inhaber eines Barbershops mit zwei Videokameras vor allem die Plätze, die zum Bedienen der Kundschaft vorgesehen sind, sowie einzelne Sitzgelegenheiten in den Wartebereichen. Konkrete Vorkommnisse, die Anlass für die Videoüberwachung hätten sein können, gab es nicht.

Im Rahmen des Aufsichtsverfahrens wiesen wir den Verantwortlichen darauf hin, dass nicht erkennbar war, inwieweit die Videoüberwachung geeignet sein soll, Vandalismus zu verhindern oder die Kassenabläufe zu kontrollieren. Zwischen den überwachten Bereichen und den angegebenen Zwecken bestand kein Zusammenhang. Zudem hat ein Verantwortlicher vor dem Einsatz von Videokameras stets zu prüfen, ob gleich geeignete, mildere Mittel zur Verfügung stehen, um den beabsichtigten Zweck zu erreichen. So hätten etwa die Beschäftigten im Falle eines Vorfalls unmittelbar reagieren oder Hilfe hinzuziehen können. Auch mechanische Sicherungen an der Kasse oder das Wegschließen wertvoller Gegenstände wären geeignete und weniger eingriffsintensive Maßnahmen gewesen. Gerade zum Schutz der Kasse sind derartige Vorkehrungen regelmäßig vorzuziehen, da sie – anders als Kameras – tatsächliche, physische Barrieren schaffen.

Haarscharfe Bilder fehl am Platz

Die eingesetzten Kameras filmten Kunden, die beispielsweise auf ihren Termin warteten oder bedient wurden, sowie die Beschäftigten während ihrer Arbeit. Dies stellte einen erheblichen Eingriff in deren Recht auf informationelle Selbstbestimmung dar. Das Interesse des Verantwortlichen an der Videoüberwachung überwog nicht. Insbesondere war keine Gefährdungslage ersichtlich, die über das allgemeine Lebensrisiko hinausging. Im Ergebnis konnte die Videoüberwachung nicht auf die Rechtsgrundlage des Artikels 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) gestützt werden. Die Datenverarbeitung war unzulässig.

Wegen dieses Verstoßes sprachen wir eine Verwarnung gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO aus. Hierbei wurde berücksichtigt, dass der Verantwortliche die Datenverarbeitung aufgrund

unserer datenschutzrechtlichen Bewertung umgehend beendet und sämtliche Kameras entfernt hatte.

7 Videoüberwachung in einem Schwimmbad

Auch in diesem Berichtszeitraum mussten wir uns wieder mit einer Videoüberwachung in einem Schwimmbad befassen – ausgelöst durch eine Beschwerde über Kameras in den Umkleidebereichen. Regelmäßig umfassen derartige Anlagen zahlreiche Kameras, die von uns einzeln datenschutzrechtlich bewertet werden. Im Beschwerdefall hatte der Verantwortliche nahezu 30 Kameras installiert.

Vor dem Hintergrund des Umfangs der Videoüberwachung hatten wir den Verantwortlichen zunächst zu einer Beratung in die Dienststelle gebeten, um anhand der eingereichten Screenshots der Kameras die datenschutzrechtlichen Erfordernisse zu erläutern und offene Fragen zu klären.

Die Datenverarbeitung mittels Videoüberwachung in Schwimmbädern durch nicht öffentliche Stellen ist am Maßstab von Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) zu messen. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, soweit dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Im vorigen Tätigkeitsbericht[13] hatten wir bereits ausgeführt, wie die Datenverarbeitung mittels Videoüberwachung in Schwimmbädern, differenziert nach den verschiedenen Erfassungsbereichen, zu bewerten ist.

Diese Grundsätze kamen auch in dem vorliegenden Beschwerdefall zur Anwendung. Zunächst war zwischen Betriebszeiten, in denen sich Gäste und Beschäftigte in dem Schwimmbad aufhalten, und Schließzeiten, in denen sich dort keine Personen mehr berechtigt befinden (auch keine Beschäftigten und kein Reinigungspersonal), zu unterscheiden.

13 Tätigkeitsbericht Datenschutz 2024, A II 3.

Bezogen auf die Betriebszeiten bewerteten wir u. a. die Videoüberwachung der Gänge vor den Spinden als unzulässig. Die zur Begründung angeführten Spindaufbrüche hat der Verantwortliche nicht konkretisiert. Im Rahmen der Interessenabwägung war u. a. zu berücksichtigen, dass die überwiegende Zahl der Gäste keinen Anlass zur Videoüberwachung gab. Im Badebereich war während der Betriebszeiten die Speicherung von Bilddaten unzulässig. Dort halten sich die Besucherinnen und Besucher im Rahmen der Freizeitgestaltung und regelmäßig nur in Badekleidung auf, darunter viele Kinder, deren Interessen nach der Datenschutz-Grundverordnung besonders schützenswert sind. Jedoch erachteten wir ein Echtzeit-Monitoring zur Unterstützung des Aufsichtspersonals als zulässig, soweit es auf schlecht einsehbare Bereiche begrenzt war und keine milderen Mittel zur Verfügung standen. Dabei galt es, die Beobachtung auf die Wasserflächen einschließlich des Beckenrandes zu beschränken. Wege sowie Liege- und Aufenthaltszonen, auch für die Gastronomie, waren von der Videoüberwachung auszunehmen. Dort halten sich die Badegäste typischerweise über längere Zeit auf, um sich zu unterhalten und zu speisen. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gäste.

Wo das Auge nicht hinreicht

Außerdem durften ständige Arbeitsplätze im Kassenbereich zum Schutz der personenbezogenen Daten der Beschäftigten während der Arbeitszeiten nicht durchgehend erfasst werden. Die Speicherung der Bilddaten war unzulässig, soweit die Speicherdauer 72 Stunden überschritt.

Außerhalb der Betriebszeiten des Schwimmbades standen einer Datenverarbeitung mittels Videoüberwachung, sei es durch Echtzeit-Monitoring oder Speicherung, keine datenschutzrechtlichen Bedenken entgegen.

Im Anschluss an die Beratung begann der Verantwortliche, die Ergebnisse sukzessive umzusetzen. Insbesondere wurden die Videokameras vor den Spinden und im Kassenbereich während der Betriebszeiten außer Betrieb genommen. Der Verantwortliche maskierte Wege, Aufenthalts- und Liegezonen sowie die Gastronomiefläche im Bad und begrenzte die Datenverarbeitung während der Betriebszeiten auf ein Echtzeit-Monitoring schwer einsehbarer Bereiche. Die

Speicherdauer für die während der Schließzeiten entstehenden Bilder reduzierte er auf ein zulässiges Maß.

Für die bis dahin stattgefundene unerlaubte Videoüberwachung hat die Landesbeauftragte den Verantwortlichen gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO verwarnt.

8 Kunst, die zum Mitmachen einlädt und Daten verarbeitet

Die Ordnungsbehörde einer Stadtverwaltung gab einen Vorgang zu einem Sprachassistenten, der im Vorgarten eines Hauses betrieben wurde und eine Lärmbelästigung verursacht hatte, an die Landesbeauftragte ab. Auch erreichte uns hierzu eine Beschwerde. Nach Anhörung des Verantwortlichen und Durchführung eines Vor-Ort-Termins stellten wir Folgendes fest:

Der Verantwortliche hatte auf seinem Grundstück in Hörweite des vorbeiführenden Gehwegs eine künstlerisch gestaltete Holzfigur aufgestellt und in diese einen digitalen Sprachassistenten eingebaut. Der Sprachassistent konnte auf Zuruf eines Signalworts sowie einer Anweisung beispielsweise Musik abspielen oder Auskünfte erteilen. Hierzu wurden die Stimmdaten der Passantinnen und Passanten unter Verwendung einer dauerhaft bestehenden Internetverbindung verarbeitet. Der Assistent konnte durch erneuten Zuruf des Signalworts deaktiviert werden. Neben der Holzfigur hatte der Verantwortliche ein Schild angebracht, auf dem er die grundsätzliche Funktionsweise des Sprachassistenten erklärte. Das Gerät ließ sich beim Vor-Ort-Termin sogar trotz herrschenden Baulärms ohne Weiteres auslösen.

Der Verantwortliche gab an, dass seine Installation Informations- und Bildungszwecken dienen sollte und sich insbesondere an interessierte Kinder und Jugendliche richtete. Der Beschwerdeführer wie auch Anwohnerinnen und Anwohner äußerten dagegen die Sorge, dass ihre auf dem Gehweg geführten Unterhaltungen unbeabsichtigt von dem Gerät mitgeschnitten und online – insbesondere zu Geschäftszwecken des Herstellers – weiterverarbeitet werden könnten.

Zunächst würdigten wir den künstlerischen Charakter der Holzfigur. Anschließend prüften wir, ob der Betrieb des Sprachassistenten integraler Teil einer künstlerischen Aussage und damit gemäß Artikel 85 Datenschutz-Grundverordnung (DS-GVO) sowie § 29 Absatz 1 und 3 Brandenburgisches Datenschutzgesetz der datenschutzrechtlichen Beurteilung weitgehend entzogen war. Im Ergebnis beschränkte sich der künstlerische Charakter auf die optische Gestaltung der Figur, ohne dass die Sprachfunktion hieran Anteil hatte. Der Sprach-

assistent musste deshalb allein anhand datenschutzrechtlicher Anforderungen bewertet werden.

Wir stellten fest, dass es für die Erhebung von Stimmdaten an einer Rechtsgrundlage fehlte. Dies galt sowohl für Personen, die bewusst mit dem Gerät interagierten, als auch für solche, deren Daten beiläufig aufgezeichnet wurden.

Hinsichtlich der erstgenannten Gruppe war problematisch, dass auch Kinder zur Interaktion mit dem Gerät animiert wurden. Zwar sind die beabsichtigten Bildungszwecke aus gesellschaftlicher Sicht ohne Weiteres zu billigen, die mit der Aufzeichnung verbundenen Eingriffe in die Privatsphäre erfordern jedoch grundsätzlich die elterliche Einwilligung. In den gegebenen Situationen war dies allerdings unrealistisch. Der Verantwortliche hatte eine Einwilligung auch gar nicht vorgesehen.

Selbst die Erhebung von Daten Erwachsener war in diesem Fall nicht rechtskonform möglich – unabhängig von der konkret gewählten Rechtsgrundlage. Dies lag daran, dass es an einer ausreichenden Betroffeneninformation gemäß Artikel 13 DS-GVO fehlte. Danach muss die betroffene Person bei der Datenerhebung über die Einzelheiten der Verarbeitung informiert werden. Über die genaue Datenverarbeitung durch den Hersteller des Sprachassistenten, insbesondere dessen Verarbeitungszwecke, hatte aber der Verantwortliche selbst keine Kenntnis. Er konnte somit auch keine Betroffeneninformationen formulieren.

Kunst hört mit

Noch gewichtiger waren unsere Bedenken hinsichtlich jener Personen, deren Stimmen beiläufig aufgezeichnet wurden. Zum einen war zu beachten, dass der Sprachassistent bereits vor Nennung des Signalworts die Umgebung abhörte und Daten verarbeitete, um den Befehl überhaupt zu erkennen. Zum anderen hatte der Vor-Ort-Termin ergeben, dass eine Auslösung des Sprachassistenten durch Nennung des Signalworts im Rahmen einer auf dem Gehweg geführten Alltagsunterhaltung erfolgen konnte. Es war also leicht möglich, dass die Stimmdaten betroffener Personen, die keine Interaktion mit dem Gerät wünschten und dessen Betrieb möglicherweise nicht einmal zur Kenntnis nehmen konnten, aufgezeichnet wurden.

Schließlich wies das Schild zwar darauf hin, die Interaktion durch erneute Nennung des Signalworts abzuschließen. Es war aber unwahrscheinlich, dass sich die Nutzerinnen und Nutzer hieran zuverlässig halten würden. Da das Gerät sich erst etwa eine halbe Minute nach Ende der letzten Nutzung von selbst abschaltete, wurde in der Zwischenzeit die Konversation auf dem Gehweg mit Sicherheit aufgezeichnet. Auch hier bestand die Gefahr der möglicherweise unbemerkten Betroffenheit von Passantinnen und Passanten, die lediglich eine Privatunterhaltung führten.

Der Verantwortliche konnte sich für die Verarbeitung der Stimmdaten auch in keinem Fall auf ein berechtigtes Interesse gemäß Artikel 6 Absatz 1 Buchstabe f DS-GVO stützen, da das Interesse der betroffenen Personen, ihre Daten nicht verarbeiten zu lassen, überwog. Dies galt insbesondere, weil sie im öffentlichen Raum vernünftigerweise nicht mit einer solchen Datenverarbeitung rechnen mussten. Es wäre auch nicht zumutbar gewesen, von ihnen zu verlangen, die Straßenseite zu wechseln, um Datenerhebungen einer Privatperson auszuweichen.

Da keine Rechtsgrundlage für die Aufzeichnung der Stimmdaten betroffener Personen bestand und auch kein tragfähiges Konzept für den datenschutzgerechten Betrieb ersichtlich war, untersagte die Landesbeauftragte dem Verantwortlichen gemäß Artikel 58 Absatz 2 Buchstabe f DS-GVO, den Sprachassistenten in einer Weise weiterzubetreiben, dass eine Auslösung vom Gehweg aus möglich ist. Die Landesbeauftragte befindet sich im Austausch mit der Stadt hinsichtlich des Vollzugs der Anordnung.

9 Bericht der Bußgeldstelle

9.1 Veröffentlichung von Sozialdaten in einem sozialen Netzwerk

Die App eines sozialen Netzwerks fordert ihre Nutzerinnen und Nutzer regelmäßig auf, aktuelle Bilder zum eigenen Standort bzw. zur gegenwärtig ausgeführten Tätigkeit anzufertigen und hochzuladen. Zum Zeitpunkt der Aufforderung waren auf den Monitoren am Arbeitsplatz einer Sozialamtsmitarbeiterin Schreiben geöffnet, die Angaben zum vollständigen Namen einer Leistungsempfängerin, ihrer Mitgliedschaft in einer Bedarfsgemeinschaft, der Art und Höhe der bezogenen Leistung sowie ihrem Wohnort in einem Seniorenheim enthielten. Die Mitarbeiterin erstellte ein Foto und veröffentlichte dieses per App. 20 Personen innerhalb des sozialen Netzwerks hatten die Möglichkeit, das Foto einschließlich der darauf abgebildeten Schreiben abzurufen. Sie wusste, dass für die Offenlegung der Angaben kein dienstlicher Anlass bestand und handelte wider die bei ihrer Einstellung unterzeichnete Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen. Außerdem ließ sie eine absolvierte Schulung zum datenschutzrechtlichen Basiswissen außer Acht.

Gemäß § 32 Absatz 1 Satz 1 Nummer 1, 5. und 7. Variante Brandenburgisches Datenschutzgesetz (BbgDSG) handelt ordnungswidrig, wer entgegen den Vorschriften der Datenschutz-Grundverordnung, dieses Gesetzes oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten personenbezogene Daten, die nicht offenkundig sind, übermittelt und zum Abruf bereithält. Gemäß § 32 Absatz 2 BbgDSG kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 50.000 Euro geahndet werden.

Bei den veröffentlichten Daten handelte es sich um Informationen, die sich jeweils auf eine identifizierte oder identifizierbare natürliche Person bezogen, und damit um personenbezogene Daten i. S. v. Artikel 4 Nummer 1 Datenschutz-Grundverordnung (DS-GVO). Darüber hinaus handelte es sich bei diesen Daten auch um Sozialdaten gemäß § 67 Absatz 2 Satz 1 Zehntes Buch Sozialgesetzbuch. Bestimmte personenbezogene Daten waren zudem der in Artikel 9 DS-GVO aufgeführten besonderen Kategorie der Gesundheitsdaten zuzuord-

nen, denn sie ließen auf eine gesundheitliche Beeinträchtigung der Leistungsempfängerin schließen.

Da keine Erlaubnisnorm die Übermittlung an und das Bereithalten der personenbezogenen Daten der Leistungsempfängerin zum Abruf über das soziale Netzwerk legitimierte, stellte dies einen Verstoß gegen Artikel 6 und 9 DS-GVO dar.

Wegen dieses Verstoßes setzten wir gegen die Sozialamtsmitarbeiterin eine Geldbuße im mittleren dreistelligen Bereich fest. Hierbei berücksichtigten wir insbesondere die besondere Schutzwürdigkeit der betroffenen Daten sowie die Anzahl der Personen, für die das Foto zum Abruf bereitstand. Zudem haben wir bei unserer Entscheidung einbezogen, dass der Verstoß geeignet war, das Vertrauen der Allgemeinheit in die Rechtmäßigkeit des Umgangs mit personenbezogenen Daten durch die damit befassten öffentlichen Stellen empfindlich zu beeinträchtigen. Auf der anderen Seite war zu berücksichtigen, dass die Mitarbeiterin sich geständig einließ und reumütig zeigte. Sie hat die Geldbuße akzeptiert.

9.2 Umfangreiche Videoüberwachung auf einem Campingplatz

Anlässlich einer anonymen Beschwerde über die Videoüberwachung auf einem Campingplatz hörten wir die Betreibergesellschaft im aufsichtsrechtlichen Verfahren an. Sie wirkte erst nach mehrmaliger Aufforderung zur Auskunftserteilung und allenfalls bruchstückhaft an der Sachverhaltsaufklärung mit. Insbesondere gab das Unternehmen an, dass eine Videoüberwachung stattfand, jedoch weder ein Auftragsverarbeitungsvertrag mit dem hinsichtlich der gespeicherten Videoaufnahmen zugriffsberechtigten externen IT-Dienstleister abgeschlossen noch ein Verzeichnis von Verarbeitungstätigkeiten erstellt worden war. Das aufgezeichnete Bildmaterial wurde auf einem Datenträger für 14 Tage aufbewahrt, um es zur Dokumentation von Unfällen oder Eigentumsdelikten zu einem späteren Zeitpunkt zu nutzen. Die Betreibergesellschaft wies in ihren Allgemeinen Geschäftsbedingungen aus, dass die Videoüberwachung zu diesen Zwecken stattfindet. Obwohl der Geschäftsführer uns im Rahmen eines persönlichen Beratungstermins zusicherte, sämtliche Videokameras zu deaktivieren, blieb die Übersendung diesbezüglicher Nachweise trotz wiederholter Nachfragen aus.

Im Rahmen einer späteren, unangekündigten Vor-Ort-Kontrolle stellten wir fest, dass entgegen der Angaben der Betreibergesellschaft sehr wohl eine Videoüberwachung stattfand. Drei Kameras erfassten anlasslos und flächendeckend die Arbeitsplätze der Beschäftigten während der Arbeits- bzw. Betriebszeiten an der Rezeption, im Innenbereich des Restaurants sowie in der Küche. Fünf Kameras beobachteten die Zufahrten zu dem Campingplatz, dem Rezeptionsbereich sowie dem Restaurant und zeigten so anlasslos, wer zu welchem Zeitpunkt die jeweiligen Bereiche betrat oder verließ. Weitere vier Kameras erfassten die Ess- und Aufenthaltsbereiche, in denen Gäste typischerweise über längere Zeit zur unbeeinträchtigten Kommunikation verweilten. Zwei Kameras waren zudem auf Stellplätze von Gästen gerichtet und filmten bis in die Vorzelte hinein.

Zelte im Visier

Die im Nachgang zu dieser Vor-Ort-Kontrolle abermals angeforderten Nachweise in Form eines Verzeichnisses der Verarbeitungstätigkeiten sowie eines Auftragsverarbeitungsvertrages mit dem IT-Dienstleister übermittelte uns die Betreibergesellschaft weiterhin nicht.

Daraufhin leiteten wir gegen die Betreibergesellschaft des Campingplatzes ein Bußgeldverfahren wegen des Verdachts der unrechtmäßigen Videoüberwachung sowie wegen der Verstöße gegen die Pflicht zur Führung eines Verzeichnisses aller Verarbeitungstätigkeiten und gegen die Pflicht zum Abschluss eines Auftragsverarbeitungsvertrages ein.

Die Videoüberwachung war von keinem der in Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) enthaltenen Erlaubnistatbestände gedeckt. Insbesondere lag keine Einwilligung der von der Videoüberwachung betroffenen Personen nach Artikel 6 Absatz 1 Buchstabe a DS-GVO vor. Keinesfalls konnte die bloße Kenntnisnahme des Hinweises auf die Videoüberwachung in den Allgemeinen Geschäftsbedingungen als Einwilligung gewertet werden. Die Videoüberwachung war auch nicht für die Wahrnehmung der berechtigten Interessen des Verantwortlichen oder eines Dritten gemäß Artikel 6 Absatz 1 Buchstabe f DS-GVO erforderlich. Die Betreibergesellschaft hatte es versäumt, die Zwecke der Videoüberwachung vor der Inbetriebnahme schriftlich für jede einzelne Videokamera festzuhalten. Auch bestand zum Zeitpunkt der Videoüberwachung weder eine tatsächliche Gefahr für Leib und Leben der Gäste und des Personals

noch drohten Eigentumsdelikte. Zudem standen der Betreibergesellschaft zur Verhütung von Unfällen oder Straftaten mildere, gleichgeeignete Alternativmaßnahmen zur Verfügung, wie die regelmäßige Anwesenheit einer ausreichenden Anzahl an Beschäftigten in den betroffenen Außenbereichen, die Sicherung wertvoller Gegenstände gegen Diebstahl sowie eine Zutrittskontrolle des Geländes. Die Videoüberwachung stellte eine schwerwiegende Beeinträchtigung des allgemeinen Persönlichkeitsrechts aller betroffenen Personen dar. Die Gäste des Campingplatzes sowie des Restaurants suchten die beobachteten Bereiche während ihres Urlaubs zum Zweck der ungezwungenen Freizeitgestaltung auf und konnten nicht erwarten, von Videokameras erfasst zu werden. Von der umfangreichen Überwachung waren auch Kinder betroffen, deren Interessen nach Artikel 6 Absatz 1 Buchstabe f DS-GVO besonders schützenswert sind. Für die von der Videoüberwachung erfassten Beschäftigten stellte sie einen schweren Eingriff in ihr Persönlichkeitsrecht dar, weil ihr Gesamtverhalten beobachtet, wiedergegeben und analysiert werden konnte. Dies erzeugte permanent Druck, sich anzupassen, um Nachteile zu vermeiden.

Da der Verantwortliche weder einen Auftragsverarbeitungsvertrag mit dem externen IT-Dienstleister abgeschlossen noch ein Verarbeitungsverzeichnis geführt hat, lagen zudem Verstöße gegen Artikel 28 und 30 DS-GVO vor.

Gegen die Betreibergesellschaft des Campingplatzes setzten wir drei Geldbußen fest, deren Summe im oberen vierstelligen Bereich lag. Hierbei berücksichtigten wir auf der einen Seite u. a. den Zeitraum der unzulässigen Videoüberwachung, die hohe Anzahl der davon betroffenen Personen sowie den Umstand, dass die Betreibergesellschaft falsche Angaben hinsichtlich der Deaktivierung der Kameras uns gegenüber machte. Trotz wiederholter Aufforderungen führte sie darüber hinaus kein Verarbeitungsverzeichnis und schloss keinen Auftragsverarbeitungsvertrag ab. Auf der anderen Seite war zu berücksichtigen, dass die Verstöße fahrlässig begangen wurden und dass zwei der Verstöße formaler Natur waren. Letzteres geht in der Regel mit weniger Risiken für die Rechte der von der Datenverarbeitung betroffenen Personen einher. Der Bußgeldbescheid ist noch nicht rechtskräftig.

9.3 Privatrecherche in polizeilicher Datenbank

Ein Polizist recherchierte in einer polizeilichen Datenbank nach Informationen zu drei Nachbarinnen und Nachbarn sowie zu seinem Hauswart. Der Beamte hatte Letzterem erzählt, dass er Halterabfragen zu Mieterinnen und Mietern der Wohnanlage durchgeführt und einen Ordner mit den daraus erlangten Informationen angelegt habe.

Aufgrund seiner beruflichen Verpflichtung auf das Datengeheimnis und der regelmäßigen Belehrungen zu Dienstanweisungen, die den Datenschutz und die Informationssicherheit betreffen, wusste er, dass ein solcher Zugriff auf polizeiliche Datenbanken nur gestattet ist, wenn die Erfüllung der polizeilichen Aufgaben dies erfordert. Dessen ungeachtet fragte er die Informationen aus rein privaten Motiven ab.

Gemäß § 32 Absatz 1 Satz 1 Nummer 2, 1. Variante Brandenburgisches Datenschutzgesetz handelt ordnungswidrig, wer entgegen der Datenschutz-Grundverordnung, dieses Gesetzes oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten personenbezogene Daten, die nicht offenkundig sind, abruft.

Nach § 39 Absatz 1 Satz 1 Brandenburgisches Polizeigesetz kann die Polizei 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. Für eine zulässige Datenverarbeitung muss ein dienstlicher Anlass vorliegen. Die Nutzung zu privaten Zwecken wie beispielsweise aus der Motivation heraus, Informationen über Personen aus dem privaten Umfeld zu erlangen, gehört nicht zur Aufgabenerfüllung der Polizei.

Gegen den Polizeibeamten setzten wir vier Geldbußen jeweils in mittlerer dreistelliger Höhe fest. Der Bußgeldbescheid ist noch nicht rechtskräftig.

III Anlasslose Prüfungen

1 Europaweit koordinierte Prüfung zum Recht auf Löschung

Der Europäische Datenschutzausschuss (EDSA) organisiert im Rahmen der Zusammenarbeit der Datenschutzaufsichtsbehörden seit 2022 jährlich koordinierte Prüfaktionen (Coordinated Enforcement Framework, CEF). Sie sollen u. a. die einheitliche Durchsetzung des Datenschutzrechts im Europäischen Wirtschaftsraum fördern.

Wie bereits im Vorjahr[14] beteiligten wir uns im Berichtszeitraum erneut an der Prüfaktion. Schwerpunktthema war das Recht auf Löschung (auch bekannt als „Recht auf Vergessenwerden“), das in Artikel 17 Datenschutz-Grundverordnung (DS-GVO) verankert und eines der am häufigsten ausgeübten Betroffenenrechte ist. Insgesamt nahmen 32 Datenschutzaufsichtsbehörden an der Prüfung teil, davon 7 aus Deutschland. Alle Behörden stimmten zunächst einen Fragebogen ab, der an die zu prüfenden Verantwortlichen versandt werden sollte. Ziel der Befragung war, einen Überblick über Herausforderungen und Probleme bei der Umsetzung des Rechts auf Löschung in der Praxis zu erhalten, aber auch bewährte Vorgehensweisen der Verantwortlichen kennenzulernen. Die teilnehmenden Aufsichtsbehörden konnten frei entscheiden, welche Verantwortlichen in ihrem Zuständigkeitsbereich sie mit Hilfe des Fragebogens prüfen. Anhand der Antworten erstellten sie zunächst nationale Berichte.[15] Diese bildeten wiederum Grundlage für den Abschlussbericht des EDSA.[16] Er greift nicht nur die Herausforderungen für Verantwortliche im Zusammenhang mit dem Recht auf Löschung auf, die in den Befragungen festgestellt wurden, sondern hebt auch posi-

14 Tätigkeitsbericht Datenschutz 2024, A III 1.

15 https://www.edpb.europa.eu/system/files/2026-02/edpb_cef-report_2025_right-to-erasure_annex_en.pdf

16 https://www.edpb.europa.eu/system/files/2026-02/edpb_cef-report_2025_right-to-erasure_en.pdf

tive Lösungsansätze hervor. Die Ergebnisse der Prüfung ermöglichen den Aufsichtsbehörden, den Bedarf an Empfehlungen und sonstigen Hilfestellungen für Verantwortliche zu bestimmen bzw. die Erstellung gemeinsamer Leitlinien in den Blick zu nehmen.

Für unsere Prüfung haben wir 10 größere Wohnungsunternehmen mit Sitz in Brandenburg ausgewählt. Dies geschah auch vor dem Hintergrund immer wieder auftretender entsprechender Beschwerden. Gerade bei Interessentinnen und Interessenten für Mietwohnungen ist das Recht auf Löschung ein wichtiges Instrument, um sicherzustellen, dass die Unternehmen die bei der Bewerbung für eine Wohnung angegebenen personenbezogenen Daten nicht weiterverarbeiten. Mithilfe des o. g. Fragebogens wollten wir insbesondere ermitteln, wie die Wohnungsunternehmen Löschanträge von betroffenen Personen handhaben. Neben den Prozessen zur Prüfung eines solchen Antrags nach Artikel 17 Absatz 1 DS-GVO interessierte uns auch, wie die Verantwortlichen mit Ausnahmen von der Löschpflicht nach Artikel 17 Absatz 3 DS-GVO umgehen und wie sie die allgemeinen Modalitäten zur Umsetzung von Betroffenenrechten aus Artikel 12 DS-GVO berücksichtigen. Schlussendlich müssen sie auch technisch in der Lage sein, entsprechende personenbezogene Daten in Dateisystemen oder Datenbanken zu finden und zu löschen. Dies ist gemäß Artikel 25 DS-GVO bereits bei der Planung einer Datenverarbeitung durch eine geeignete Gestaltung der IT-Systeme zu beachten.

Auf Löschung gut vorbereitet sein

Im Einzelnen ergaben sich bei den geprüften brandenburgischen Wohnungsunternehmen folgende Resultate:

- Wir stellten fest, dass die Verantwortlichen ihre Beschäftigten nicht immer ausreichend zu datenschutzrechtlichen Themen schulen und unterweisen. Zwar treffen viele der Unternehmen auf dem Papier Festlegungen, etwa zu Ansprechpersonen oder zum Umgang mit Auskunfts- und Löschanträgen. Jedoch besteht ohne regelmäßige Schulungen und Kontrollen die Gefahr, dass diese Vorgaben schrittweise immer weniger Beachtung finden, langfristig ausgehöhlt werden und die Praxis letztendlich erheblich von Geschäftsanweisungen abweicht.

- Artikel 12 Absatz 3 DS-GVO verpflichtet Verantwortliche, Löschanträge unverzüglich, spätestens aber innerhalb eines

Monats nach Eingang zu beantworten. Gerade für Beschäftigte, die regelmäßig Kontakt zu Mieterinnen und Mietern oder zu Wohnungssuchenden haben, sind deshalb spezielle Schulungen erforderlich. Sie müssen wissen, dass betroffene Personen ihre Rechte formlos gegenüber Verantwortlichen geltend machen können. Wenn solche Begehren fälschlicherweise nicht als datenschutzrechtliches Anliegen interpretiert werden und die unternehmensspezifischen Datenschutzprozesse gar nicht oder erst zu spät beginnen, liegt schnell ein Rechtsverstoß vor.

- Neben Schulungen stellen auch die regelmäßige Überprüfung und ggf. Anpassung der eigenen Prozesse des Verantwortlichen sicher, dass Löschbegehren betroffener Personen rechtskonform bearbeitet werden. Hier identifizierten wir bei der Prüfung ebenfalls Nachholbedarf. Das Argument einiger Unternehmen, Schulungen der Beschäftigten und Evaluierungen der Vorgehensweisen nähmen zu viel Zeit in Anspruch, überzeugt nicht. Gerade gut abgestimmte Prozesse und ein reibungsloser Ablauf bewirken Arbeitserleichterungen und Zeitersparnisse.

- Einige Verantwortliche benannten Schwierigkeiten, sämtliche personenbezogenen Daten zu einer Person aufzufinden, die eine Löschung begehrt – insbesondere dann, wenn die Daten über viele verschiedene Stellen bzw. IT-Systeme verstreut verarbeitet werden. Andere Verantwortliche zeigten jedoch, dass sich dieses Problem durch eine geeignete, umfassende Dokumentation lösen lässt. Insbesondere sollte das Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO genutzt werden, um den Überblick über die verschiedenen Verarbeitungen zu behalten und relevante Informationen – auch bei Löschanträgen – rasch zu ermitteln.

- Über die Hälfte der befragten Wohnungsunternehmen zeigte Missverständnisse bei der Interpretation von Artikel 17 DS-GVO i. V. m. anderen Rechtsvorschriften. Konkret erkannten viele Verantwortliche beispielsweise nicht, dass der Widerruf einer Einwilligung als Löschgrund gemäß Artikel 17 Absatz 1 Buchstabe b DS-GVO nur einschlägig sein kann, wenn die ursprüngliche Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a DS-GVO beruhte. Ähnliches stellten wir fest, wenn als Löschgrund ein Widerspruch gegen die Verarbeitung nach Artikel 17 Absatz 1 Buchstabe c DS-GVO genannt wurde. Ver-

antwortliche müssen zunächst prüfen, ob überhaupt ein Widerspruch gegen die Datenverarbeitung gemäß Artikel 21 DS-GVO möglich ist. Dies ist z. B. dann der Fall, wenn die ursprüngliche Verarbeitung auf das berechtigte Interesse des Verantwortlichen gemäß Artikel 6 Absatz 1 Buchstabe f DS-GVO gestützt wurde. Analog ist mit Ausnahmen von der Löschverpflichtung zu verfahren: Wohnungsunternehmen hatten Schwierigkeiten zu erkennen, dass eine Löschung z. B. nicht erfolgen darf, wenn die Weiterverarbeitung der Daten zur Wahrung einer rechtlichen Verpflichtung gemäß Artikel 6 Absatz 1 Buchstabe c DS-GVO erforderlich ist (etwa nach dem Geldwäschegesetz).

- Aus technischer Perspektive ergab unsere Prüfung Unsicherheiten bei der Löschung im Kontext von Datensicherungen (Backups). Grundsätzlich hat eine Datenlöschung unverzüglich zu erfolgen. Es kann allerdings sehr aufwendig sein, im Einklang mit der erforderlichen Integrität von Datensicherungen dort gespeicherte Daten selektiv zu löschen. Verantwortliche müssen insofern ihre Backup-Strategie überprüfen und ggf. insbesondere die Zyklen anpassen, in denen Datensicherungen überschrieben werden. Zusätzlich sind auch Szenarien zu berücksichtigen, in denen Datensicherungen zur Wiederherstellung von Daten (z. B. nach einem Defekt des Speichermediums) verwendet werden. Der Verantwortliche muss hierbei gewährleisten, dass zuvor gelöschte Daten durch das Einspielen der Datensicherung nicht wiederhergestellt werden. Da sich derartige Probleme aufgrund der komplexen IT-Infrastruktur nur schwer ad hoc lösen lassen, ist es essenziell, geeignete Konzepte im Sinne des Datenschutzes durch Technikgestaltung gemäß Artikel 25 DS-GVO bereits bei der Planung einer Datenverarbeitung und der IT-Systeme zu erstellen.

- Sollen nach der Löschung personenbezogener Daten die übrigen Daten etwa für statistische Auswertungen weiterverarbeitet werden, greifen manche Verantwortliche zum Mittel der Anonymisierung. Hier besteht die Herausforderung, dass die Löschung identifizierender Daten irreversibel sein muss, allerdings auch ein nicht zu unterschätzendes Restrisiko einer Re-Identifizierung von Personen bestehen kann. So lässt sich ein Personenbezug ggf. durch eine Verkettung der anonymen Daten mit anderen Datenquellen oder durch Einsatz neuer Technologien (evtl. auch erst zukünftig) wiederherstellen. Ver-

antwortliche müssen insoweit sowohl die Rechtmäßigkeit der Anonymisierung sicherstellen als auch eine geeignete Anonymisierungsmethode finden. Um sie bei diesem sehr komplexen Thema zu unterstützen, plant der Europäische Datenschutzausschuss die Veröffentlichung entsprechender Richtlinien.

- Überraschend war für uns, dass bei den geprüften Unternehmen die Anzahl der eingegangenen Löschanträge relativ niedrig war. Dies könnte bedeuten, dass sich die Wohnungssuchenden ihrer Rechte nicht vollumfänglich bewusst sind.

Zusammenfassend ist festzuhalten, dass wir mit den ausgewählten Wohnungsunternehmen in Brandenburg während der koordinierten Prüfung gut zusammengearbeitet haben. Es hat sich gezeigt, dass sie bei der Umsetzung des Rechts auf Löschung schon vieles richtig machen, aber auch vor einigen Herausforderungen stehen. Wir werden die verantwortlichen Stellen in Brandenburg deshalb weiter zu diesem Thema sensibilisieren und mit Hilfestellungen unterstützen. Hierbei werden wir die Erkenntnisse aus der europäischen Zusammenarbeit der Datenschutzaufsichtsbehörden einbeziehen.

2 Bezahlkarte für Geflüchtete

Menschen, die in Deutschland einen Asylantrag stellen, haben Anspruch auf Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG). Die Sozialämter der Landkreise und kreisfreien Städte zahlten die Leistungen an die betroffenen Personen bislang bar aus. Durch die Bezahlkarte wird die bisherige Praxis abgelöst. Hierbei handelt es sich um eine guthabenbasierte Karte mit Debit-Funktion, die wie eine Giro- oder Kreditkarte an entsprechenden Terminals zur Bezahlung von Waren und Dienstleistungen eingesetzt werden kann; Überweisungen und Lastschriften sind hingegen grundsätzlich nicht möglich. Nachdem ein Landkreis in Brandenburg eine eigene Bezahlkarte eingeführt hatte, erhielten wir Kenntnis davon, dass dieser Lastschriften und Überweisungen punktuell für bestimmte und zuvor geprüfte Zahlungsempfängerinnen und -empfänger durch die Führung einer Freigabeliste (sogenannte Whitelist) ermöglichen möchte. Soweit es sich hierbei um natürliche Personen handelt, geht dies mit der Verarbeitung personenbezogener Daten einher.

Wir führten deshalb eine Vor-Ort-Prüfung durch. Bei dieser konzentrierten wir uns auf die konkrete Umsetzung der Führung der Whitelist, insbesondere im Hinblick auf die Einhaltung der datenschutzrechtlichen Transparenzpflichten und die erforderliche Datenschutz-Folgenabschätzung.

Prüfungsgegenstand war hingegen nicht, ob die Führung einer Whitelist datenschutzrechtlich zulässig ist. Zwar haben wir dies noch im letzten Berichtszeitraum mangels einer datenschutzrechtlichen Rechtsgrundlage kritisch bewertet.[17] Zwischenzeitlich hat jedoch eine Arbeitsgruppe unter Beteiligung mehrerer Datenschutzaufsichtsbehörden einen bundeseinheitlichen Rahmen für die Bezahlkarte entwickelt. Danach kann die Führung einer Whitelist grundsätzlich auf die datenschutzrechtlichen Generalklauseln der Länder gestützt werden. Wir schließen uns im Sinne einer bundesweit einheitlichen Aufsichtspraxis und zur Gewährleistung einer rechtssiche-

17 Tätigkeitsbericht Datenschutz 2024, A V 5.3.

ren Anwendung dem Ergebnis der Arbeitsgruppe dem Grunde nach an.

Am Tag der Prüfung suchten wir mehrere Geflüchtetenunterkünfte, eine Außenstelle des Sozialamts sowie die zentrale Kreisverwaltung auf, sprachen mit den zuständigen Personen und nahmen Einsicht in Unterlagen und Systeme.

Damit eine geflüchtete Person Überweisungen vornehmen oder Lastschriftmandate einrichten kann, muss sie einen formlosen Antrag zur Freischaltung von Zahlungsempfängerinnen bzw. -empfängern bei ihrer Unterkunftsleitung oder den zuständigen Sozialarbeiterinnen bzw. -arbeitern stellen. Hierbei sind Name und IBAN der gewünschten Zahlungsempfängerin bzw. des Zahlungsempfängers anzugeben. Diese Informationen werden per E-Mail mit der Bitte um Freigabe an das zuständige Sozialamt übersandt. Alternativ können sich die Geflüchteten auch direkt dorthin wenden. Das Sozialamt prüft die Vertrauenswürdigkeit der Empfängerin bzw. des Empfängers und speichert den Namen und die IBAN bei positivem Ausgang auf einer Whitelist. Ab dem Zeitpunkt der Speicherung können alle Geflüchteten im Landkreis Überweisungen oder Lastschriftmandate für die freigegebenen Bankverbindungen einrichten. Personenbezogene Daten der Geflüchteten oder Gründe der Überweisung (Vertragsinformationen, Rechnungen o. Ä.) werden nicht verarbeitet. Der Landkreis stützt die Führung der Whitelist auf Artikel 6 Absatz 1 Buchstabe e und Absatz 3 Buchstabe b Datenschutz-Grundverordnung (DS-GVO) i. V. m. § 5 Brandenburgisches Datenschutzgesetz (BbgDSG).

Bei Einsicht in die Whitelist stellten wir fest, dass darin auch die Namen und IBAN von Privatpersonen verarbeitet werden, etwa jener, die eine Klassenkasse verwalten. Diese Datenverarbeitung sehen wir kritisch, da sie intransparent ist. Artikel 14 DS-GVO verpflichtet den Landkreis grundsätzlich dazu, die Privatpersonen über die Verarbeitung ihrer personenbezogenen Daten in der Whitelist zu informieren. Da dies nicht geschieht, haben die Privatpersonen keine Kenntnis hiervon und können daher ihre Betroffenenrechte nicht geltend machen.

Hinzu kommt, dass wir keine hinreichenden Konzepte für die Löschung feststellen konnten. Der datenschutzrechtliche Grundsatz der Speicherbegrenzung aus Artikel 5 Absatz 1 Buchstabe e DS-GVO

verpflichtet den Landkreis grundsätzlich dazu, personenbezogene Daten nur so lange zu speichern, wie es für die jeweiligen Verarbeitungszwecke erforderlich ist. Das hat zur Folge, dass der Landkreis in regelmäßigen Abständen zu überprüfen hat, ob die einzelnen personenbezogenen Daten der Zahlungsempfängerinnen bzw. -empfänger für die Führung der Whitelist weiterhin erforderlich sind. Ist dies nicht der Fall, sind die personenbezogenen Daten zu löschen. Kurze Löschfristen halten wir insbesondere bei den Klassenkassen für erforderlich, da sich Eltern in deren Verwaltung oft abwechseln.

Zudem stellten wir fest, dass alle Beschäftigten des Sozialamts Einblick in die Guthabenstände der einzelnen Bezahlkartenkonten haben. Der Landkreis gab an, dass dies zum einen der Anspruchsprüfung diene, da Geflüchtete vor dem Bezug von Asylbewerberleistungen zunächst eigenes Einkommen und Vermögen zu verbrauchen hätten. Zudem vertritt der Landkreis die Auffassung, er bleibe auch nach Auszahlung der Leistung Eigentümer des Geldes. Das Eigentum gehe erst dann auf die Geflüchteten über, wenn diese die Leistungen ausgegeben hätten. Als Eigentümer müsse er die genauen Beträge zu jeder Zeit einsehen können.

Die umfassende Möglichkeit der Einsichtnahme in den Guthabenstand der Karten aller Geflüchteten durch alle Beschäftigten des Sozialamts sehen wir ebenfalls kritisch, da die Voraussetzungen der einzig in Betracht kommenden Rechtsgrundlage des Artikels 6 Absatz 1 Buchstabe c und e sowie Absatz 3 Buchstabe b DS-GVO i. V. m. § 5 Absatz 1 BbgDSG nicht vorliegen. Hiernach ist eine Datenverarbeitung rechtmäßig, wenn diese zur Erfüllung einer rechtlichen Verpflichtung oder der Aufgaben des Landkreises erforderlich ist.

Die Aufgabe des Landkreises besteht im vorliegenden Fall insbesondere darin, Ansprüche Geflüchteter zu prüfen und gesetzlich bestimmte Leistungen an Leistungsberechtigte auszuzahlen. Hierfür bedarf es natürlich der Kenntnis anspruchsbegründender personenbezogener Daten. Dass jedoch alle Beschäftigten des Sozialamts zu jeder Zeit die Guthabenstände aller Karten einsehen können, ist unseres Erachtens für diese Aufgabenerfüllung nicht erforderlich. Diese Verfahrensweise stellt einen erheblichen Eingriff in die Rechte der Geflüchteten dar, baut einen Überwachungsdruck auf und kommt einem direkten Blick in das Portemonnaie gleich.

Zwar hat der Gesetzgeber durch das Einfügen des Wortes „Bezahlkarte“ in die §§ 2, 3 und 11 AsylbLG deutlich gemacht, dass die zuständigen Behörden Leistungen durch den Einsatz einer guthabenbasierten Karte mit Debit-Funktion erbringen dürfen. Weder der Gesetzestext noch die dazugehörigen Begründungen enthalten aber einen Hinweis darauf, dass Leistungsbehörden berechtigt sind, umfassend und anlasslos Einsicht in den Guthabenstand zu nehmen. Der Gesetzgeber sieht die Bezahlkarte als Ersatz der bisherigen Bargeldleistungen. Er hat hingegen nicht vorgesehen, dass die Bezahlkarte den Leistungsbehörden ein Mehr an Informationen über die Leistungsberechtigten verschafft. Eine vergleichbare Kontrollmöglichkeit bei der Ausgabe von Sachleistungen, Wertgutscheinen oder Bargeld existiert nicht. Dementsprechend würde durch eine Einsichtnahme-Funktion ein zusätzlicher Eingriff erfolgen, der geeignet ist, den betroffenen Leistungsberechtigten das Gefühl ständiger Überwachung zu vermitteln, der offenkundig nicht benötigt wird, um die Leistung als solche zu gewähren.

Auch wenn eine Leistungsbehörde im Einzelfall Kenntnis des Guthabenstands benötigt, weil etwa eine geflüchtete Person ihre Karte verloren hat und ein bestehendes Guthaben auf eine neue Karte übertragen werden soll, bedarf es keines technischen Direktzugriffs der Behörde, da es gleich wirksame und eingriffsärmere Alternativen gibt. So können die Geflüchteten über die Mitwirkungspflichten nach § 9 Absatz 3 AsylbLG i. V. m. §§ 60 und 61 Erstes Buch Sozialgesetzbuch (SGB I) dazu angehalten werden, der Behörde beispielsweise vor Ort an einem Behördencomputer die Einsicht in den Guthabenstand zu ermöglichen. Wird die Mitwirkung verweigert, entfällt grundsätzlich der Leistungsanspruch gemäß § 66 Absatz 1 SGB I. Es ist somit in aller Regel davon auszugehen, dass die Betroffenen bei drohendem Leistungsausfall einen hinreichenden Anreiz zur Mitwirkung haben.

Aus gleichem Grund halten wir die Einsichtnahme zur Anspruchsprüfung für nicht erforderlich. Zwar ist zutreffend, dass die Geflüchteten vor dem Leistungsbezug eigenes Einkommen und Vermögen von mehr als 200 Euro zu verbrauchen haben. Allerdings ist dies eine anspruchsbegründende Grundvoraussetzung, um überhaupt in den Bezug von Asylbewerberleistungen zu kommen. Erst wenn kein ausreichendes Einkommen oder Vermögen vorhanden ist, erhalten Geflüchtete eine Bezahlkarte, auf welche die Leistungen sodann geladen werden können. Die Prüfung ist somit grundsätzlich eine vor-

gelagerte Grundvoraussetzung des Auszahlungsanspruchs und des Erhalts einer Bezahlkarte.

Dies gilt auch dann, wenn die Prüfung auf ein Fortbestehen des Anspruchs gerichtet ist. Auch in diesem Fall unterliegen die Betroffenen einer Mitwirkungspflicht, sodass es einer so umfassenden Guthabenüberwachung nicht bedarf.

Soweit der Landkreis ausführt, zur Einsicht in den Guthabenstand berechtigt zu sein, da das Eigentum an dem Guthaben erst mit dessen Verbrauch auf die Geflüchteten übergeht, bestehen unsererseits erhebliche Zweifel. Da hierfür eine spezialgesetzliche Regelung, die einen entsprechenden Eigentumsübergangstatbestand regelt, weder vorgetragen noch ersichtlich ist, dürfte sich der Eigentumsübergang nach allgemeinen Regeln bestimmen. Der Eigentumsübergang würde sodann mit der Bereitstellung des Leistungsbetrags an die Geflüchteten erfolgen.

Schließlich stellten wir auch fest, dass der Landkreis keine Datenschutz-Folgenabschätzung gemäß Artikel 35 DS-GVO für das Verwaltungsportal der Bezahlkarte erstellt hatte. Zwar kam er in einer „Datenschutz-Risikoanalyse“ zu dem Ergebnis, dass keine Datenschutz-Folgenabschätzung erforderlich sei, allerdings wurde hierbei übersehen, dass eine solche für die umfangreiche Verarbeitung von Daten schutzbedürftiger Personen (insbesondere Asylsuchender) stets zu erfolgen hat.[18]

Zum Zeitpunkt des Redaktionsschlusses dieses Berichts war das Prüfverfahren noch nicht vollständig abgeschlossen.

18 Grundlage ist unsere Liste von Verarbeitungsvorgängen nach Artikel 35 Absatz 4 DS-GVO für den öffentlichen Bereich.

IV Ausgewählte Fälle

1 Georeferenzierte Fotos per App für den Antrag zur Agrarförderung

Im Berichtszeitraum lagen uns mehrere Beschwerden von Personen vor, die EU-Agrarfördermittel beantragt hatten. Sie wandten sich gegen die Aufforderung der kommunalen Landwirtschaftsbehörden, im Rahmen des so genannten Flächenmonitorings mit Hilfe georeferenzierter Fotos Nachweise über die landwirtschaftlichen Aktivitäten auf ihren Nutzflächen zu erbringen und hierfür eine vorgegebene App auf ihren Mobiltelefonen einzusetzen. Derartige Fotos sind Aufnahmen, die geografischen Koordinaten zugeordnet werden können. Die Beschwerdeführer äußerten Zweifel an den Rechtsgrundlagen für die Erhebung dieser Daten sowie Bedenken zu technischen Aspekten der über das Landwirtschaftsministerium bereitgestellten Software. Es sei u. a. nicht transparent, auf welche Geräteeinstellungen die App Zugriff habe und wie sie Daten und Zugriffe verwalte. Zum Zeitpunkt der Einreichung der Beschwerden war die App bereits im Einsatz, ohne dass uns die zuständigen Behörden im Vorfeld eingebunden hatten.

Wir wandten uns an das Ministerium und baten um eine Stellungnahme. Aus der Antwort ging hervor, dass die georeferenzierten Daten verarbeitet werden, um zu prüfen, ob die Anforderungen für den Erhalt von Direktzahlungen sowie Agrarumwelt- und Klimamaßnahmen erfüllt werden. Die App dient der Erstellung von Nachweisen im Rahmen der Kontrolle von flächenbezogenen Maßnahmen nach Förderprogrammen der Europäischen Union. Die Standortdaten und Fotos werden verwendet, um sicherzustellen, dass die tatsächlichen Bedingungen auf den Feldern mit den Angaben im Förderantrag übereinstimmen.

Weiter teilte das Ministerium mit, dass es sich bei den georeferenzierten Fotos nicht um personenbezogene Daten handele. Dieser Auffassung traten wir entgegen: Geodaten können einen Personenbezug aufweisen, wenn sie durch den direkten oder indirekten Bezug zu einem bestimmten Standort oder geografischen Gebiet auch

Einzelangaben über die persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren Person beinhalten. Genau dies ist hier der Fall, da die in Rede stehenden Fotos stets auf einen bestimmten Förderantrag sowie die antragstellende Person bezogen sind und landwirtschaftliche Aktivitäten auf den jeweils zugeordneten Flächen abbilden.

In Bezug auf die Rechtsgrundlagen der Datenerhebung verwies das Ministerium auf das Gesetz zur Durchführung des im Rahmen der Gemeinsamen Agrarpolitik einzuführenden Integrierten Verwaltungs- und Kontrollsystems (GAPInVeKoSG) und die zugehörige Verordnung zur Durchführung des Integrierten Verwaltungs- und Kontrollsystems (GAPInVeKoSV). Aus § 8 GAPInVeKoSG ergibt sich bei den flächen- und tierbezogenen EU-Agrarfördermaßnahmen eine weitgehende Mitwirkungspflicht für die Beantragung. Nach § 41 Absatz 2 GAPInVeKoSV sind Betriebsinhaberinnen bzw. -inhaber verpflichtet, im Rahmen von Kontrollen mitzuwirken und die geforderten Belege vorzulegen. Hierzu gehören auch georeferenzierte Fotos. § 32 Absatz 2 Nummer 2 GAPInVeKoSV ermöglicht der zuständigen Behörde die Überprüfung der Anträge anhand dieser Daten.

Agrarflächen im Fokus

Geeignete Alternativen zur Verwendung der App sah das Ministerium grundsätzlich nicht. Es verwies in diesem Zusammenhang darauf, dass durch die Software z. B. die Manipulation der georeferenzierten Fotos, die Bearbeitung der Aufnahmen oder die Fälschung von Standortdaten verhindert werden können. Die App unterstützt darüber hinaus die Antragstellerinnen und Antragsteller beim Fertigen der Fotos und übernimmt die Kommunikation mit den zuständigen kommunalen Landwirtschaftsbehörden (Übermitteln von Aufträgen zur Nachweiserbringung, Zuordnen der Fotos zu konkreten Anträgen und Hochladen der erstellten Nachweise). Dabei muss kein privates Mobiltelefon genutzt werden, die Nutzung geschäftlicher Endgeräte ist genauso möglich wie die Beauftragung Dritter mit der Erstellung der Fotos.

Sollte es einer antragstellenden Person im Einzelfall nicht möglich sein, ein georeferenziertes Bild über die App einzureichen, kann es nach Darstellung des Ministeriums dazu kommen, dass sich die Bewilligung verzögert, eine Vor-Ort-Kontrolle zur Aufklärung der Flächennutzung stattfindet oder die Fördervoraussetzung als nicht er-

füllt gilt und für die betroffene Parzelle ggf. keine Zahlung geleistet wird.

Aus technischer Sicht sollen mit der App keine zusätzlichen personenbezogenen Daten erhoben werden. Das Ministerium teilte mit, dass sie ausschließlich der Anfertigung und Übermittlung der georeferenzierten Nachweisfotos dient. In der Software angezeigte weitere Daten entstammen dem digital gestellten Förderantrag. Alle Datenübertragungen von bzw. zu Servern erfolgen stets in verschlüsselter Form. Zugriff auf die Daten sollen ausschließlich die jeweils zuständigen Prüferinnen und Prüfer haben, die auch den jeweiligen Antrag bearbeiten.

Bei der Entwicklung der App wurde laut Ministerium beachtet, dass nur diejenigen Berechtigungen auf dem mobilen Endgerät zur Bestätigung angefragt werden, die für die Funktionsfähigkeit unbedingt erforderlich sind. Verweigert die Nutzerin bzw. der Nutzer die Erteilung von solchen Berechtigungen, funktioniert die App nur eingeschränkt. Weitere Berechtigungen – auch hinsichtlich anderer Apps – werden nicht verwendet. Die App speichert die Daten in einem spezifischen Ordner; sensible Daten werden dort verschlüsselt abgelegt. Andere Apps haben keinen Zugriff auf diesen spezifischen Ordner, damit eine Manipulation der Nachweise möglichst ausgeschlossen ist. Umgekehrt greift die App auch nicht auf andere Speicherbereiche des Endgeräts zu.

Einen weiteren Aspekt aus den Beschwerden haben wir aufgenommen und an das Ministerium adressiert: Gegenwärtig ist das Herunterladen und Installieren der App nur aus den gängigen App Stores großer amerikanischer Anbieter möglich. Wir empfahlen, zusätzliche Installationsmöglichkeiten über freie, unabhängige Plattformen oder über die Webseiten des Ministeriums anzubieten. Nutzerinnen und Nutzer, die keine Spuren bei den großen Anbietern hinterlassen wollen, könnten so auf datenschutzgerechte Alternativen ausweichen. Dieser Empfehlung folgte das Ministerium bislang nicht.

Darüber hinaus haben wir das Ministerium hinsichtlich der Einbindung eines großen, international tätigen Internetkartendienstes in der App beraten. Durch die Kartendarstellung der jeweils in Bezug genommenen Agrarflächen sollten die Nutzerinnen und Nutzer der App besser unterstützt werden. Wir legten Wert darauf, dass die Einbindung dieses Kartendienstes optional ist und stets der vorheri-

gen ausdrücklichen Zustimmung der Nutzerin bzw. des Nutzers bedarf. Zudem sollte im Zuge der Einholung dieser Zustimmung auf die Datenschutzerklärung des Kartendienstes verwiesen werden. Das Ministerium folgte diesen Empfehlungen.

Im Ergebnis konnten die in den Beschwerden geäußerten Bedenken nach umfangreicher Korrespondenz und mündlichen Erörterungen mit dem Ministerium weitgehend ausgeräumt werden. Wir hätten es jedoch bevorzugt, bereits im Vorfeld von den zuständigen Stellen bei den grundsätzlichen Fragen einbezogen zu werden. Letztlich helfen die Gewährleistung umfassender Transparenz, die Berücksichtigung der Sorgen betroffener Personen sowie die Beachtung der datenschutzrechtlichen und technischen Anforderungen auch, die Akzeptanz digitaler Lösungen zu sichern – ein bei der Verwaltungsmodernisierung und -digitalisierung nicht zu unterschätzender Vorteil.

2 Veröffentlichung privat angefertigter Mitschriften aus einer Gemeindevertretung

Im Berichtsjahr erreichte uns die Anfrage eines Vereins, der eine Fraktion in einer Gemeindevertretung stellte. Er bat um Auskunft, ob, in welchem Umfang und unter welchen Bedingungen die Anlage eines öffentlich zugänglichen „Online-Archivs“ selbstgefertigter Mitschriften von Sitzungen der Gemeindevertretung in personenbezogener Form datenschutzrechtlich zulässig sei. Zugleich beschwerte sich ein betroffener Gemeindevertreter über dieses bereits umgesetzte Vorhaben. Er sah sich in seinen Datenschutzrechten verletzt.

Zunächst ist anzumerken, dass die Gemeinden selbst gemäß § 42 Absatz 1 Brandenburgische Kommunalverfassung (BbgKVerf) die Aufgabe haben, von allen Sitzungen der Gemeindevertretung Niederschriften zu fertigen. Ihr Mindestinhalt umfasst u. a. die Namen der Teilnehmerinnen und Teilnehmer, den vollständigen Wortlaut der Anträge und Beschlüsse sowie die Ergebnisse der Wahlen und Abstimmungen, nicht aber einzelne Wortbeiträge. Es steht den Gemeinden jedoch frei, über den Mindestinhalt hinaus Wortbeiträge zu protokollieren und – soweit die Betroffenen aktive Teilnehmerinnen bzw. Teilnehmer an den Sitzungen im Sinne des § 30 Absatz 3 Satz 1 BbgKVerf sind – diese Beiträge auch in personenbezogener Form zu veröffentlichen. Das ist gängige und von uns grundsätzlich nicht in Frage gestellte Praxis. Aufgrund ihrer Pflicht zur Unterrichtung der Einwohnerinnen und Einwohner in wichtigen Gemeindeangelegenheiten gemäß § 13 Absatz 1 BbgKVerf veröffentlichen die Gemeinden die Niederschriften des öffentlichen Teils der Sitzung nach deren Genehmigung in aller Regel aktiv im Internet. Adressatin der Erlaubnisnorm des § 42 Absatz 1 BbgKVerf ist allerdings ausschließlich die Gemeinde selbst; ein Verein kann sich darauf nicht stützen.

Gemäß Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) darf ein Verein personenbezogene Daten aber verarbeiten, wenn dies zur Wahrung seiner berechtigten Interessen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Folgende Voraussetzungen sahen wir in dem beschriebenen Fall als erfüllt an:

- Die Herstellung von Transparenz über politische Vorgänge in einer Gemeinde kann durchaus dem satzungsmäßigen Zweck eines Vereins entsprechen und Ausdruck der verfassungsrechtlich gewünschten Sichtbarkeit der Kommunalpolitik im Alltag sein. Sie ist ein im demokratischen Rechtsstaat anerkanntes Anliegen. Auch die Veröffentlichung von namentlichen Wortbeiträgen kann zu diesem Zweck legitim sein. Ein berechtigtes Interesse des Vereins an der Datenverarbeitung, die der Erstellung und Veröffentlichung der Mitschriften zugrunde liegt, ist deshalb durchaus möglich.

- Aus Gründen der Erforderlichkeit und Verhältnismäßigkeit darf die Veröffentlichung personenbezogener Daten dem Umfang nach jedoch nicht über dasjenige hinausgehen, was die Gemeinde selbst in Erfüllung ihrer Informationsaufgaben publiziert.

- Im Ergebnis der Abwägung des berechtigten Interesses des Vereins mit dem der Gemeindevertreterinnen bzw. -vertreter, dass deren personenbezogenen Daten nicht (zusätzlich) erhoben und veröffentlicht werden, haben es die Betroffenen in der Regel hinzunehmen, dass ihre öffentliche Tätigkeit, die ohnehin von allen Anwesenden bei öffentlichen Sitzungen der Gemeindevertretung zur Kenntnis genommen werden kann, auch weiteren Kreisen zugänglich wird.

Unabhängig vom konkreten Beschwerdefall bestehen weitere wesentliche Bedingungen für die Zulässigkeit der Veröffentlichung von Mitschriften. Diese Regeln gelten immer auch für die Gemeinde selbst:

- Eine Berichterstattung aus der nicht öffentlichen Sitzung oder aus Sitzungspausen in Form der Protokollveröffentlichung ist einem Verein genauso wenig erlaubt wie der Gemeinde selbst.

- Einwohnerinnen bzw. Einwohner, die sich in einer Einwohnerfragestunde zu Wort gemeldet haben, dürfen namentlich nicht mit ihren Redebeiträgen in Verbindung gebracht werden, es sei denn, sie haben hierfür ihre Einwilligung erteilt.

- Sonstige personenbezogene Daten Dritter, die in der Sitzung erwähnt werden, dürfen nur nach strenger Prüfung veröffentlicht werden. Den Mitschriften eines Vereins dürfen zudem keine personenbezogenen Daten Dritter – z. B. in eigenen Anmerkungen – hinzugefügt werden.

- Die Mitschriften einschließlich der darin enthaltenen Bezüge zu natürlichen Personen dürfen nur veröffentlicht werden, soweit sie in Bezug auf die Vorgänge in der Gemeindevertretung richtige Tatsachenbehauptungen enthalten.

- Der Verantwortliche muss anhand der offiziell von der Gemeinde veröffentlichten Niederschriften überprüfen, ob die von ihm selbst veröffentlichten Mitschriften in Bezug auf personenbezogene Daten davon abweichen. Etwaige Diskrepanzen sind unverzüglich zugunsten der offiziellen Niederschrift zu beheben.

- Ein berechtigtes Interesse zur Publikation privater Mitschriften aus Sitzungen kommunaler Vertretungen währt nur so lange wie die Gemeinde selbst die offiziellen Niederschriften veröffentlicht. Entfernt die Gemeinde die Niederschriften aus ihrem Internetangebot, muss auch die Publikation der Mitschrift rückgängig gemacht werden.

- Angemessene technisch-organisatorische Maßnahmen gemäß Artikel 32 DS-GVO i. V. m Artikel 5 Absatz 1 Buchstabe f DS-GVO sind zu ergreifen, um die Integrität der Daten und die sonstige Datensicherheit zu gewährleisten.

Im Ergebnis hatten wir keine grundsätzlichen Bedenken gegen die mit dem Erstellen und Veröffentlichen des „Online-Archivs“ verbundene Datenverarbeitung. Ein berechtigtes Interesse haben wir bejaht. Insbesondere hielten wir die Publikation der Mitschriften deshalb für unproblematisch, weil die Gemeinde selbst nahezu vollständige Niederschriften inklusive personenbezogener Wortbeiträge veröffentlicht hatte. Anhaltspunkte dafür, dass das Geheimhaltungsinteresse der betroffenen Mandatsträgerinnen und Mandatsträger das Interesse des Vereins an der Veröffentlichung überwogen hätte, vermochten wir nicht zu erkennen. Wir haben die Beschwerde des betroffenen Gemeindevertreters deshalb abgewiesen.

Schließlich haben wir den verantwortlichen Verein verpflichtet, die weiteren, o. g. Bedingungen für eine Veröffentlichung seiner Mitschriften aus den Gemeindevertretersitzungen in seiner künftigen Veröffentlichungspraxis einzuhalten. Der Verein sagte dies zu; eine Überprüfung behält sich die Landesbeauftragte vor.

3 Selbstbestimmung bei der Übermittlung von Meldedaten?

Im Berichtszeitraum erreichte uns eine Vielzahl von Beschwerden, in denen sich Bürgerinnen und Bürger davon überrascht zeigten, von unerwarteter Stelle Post zu erhalten. Ob von Parteien, der Bundeswehr oder dem Beitragsservice der öffentlich-rechtlichen Rundfunkanstalten – oft sind Beschwerdeführerinnen und Beschwerdeführer der Ansicht, dass u. a. Adressdaten den Absenderinnen und Absendern eigentlich nicht bekannt sein dürften. Tatsächlich aber sind die Meldebehörden in vielen Fällen berechtigt oder sogar verpflichtet, Meldedaten an andere Behörden und sonstige Dritte zu übermitteln. Betroffene Personen haben lediglich in bestimmten Konstellationen die Möglichkeit, diese Weitergabe zu verhindern.

Es ist grundsätzlich Aufgabe der Meldebehörden, auf Basis der geltenden Rechtsvorschriften anderen Behörden und nicht öffentlichen Stellen Daten aus dem Melderegister zur Verfügung zu stellen. Öffentliche Stellen erhalten gemäß § 34 Bundesmeldegesetz (BMG) diese Daten, soweit sie zur Erfüllung ihrer Aufgaben erforderlich sind. Sie bekommen Meldedaten auch dann, wenn ihre Übermittlung vom Gesetzgeber vorgesehen ist (z. B. im Falle von Übermittlungen nach den Meldedatenübermittlungsverordnungen von Bund und Land). Private Stellen erhalten die Daten in der Regel im Rahmen von Melderegisterauskünften gemäß §§ 44 ff. BMG. Auf Antrag werden politischen Parteien vor Wahlen gemäß § 50 Absatz 1 BMG Datensätze zur Durchführung ihres Wahlkampfes zur Verfügung gestellt.

Um derartige Auskünftige zu verhindern, stehen betroffenen Personen je nach Rechtsgrundlage unterschiedliche Möglichkeiten zur Verfügung. Den weitestgehenden Schutz vor der Übermittlung von Meldedaten an nicht öffentliche Stellen bietet die Auskunftssperre gemäß § 51 Absatz 1 Satz 1 BMG. Soweit Tatsachen vorliegen, die eine Gefahr für besonders wichtige persönliche Rechtsgüter im Falle einer Melderegisterauskunft verursachen können, besteht Anspruch auf die Eintragung einer Auskunftssperre. Eine solche kann nach dem Wortlaut des Gesetzes grundsätzlich nur Melderegisterauskünfte, also Auskünfte an nicht öffentliche Stellen, verhindern. Eine praktisch bedeutsame Ausnahme findet sich in § 8 Absatz 3 der Verordnung über regelmäßige Datenübermittlungen der Meldebe-

hörden (MeldDÜV) des Landes Brandenburg, nach der bei Vorliegen einer Auskunftssperre keine Meldedaten an den Beitragsservice der öffentlich-rechtlichen Rundfunkanstalten übermittelt werden.

Einen eingeschränkteren Schutz gegen Melderegisterauskünfte bietet der bedingte Sperrvermerk gemäß § 52 BMG. Dieser wird im Fall bestimmter Pflege-, Behandlungs- und Schutzeinrichtungen eingetragen. Er bewirkt, dass Auskunft zu den Meldedaten dort wohnhafter Personen nur erteilt werden kann, wenn eine Beeinträchtigung schutzwürdiger Interessen ausgeschlossen und die betroffene Person hierzu angehört worden ist. Insbesondere in Wahljahren bedeutsam ist zudem die nicht begründungsbedürftige Möglichkeit nach § 50 Absatz 5 i. V. m. Absatz 1 BMG, der Weitergabe der Meldedaten an politische Parteien zum Zweck der Wahlwerbung zu widersprechen.

Eigene Entscheidung – nicht immer

Die Übermittlung von Meldedaten an andere öffentliche Stellen durch einen Widerspruch zu verhindern, ist nur in besonderen Fällen möglich. In den an uns gerichteten Anfragen und Beschwerden kam das Widerspruchsrecht gegen die Datenübermittlung an das Bundesamt für das Personalmanagement der Bundeswehr gemäß § 36 Absatz 2 BMG i. V. m. § 58c Soldatengesetz (SG) zur Übersendung von Informationsmaterial besonders häufig zur Sprache.[19] Seltener thematisiert wurde der Widerspruch gemäß § 50 Absatz 5 BMG bzw. § 14 Absatz 3 MeldDÜV gegen die Weitergabe von Angaben zu Alters- und Ehejubiläen zum Zweck der Ehrung.

Wir waren im Berichtszeitraum mit zahlreichen Missverständnissen in Bezug auf Widerspruchsrechte gegen Meldedatenübermittlungen konfrontiert. Einige Bürgerinnen und Bürger hatten – ohne dass die Voraussetzungen des § 51 BMG gegeben waren und teils ganz ohne Begründung – der Weitergabe von Meldedaten insgesamt bei

19 Das Recht, der Datenübermittlung zwecks Zusendung von Informationsmaterial der Bundeswehr zu widersprechen (früher § 36 Absatz 2 Bundesmeldegesetz), wurde durch Artikel 12 Nummer 2 i. V. m. Artikel 20 Absatz 1 des Gesetzes zur Modernisierung des Wehrdienstes vom 22. Dezember 2025 (BGBl. 2025 I Nr. 370) mit Wirkung zum 1. Januar 2026 gestrichen.

der Meldebehörde widersprochen. Formulare hierfür kursierten im Internet. Dies betraf insbesondere Vorgänge im Zusammenhang mit dem öffentlich-rechtlichen Rundfunk.

In diesen Fällen wiesen wir darauf hin, dass die Meldebehörden gemäß § 8 BMG bei der Datenweitergabe zwar ihr bekannte schutzwürdige Interessen betroffener Personen beachten müssen, die betroffene Person selbst jedoch die Übermittlung ihrer Meldedaten nur verhindern kann, wenn das Gesetz ein Widerspruchsrecht ausdrücklich vorsieht. Erst recht sind Übermittlungen von Meldedaten nicht einwilligungsbedürftig, da stets eine gesetzliche Grundlage nach Artikel 6 Absatz 1 Buchstabe e und Absatz 3 Datenschutz-Grundverordnung (DS-GVO) besteht.

Darüber hinaus wandte sich ein Elternteil eines vor der Volljährigkeit stehenden jungen Mannes an uns, dessen Meldedaten gemäß § 58c SG an die Bundeswehr übermittelt und von ihr genutzt worden waren. Für die Familie war eine Auskunftssperre nach § 51 BMG eingetragen. Sie war der Auffassung, die Übermittlung hätte nicht stattfinden dürfen. Wir wiesen darauf hin, dass § 51 BMG sich nahezu ausschließlich auf Melderegisterauskünfte auswirkt und daher grundsätzlich nicht geeignet ist, Datenübermittlungen zwischen Behörden zu unterbinden. Aus dem Sachverhalt ergab sich, dass offenbar aufgrund fehlender Kenntnis kein Widerspruch nach § 36 Absatz 2 BMG eingelegt worden war. Die Datenübermittlung war damit rechtmäßig.

Im Berichtszeitraum erreichten uns zudem anlässlich der Oberbürgermeisterab- bzw. -neuwahl in der Landeshauptstadt Potsdam Beschwerden von Bürgerinnen und Bürgern, die von einer Partei angeschrieben worden waren und aufgrund der anliegenden Information nach Artikel 14 Absatz 2 Buchstabe f DS-GVO die Meldebehörde der Landeshauptstadt als Quelle ihrer Adressdaten ausgemacht hatten. Auch hier war die Widerspruchsmöglichkeit nach § 50 Absatz 5 BMG stets unbekannt und damit ungenutzt geblieben. Wir hatten in keinem Fall Anlass, von einer rechtswidrigen Datenübermittlung auszugehen, und informierten die Beschwerdeführerinnen bzw. Beschwerdeführer jeweils über die Rechtslage.

Aufgabe der Gemeinden ist, auf die Möglichkeiten des Widerspruchs gegen Meldedatenübermittlungen sowohl bei der Wohnsitzanmeldung als auch einmal jährlich durch ortsübliche Bekanntmachung

hinzuweisen. Dies erfolgt im gedruckten Amtsblatt oder online. Möglicherweise könnten auch die Gemeinden diese Informationen künftig noch besser sichtbar platzieren, um die Bürgerinnen und Bürger dabei zu unterstützen, ihre Selbstbestimmungsrechte frühzeitig auszuüben.

4 Gesundheitsamt erhebt Daten von Kita-Kindern

Das Gesundheitsamt eines Landkreises ignorierte gleich in zwei Fällen, dass die Verarbeitung personenbezogener Daten von Kita-Kindern nur mit Einwilligung der Sorgeberechtigten erlaubt war. So hinterfragte eine Mutter die Praxis, dass das Personal der Einrichtung ohne ihr Wissen und auf Anweisung des Gesundheitsamts von ihrem Kind eine Stuhlprobe entnahm. Darüber hinaus erhielten wir eine Meldung gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO): Eine Stadt als Trägerin mehrerer Kindertagesstätten teilte uns darin mit, dass diese ebenfalls nach Aufforderung durch den Landkreis personenbezogene Daten der dort betreuten Kinder an das Gesundheitsamt übermittelt hatten, um kinderärztliche Untersuchungen vorzunehmen.

Häufungen von Magen-Darm-Erkrankungen sind in Kitas keine Seltenheit. In der irrigen Annahme, dass §§ 16 und 34 Infektionsschutzgesetz (IfSG) es erlauben, wies das Gesundheitsamt die Kindertagesstätten an, bei den Kleinen Stuhlproben zu nehmen und zur Auswertung an die Behörde zu senden. Es verkannte dabei, dass sich gemäß § 16 Absatz 2 IfSG die Berechtigung zur Entnahme von Proben ausschließlich auf Räume und Gegenstände bezieht. Die Entnahme von körperlichem Material ist nicht durch die Vorschrift gedeckt.

Geruchsintensive Zusatzaufgabe für Kitapersonal?

Im Ergebnis hat das Gesundheitsamt die Unzulässigkeit der Maßnahme eingeräumt und die Einrichtungen in seiner Zuständigkeit über die Rechtslage informiert. Die Bereitstellung des Untersuchungsmaterials soll fortan ausschließlich durch die Sorgeberechtigten erfolgen.

In dem o. g. zweiten Fall verlangte das Gesundheitsamt wenige Monate später von den Kindertagesstätten für die Planung und Durchführung kinderärztlicher Untersuchungen die Namen und Geburtsdaten der dort betreuten Kinder, ohne die Einwilligung der Sorgeberechtigten einzuholen. Zum Zeitpunkt der Meldung nach Artikel 33 DS-GVO waren bereits sieben städtische Kitas dieser Forderung nachgekommen. Als Rechtsgrundlage für die Datenerhebung

berief sich das Gesundheitsamt auf § 6 Brandenburgisches Gesundheitsdienstgesetz und § 11 Kindertagesstättengesetz, welche eine solche Befugnis jedoch nicht enthalten. Stattdessen bedarf es hierfür der Einwilligung der Sorgeberechtigten. Bei den Datenübermittlungen handelte es sich somit um Datenschutzverletzungen.

Wir wiesen das Gesundheitsamt auf die Rechtswidrigkeit seiner Datenerhebung hin und verlangten, alle Einrichtungen entsprechend zu informieren. Darüber hinaus forderten wir es zur Löschung der bereits erhaltenen Daten auf. Das Gesundheitsamt bestätigte, so verfahren zu sein. Im Ergebnis konnten wir außerdem erreichen, dass künftig alle Eltern unmittelbar durch den Landkreis angeschrieben und befragt werden, ob sie der Untersuchung zustimmen. Die hierfür erforderlichen Daten erhält der Landkreis gemäß § 6 Absatz 2 Satz 3 Brandenburgisches Gesundheitsdienstgesetz von den Meldebehörden.

Um sicherzustellen, dass auch die Gesundheitsämter anderer Landkreise in den beschriebenen Angelegenheiten datenschutzkonform verfahren, informierten wir das Gesundheitsministerium darüber. Im Fall der Stuhlprobenentnahmen ließ es allen brandenburgischen Amtsärztinnen und Amtsärzten ein von der Landesbeauftragten erstelltes Aufklärungsschreiben zukommen. Zur Problematik der Datenübermittlung für kinderärztliche Untersuchungen klärte das Ministerium mit einem Rundschreiben über die Rechtslage auf. Wir begrüßen es sehr, dass hierdurch auf eine Einhaltung datenschutzrechtlicher Regelungen in allen Gesundheitsämtern hingewirkt wurde.

5 Ausweiskopien des Pflegepersonals für das Gesundheitsamt

Ein Anbieter von Pflegeleistungen erkundigte sich, ob das Gesundheitsamt eines Landkreises berechtigt sei, sich Personalausweiskopien der einzelnen Beschäftigten vorlegen zu lassen. Diese Forderung hatte die Behörde damit begründet, dass der Dienstleister einerseits nach § 12 Absatz 2 Brandenburgisches Gesundheitsdienstgesetz (BbgGDG) verpflichtet sei, dem Gesundheitsamt die Ausübung bestimmter Berufe im Gesundheitswesen anzuzeigen. Außerdem verwies sie auf ihre eigene Befugnis nach § 13 Absatz 1 Nummer 4 BbgGDG, im Rahmen ihrer Überwachungsaufgaben Auskünfte und Unterlagen einzufordern. Das Unternehmen hingegen vertrat die Auffassung, eine Übermittlung von Ausweiskopien verstoße gegen § 20 Absatz 2 Satz 2 Personalausweisgesetz. Danach dürfen andere Personen als die Inhaberin oder der Inhaber des Personalausweises Kopien hiervon nicht an Dritte weitergeben.

Für uns war bereits nicht nachvollziehbar, weshalb das Gesundheitsamt zu Überwachungszwecken die Kopien der Personalausweise überhaupt benötigte. Schließlich dient ein Personalausweis ausschließlich dem Nachweis der Identität einer Person; diese Aufgabe stand hier gar nicht in Rede. Darüber hinaus fehlte eine Rechtsgrundlage, nach der die Kopien einerseits vorzulegen gewesen wären und die Daten andererseits hätten verarbeitet werden dürfen. Die von der Behörde angeführten Vorschriften des Brandenburgischen Gesundheitsdienstgesetzes enthalten eine solche konkrete Verpflichtung bzw. Befugnis nämlich gerade nicht.

Auch aus der allgemeinen Anzeigepflicht für die Inbetriebnahme einer unterstützenden Wohnform gemäß § 7 Absatz 2 Brandenburgisches Pflege- und Betreuungswohngesetz (BbgPBWoG) oder aus den zusätzlichen Anzeigepflichten gemäß § 12 Absatz 1 und 2 BbgPBWoG ergibt sich keine Verpflichtung zur Vorlage von Ausweiskopien der Beschäftigten von Pflegeeinrichtungen. Nach § 12 Absatz 2 BbgPBWoG kann zudem nur die zuständige Behörde weitere Angaben verlangen, soweit sie zu ihrer zweckgerichteten Aufgabenerfüllung erforderlich sind. Zuständig ist hier aber das Landesamt für Soziales und Versorgung und nicht das Gesundheitsamt des jeweiligen Landkreises.

Wir haben dem Anbieter von Pflegeleistungen diese mit dem Gesundheitsministerium abgestimmte Rechtsauffassung mitgeteilt. Zudem hat das Ministerium alle Amtsärztinnen und Amtsärzte auf die Rechtslage aufmerksam gemacht und klargestellt, dass Gesundheitsämter keine Kopien von Personalausweisen des Pflegepersonals verlangen dürfen.

6 Veröffentlichung von Beschäftigtendaten in einer Kita-App

In den vergangenen Jahren erreichten uns immer häufiger Anfragen, Beschwerden sowie Meldungen zu Datenschutzverletzungen, die sich auf die Nutzung von Kita-Apps bezogen. Derartige Programme können über unterschiedliche Funktionen verfügen. Sie reichen vom einfachen Informationsaustausch zwischen Kita, Träger und Eltern über die Dokumentation des Kita-Alltags (z. B. mit Fotos und Videos) bis hin zur Verwaltung sensibler Daten der Kinder, die z. B. ihre Gesundheit oder Entwicklung betreffen. In den Anfragen an uns ging es oft darum, welche Apps überhaupt genutzt, welche Daten dort verarbeitet und unter welchen Bedingungen welche Daten veröffentlicht werden dürfen.

Ein gravierender Fall der Verletzung datenschutzrechtlicher Vorschriften in diesem Kontext wurde uns durch eine Meldung nach Artikel 33 Datenschutz-Grundverordnung (DS-GVO) bekannt, die ein Kita-Träger bei uns abgab. Die Leitung einer Kita hatte Daten von Beschäftigten in einer Kita-App für alle Eltern und alle anderen Mitarbeiterinnen und Mitarbeiter veröffentlicht. Darin enthalten war z. B. die Information, dass eine namentlich genannte Erzieherin schwanger ist und demnächst in den Mutterschutz gehen wird, eine andere namentlich genannte Erzieherin aus dem Mutterschutz zurückkehrt und einer dritten namentlich genannten Erzieherin vom Träger gekündigt wurde. Nachdem letztere sich über die Preisgabe der Information an alle Nutzerinnen und Nutzer der App bei der Kita-Leitung beschwert hatte, änderte diese die Veröffentlichung zwar ab, verzichtete jedoch lediglich darauf, den Träger als Initiator der Kündigung zu benennen. Die Tatsache an sich war weiterhin zu lesen. Erst als die Personalleitung davon erfuhr, entfernte sie sämtliche Daten, die Beschäftigte betrafen, aus der App und veranlasste die o. g. Meldung.

Die Aufarbeitung des Vorfalls seitens des Trägers führte nicht nur zu arbeitsrechtlichen Konsequenzen für die Kita-Leitung. Erneut sensibilisierte er alle Mitarbeiterinnen und Mitarbeiter für Datenschutzfragen durch eine entsprechende Schulung. Darüber hinaus legte er fest, dass alle in der Kita-App zu veröffentlichenden Inhalte zuvor durch die Geschäftsführung freizugeben sind. Wegen des unverzüg-

lichen Tätigwerdens des Trägers und der eingeleiteten Maßnahmen verzichteten wir auf Sanktionen. Wir empfahlen aber, die Häufigkeit und die Wirksamkeit der Datenschutzschulungen regelmäßig zu evaluieren sowie Kriterien und Inhalte der Information betroffener Personen zu Datenschutzverletzungen zu überprüfen.

Die Nutzung von Kita-Apps ist in jedem Einzelfall datenschutzrechtlich zu prüfen. Maßnahmen zur Minderung des Risikos für die Rechte und Freiheiten betroffener Personen sind sorgfältig anhand der Art und des Umfangs der verarbeiteten Daten sowie der Nutzungsszenarien zu bestimmen und umzusetzen – selbstverständlich unter besonderer Berücksichtigung des Schutzes der Rechte von Kindern. Apps, die nur wenige personenbezogene Daten mit geringer Sensibilität verarbeiten, unterliegen geringeren Anforderungen an technische Maßnahmen als Apps, die Fotos, Gesundheitsdaten oder Entwicklungsberichte zu Kindern speichern bzw. Eltern zur Verfügung stellen.

Apps nicht wahllos verwenden

Unsere Empfehlung ist daher, eine Kita-App in einer ersten Ausbaustufe eher als digitales schwarzes Brett zu nutzen, um Eltern Informationen zukommen zu lassen, die keine personenbezogenen Daten enthalten (z. B. über Elternabende, Kita-Feste oder Fotografentermine). Auf Daten, die die Beschäftigungsverhältnisse des Kita-Personals oder die Gesundheit der Kinder betreffen, sollte zunächst verzichtet werden.

Werden in einer weiteren Ausbaustufe auch sensible personenbezogene Daten oder besondere Kategorien dieser Daten i. S. v. Artikel 9 DS-GVO in der Kita-App verarbeitet, empfehlen wir, mögliche Risiken sowie geeignete technische und organisatorische Gegenmaßnahmen im Rahmen einer Datenschutz-Folgenabschätzung gemäß Artikel 35 DS-GVO zu bestimmen. Zu den technischen Maßnahmen können etwa die Umsetzung einer Ende-zu-Ende-Verschlüsselung, die Mehrfaktorauthentisierung der Nutzerinnen und Nutzer sowie ein strenges Rollen-Rechte-Konzept mit eng begrenzten Zugriffsrechten gehören. Auch sollte darauf geachtet werden, dass die Softwarefirma, welche die App entwickelt, sowie möglicherweise mit dem Betrieb der Serversysteme beauftragte Unternehmen ihren Hauptsitz in der Europäischen Union haben, sodass diese auch direkt der Datenschutz-Grundverordnung unterliegen.

Die technische Umsetzung sollte von organisatorischen Maßnahmen flankiert werden. So können im Rahmen einer Geschäftsanweisung z. B. Vorgaben getroffen werden, die eine datensparsame und die ausschließlich an zuvor festgelegte Zwecke gebundene Nutzung der App gewährleisten. In diesem Kontext lassen sich auch Prozesse und Verantwortlichkeiten für die Veröffentlichung von personenbezogenen Daten in der App sowie zum Umgang mit Datenschutzverletzungen festlegen.

7 Bewertung von Beschäftigten im Internet

Viele Menschen suchen heutzutage im Internet nach Bewertungen, bevor sie z. B. ein Produkt erwerben, ein Hotel buchen oder eine Arztpraxis aufsuchen. Es überrascht nicht, dass seit einigen Jahren auch Arbeitgeberinnen und Arbeitgeber von ihren (ehemaligen oder aktuellen) Beschäftigten bewertet werden können und hierfür spezialisierte Internetplattformen existieren. Im Berichtszeitraum hatten wir uns mit einigen Beschwerden zu befassen, die betroffene Personen bei uns einreichten, weil ehemalige Arbeitgeberinnen bzw. Arbeitgeber ihre Daten aus dem Beschäftigungsverhältnis auf solchen Plattformen veröffentlicht hatten.

Im Regelfall bewerteten Beschäftigte zunächst ihre Arbeitgeberinnen bzw. Arbeitgeber auf der jeweiligen Plattform kritisch. Diese sahen sich dann veranlasst, in einer Erwiderung ihre Sicht der Dinge darzustellen. Die Reaktionen der jeweiligen Arbeitgeberinnen und Arbeitgeber enthielten oftmals auch personenbezogene Daten, die während des Beschäftigungsverhältnisses angefallen waren. Dabei handelte es sich beispielsweise um Angaben zu unentschuldigten Abwesenheiten, häufigen oder langen krankheitsbedingten Ausfällen, zur Nichtbeachtung von Anweisungen oder zu schlechten Arbeitsleistungen der Beschäftigten. Letztere beschwerten sich in der Folge bei uns über die Offenbarung derartiger Details im Internet.

Einen Teil der Fälle konnten wir nicht mehr nachvollziehen, da zum Zeitpunkt unserer Befassung die entsprechenden Daten auf der Plattform bereits gelöscht waren. Wenn die Veröffentlichung andauerte, prüften wir zunächst den Personenbezug der publizierten Daten. Dieser war in allen Fällen gegeben, da z. B. die Bewertung unter dem echten Namen vorgenommen oder die bewertende Person in der Erwiderung direkt mit ihrem Namen angesprochen wurde. Anschließend klärten wir, ob die jeweilige Reaktion tatsächlich dem bewerteten Unternehmen zuzurechnen war. Auch in dieser Hinsicht bestätigten sich die Beschwerden – die Antworten stammten entweder von der jeweiligen Geschäftsführung selbst oder waren durch sie veranlasst.

In den durch uns eingeholten Stellungnahmen führten die Unternehmen aus, dass sie sich durch die negativen, aus ihrer Sicht falschen

Bewertungen in ihren Rechten verletzt sahen, die Reputation der Firma wiederherstellen wollten und oftmals ein „Nachtreten“ ehemaliger Beschäftigter vermuteten. Zur Klarstellung gegenüber der Öffentlichkeit wurden deshalb z. B. auch die Gründe für verhaltensbedingte Kündigungen dargelegt.

So nachvollziehbar und verständlich die Motivation der Unternehmen auch ist – ihr Handeln muss sich stets an den datenschutzrechtlichen Vorgaben messen lassen und im Rahmen des gesetzlich Erlaubten bewegen. Insbesondere ist zu prüfen, ob das berechtigte Interesse eines Unternehmens, seinen guten Ruf und sein Ansehen zu verteidigen sowie Schaden abzuwenden, eine Veröffentlichung der personenbezogenen Daten ehemaliger Beschäftigter erfordert. Selbst wenn dies bejaht wird, müssen die Unternehmensinteressen gemäß Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) mit den schutzwürdigen Interessen der betroffenen Person abgewogen werden – hier der Person, die das Unternehmen kritisch und oftmals einseitig bewertet hatte. Falls deren schutzwürdige Interessen überwiegen, muss die Publikation personenbezogener Daten unterbleiben. Im Hinblick auf sensible Gesundheitsdaten trifft Artikel 9 Absatz 2 DS-GVO spezifische Einschränkungen, sodass deren Veröffentlichung ohnehin nur mit einer Einwilligung der betroffenen Person zulässig wäre.

Schlechte Publicity – Reaktion erlaubt?

Vor diesem Hintergrund haben beispielsweise Gesundheitsdaten von Beschäftigten nichts in öffentlich abrufbaren Erwiderungen auf kritische Bewertungen eines Unternehmens zu suchen. Auch bei Einschätzungen der Arbeitgeberin bzw. des Arbeitgebers zur Arbeitsleistung oder zum Sozialverhalten der Beschäftigten stehen deren Interessen einer schrankenlosen Publikation der Information durch das Unternehmen im Internet entgegen. Zulässig sind unserer Ansicht nach abstrakte Erwiderungen auf kritische Bewertungen, die die abweichende Sicht des Unternehmens zum Ausdruck bringen und auf personenbezogene Details verzichten. Zu beanstanden ist in der Regel auch nicht, wenn das Unternehmen in seiner Reaktion die bewertende Person direkt mit Namen anspricht. Voraussetzung hierfür ist allerdings, dass diese Person sich bereits zuvor zu erkennen gegeben und öffentlich gemacht hat, dass ein Beschäftigungsverhältnis besteht oder bestand.

Selbstverständlich kommt als Reaktion des Unternehmens auch ein Antrag bei der Plattformbetreiberin bzw. bei dem Plattformbetreiber in Betracht, die negative Bewertung zu löschen. Hier ist jedoch zu bedenken, dass manche ehemalige Beschäftigte sich durch eine gewisse „Hartnäckigkeit“ auszeichnen und das Unternehmen daraufhin erneut negativ bewerten. So geschah es auch in einem Beschwerdefall: Nach Löschung der ersten Bewertung durch den Plattformbetreiber erschien diese wortgleich erneut im Internet. Dies fasste das Unternehmen als Provokation auf. Seine Erwiderung unter Angabe personenbezogener Daten, die aus dem Arbeitsverhältnis stammten, führte zur Beschwerde der bewertenden Person bei uns. Im Ergebnis unseres Tätigwerdens änderte das Unternehmen seine Reaktion auf die Bewertung und verzichtete auf die Veröffentlichung der entsprechenden Daten. Außerdem wurden die unternehmensinternen Prozesse so angepasst, dass eine Wiederholung in ähnlichen Fällen ausgeschlossen ist.

Auch die anderen uns vorgelegten Beschwerden konnten unkompliziert geklärt werden, sodass sich ein weiteres aufsichtsbehördliches Einschreiten erübrigte.

8 Auskunftsanspruch bei Identitätsdiebstahl

Ein Beschwerdeführer meldete sich nach einem vermeintlichen Betrug bei einem Online-Händler. Er ging davon aus, dass seine personenbezogenen Daten im Rahmen eines Identitätsdiebstahls genutzt worden waren, um Waren in seinem Namen zu bestellen. Hiervon hatte er durch eine Mahnung des Zahlungsdienstleisters erfahren und beim Online-Händler sofort einen Antrag auf Auskunft nach Artikel 15 Datenschutz-Grundverordnung (DS-GVO) gestellt, der zunächst nicht erfüllt wurde.

Nach unserem Herantreten an den Verantwortlichen holte dieser die Auskunft nach Artikel 15 DS-GVO nach. Allerdings beinhaltete sie keine Informationen über die IP-Adresse der Person, die im Namen des Beschwerdeführers Waren bestellt hatte. Der Rechtsvertreter des Unternehmens erbat hierzu eine Beratung durch uns.

Wir teilten mit, dass unseres Erachtens zwar dem Wortlaut von Artikel 15 Absatz 1 DS-GVO nach grundsätzlich gegenüber der antragstellenden Person nur „sie betreffende personenbezogene Daten“ herauszugeben sind. Im Fall eines Identitätsdiebstahls sehen wir aber zumindest einen mittelbaren Bezug zwischen den verarbeiteten Daten und der geschädigten Person. Nach Sinn und Zweck der Vorschrift sollte das Opfer des Identitätsdiebstahls die Informationen über alle personenbezogenen Daten erhalten, die der Verantwortliche im Zusammenhang mit seiner Identität speichert. Dazu gehören auch diejenigen Daten, die auf der Grundlage der Handlungen der Betrügerin bzw. des Betrügers erhoben wurden, hier die IP-Adresse. Ein solches Vorgehen empfiehlt auch der Europäische Datenschutzausschuss in seinen Leitlinien zu den Betroffenenrechten.[20]

Letztlich folgte das Unternehmen unserer Auffassung und teilte dem Beschwerdeführer die IP-Adresse, die im Zuge des Identitätsdiebstahls verwendet wurde, mit.

---

20 Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.1, angenommen am 28. März 2023, Rn 107 sowie Beispiel 17.

9 Aufgepasst beim Weiterverkauf gebrauchter Pkw

Im Berichtszeitraum wandte sich ein Beschwerdeführer an uns, nachdem er seinen Pkw an einen Autohändler verkauft und diesem das Fahrzeug samt Nummernschild überlassen hatte. Einige Tage später fand er Fotos des Wagens auf einer großen Verkaufsplattform im Internet. Der Händler hatte sie dort eingestellt, ohne das Kfz-Kennzeichen unkenntlich zu machen.

Kfz-Kennzeichen stellen ein personenbezogenes Datum nach Artikel 4 Nummer 1 Datenschutz-Grundverordnung dar. Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung (z. B. einem Namen zu einer Kennnummer oder Standortdaten), identifiziert werden kann. Kennzeichen können zumindest mittelbar der jeweiligen Halterin bzw. dem Halter individuell zugeordnet werden; sie sind damit grundsätzlich personenbezogen. Dies hat bereits das Bundesverfassungsgericht festgestellt.[21]

Kennzeichen schwärzen!

Im vorliegenden Fall holte der Autohändler die notwendigen Schwärzungen auf den Fotos umgehend nach. Einer seiner Mitarbeiter, der mit datenschutzrechtlichen Anforderungen nicht ausreichend vertraut war, hatte dies zuvor versäumt. Im Rahmen des Vorfalls überprüfte der Verantwortliche unaufgefordert auch die vorhandenen Unternehmensprozesse und den internen Schulungsbedarf zum Datenschutz. Von weiteren Maßnahmen durch unsere Behörde konnte aufgrund dessen abgesehen werden.

Unternehmen aller Branchen und jeder Größe sind gut beraten, rechtzeitig und umfassend geeignete und angemessene Prozesse zur Umsetzung der datenschutzrechtlichen Anforderungen zu etablieren und deren Einhaltung zu kontrollieren. Um der Rechenschaftspflicht

21 Beschluss des Bundesverfassungsgerichts vom 18. Dezember 2018, 1 BvR 142/15, Rn 40.

nach Artikel 5 Absatz 2 Datenschutz-Grundverordnung nachzukommen, bedarf es auch einer entsprechenden Nachweisführung und Dokumentation. Unabhängig davon kann die Einhaltung des Datenschutzrechts die Kundenzufriedenheit erhöhen und Beschwerden bei uns vermeiden.

10 Geheimnisse der Mystery Box

Wer freut sich nicht über ein Überraschungspaket? Seit einiger Zeit finden sich an vielen Orten Automaten, an denen Verbraucherinnen und Verbraucher Retourenpakete kaufen können, ohne ihren Inhalt zu kennen. Sie werden gern als Mystery Boxes oder Secret Packs bezeichnet. Auch in den sozialen Medien ist der Trend, Überraschungspakete vor der Kamera auszupacken, nicht zu übersehen (sogenanntes Unboxing). Die Pakete können allerdings ungewollte Überraschungen bergen: Da es sich um Retouren handelt, kleben auf ihnen noch die Rücksendeetiketten. Diese enthalten personenbezogene Daten der ursprünglichen Paketempfängerinnen und -empfänger; außerdem kann der Inhalt Persönliches über sie verraten.

Die Landesbeauftragte erhielt konkrete Hinweise auf einen solchen Automaten mit Retourenpaketen in der Landeshauptstadt. Uns wurde mitgeteilt, dass Adressdaten und zum Teil sogar Telefonnummern auf den Rücksendeetiketten der Überraschungspakete nicht ausreichend geschwärzt waren. Dem gingen wir nach und leiteten ein Prüfverfahren ein.

Wer hat was bestellt?

Im Rahmen einer Vor-Ort-Kontrolle nahmen wir den Automaten gemeinsam mit dem Betreiber in Augenschein. Es bestätigte sich, dass die angebotenen Pakete noch mit dem ursprünglichen Etikett versehen waren. Die dort aufgedruckten Adressdaten waren lediglich händisch und in unterschiedlicher Gründlichkeit mit einem schwarzen Stift übermalt worden. Hierzu erläuterte der Betreiber, dass er die Pakete bereits mit geschwärzten Aufklebern von einem Zwischenhändler erhält. Dieser wiederum kauft die Pakete palettenweise von europaweit tätigen Versandunternehmen ohne Schwärzungen. Der Zwischenhändler macht die personenbezogenen Daten auf den Etiketten unkenntlich, bevor er die Pakete an den Automatenbetreiber weitervermittelt. Letzterer überprüft das Ergebnis und bessert bei Bedarf nach.

Bei der Kontrolle räumte der Betreiber ein, dass bei einigen Paketen die Schwärzungen nicht ausreichend waren, da Daten übersehen wurden oder die Farbe sich wieder abwischen ließ. Auch waren Adressen trotz der Schwärzungen in bestimmtem Licht teilweise

noch lesbar. Wir wiesen ihn darauf hin, dass auf diese Weise personenbezogene Daten offengelegt werden. Hierfür gab es keine Rechtsgrundlage.

Im Ergebnis haben wir dem Automatenbetreiber empfohlen, Schwärzungen bei allen Paketen stets vollständig und irreversibel vorzunehmen. Da auch Strichcodes personenbezogene Daten enthalten können, sollten auch sie geschwärzt werden. Der Verantwortliche zeigte sich einsichtig. Auf weitere aufsichtsrechtliche Maßnahmen verzichteten wir.

Darüber hinaus war es uns ein Anliegen, dass die Pakete gar nicht erst mit lesbaren Etiketten an den Automatenbetreiber ausgeliefert werden. Deshalb haben wir die für den Zwischenhändler zuständige Datenschutzaufsichtsbehörde in einem anderen Bundesland über die Angelegenheit informiert.

V Ausgewählte Beratungen

1 Verwaltungsdigitalisierung und Umsetzung des Onlinezugangsgesetzes

Bereits im vorherigen Berichtszeitraum traten Änderungen des Onlinezugangsgesetzes (OZG) sowie weiterer Vorschriften zur Digitalisierung der Verwaltung in Kraft.[22] Von besonderer Bedeutung sind in diesem Kontext die Festlegungen des § 8a OZG. Sie beseitigen Rechtsunsicherheiten, die uns zuvor bei der Begleitung und Bewertung von länderübergreifenden Onlinediensten nach dem Einer-für-Alle-Prinzip (EfA)[23] regelmäßig begegneten. Konkret bestehen nun mit § 8a Absatz 1 OZG eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten im länderübergreifenden Onlinedienst und mit § 8a Absatz 4 OZG eine klare Zuweisung der datenschutzrechtlichen Verantwortlichkeit an die den jeweiligen Dienst betreibende Behörde. Laut der Gesetzesbegründung ist strikt zu unterscheiden zwischen der Beantragung von Verwaltungsleistungen im Onlinedienst und dem anschließenden Fachverfahren. Für die zuerst genannte Phase ist die den Dienst betreibende Behörde länderübergreifend allein datenschutzrechtlich verantwortlich; die Verantwortlichkeit der jeweils zuständigen Fachbehörden (meist in den Kommunalverwaltungen) beschränkt sich auf die zuletzt genannte Phase.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat eine Arbeitsgruppe eingerichtet, die sich mit Fragen der Umsetzung des Onlinezugangsgesetzes befasst und in der wir aktiv mitwirken. Darüber hinaus werden entsprechende Themen regelmäßig im Arbeitskreis Verwaltung der Datenschutzkonferenz erörtert, dem wir zusammen mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg vorsitzen. Wir berichten im Folgenden über wesentliche Aktivitäten in beiden Gremien.

22 Tätigkeitsbericht Datenschutz 2024, A V 5.
23 ebenda

1.1 Orientierungshilfe der Datenschutzkonferenz zu § 8a OZG

Bereits gegen Ende des vorherigen Berichtszeitraums hat die Datenschutzkonferenz in der „Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG)“ die aus ihrer Sicht wesentlichen datenschutzrelevanten Änderungen im Onlinezugangsgesetz gegenüber der alten Rechtslage zusammengestellt und die Auswirkungen erörtert. Ein weiteres Ziel des Dokuments bestand darin, den von den Gesetzesänderungen betroffenen öffentlichen Stellen Hinweise und Unterstützung bei der Entwicklung bzw. der Nachnutzung länderübergreifender Onlinedienste zu geben.

Im Berichtszeitraum haben die Datenschutzaufsichtsbehörden viele Erfahrungen mit der Anwendung dieser Orientierungshilfe gesammelt. Darüber hinaus ergaben sich im Rahmen der Beratungs- und Prüfpraxis neue Fragestellungen. Die o. g. Arbeitsgruppe der Datenschutzkonferenz schrieb das Papier deshalb fort und ergänzte es um neue Inhalte. Die Version 1.1 wurde gegen Ende des Berichtszeitraums nach einer Erörterung im Arbeitskreis Verwaltung von der Konferenz verabschiedet und veröffentlicht.

Zu den wesentlichen Ergänzungen in der neuen Fassung der Orientierungshilfe gehören Erläuterungen zum Verständnis des Begriffs „länderübergreifender Onlinedienst“. Diese sind essenziell für die Anwendung der Vorschriften von § 8a OZG, die mit der Novellierung in das Gesetz eingefügt wurden. Die Orientierungshilfe nimmt insofern eine Interpretation der gesetzlichen Definition von § 2 Nummer 8 OZG vor. Sie hilft auch Stellen, die derartige Onlinedienste nachnutzen, in Zweifelsfällen ihre datenschutzrechtliche Verantwortlichkeit und Zuständigkeit besser abzugrenzen.[24]

Neu ist darüber hinaus ein Abschnitt, der die Auffassung der Datenschutzaufsichtsbehörden zu Vereinbarungen über die Auftragsverarbeitung oder über eine gemeinsame datenschutzrechtliche Verantwortung im Kontext länderübergreifender Onlinedienste darstellt. Derartige Vereinbarungen wurden in der Vergangenheit häufig zwischen der den Dienst anbietenden Stelle und den nachnutzenden Behörden geschlossen. Wegen der Vorschriften in § 8a OZG bedarf

24 Siehe A V 1.3.3.

es dieser Dokumente nicht mehr.[25] Bereits geschlossene Vereinbarungen sind nach Auffassung der Aufsichtsbehörden aufzuheben.

Weitere Ergänzungen und Änderungen der Orientierungshilfe betreffen die Anpassung der Datenschutzerklärung für einen länderübergreifenden Onlinedienst, die Einbindung von Nutzerkonten zur Identifizierung und Authentifizierung der Nutzerinnen bzw. Nutzer von Onlinediensten sowie Dokumentations- und Nachweispflichten der Verantwortlichen, etwa im Hinblick auf das Verzeichnis der Verarbeitungstätigkeiten, die Umsetzung von technischen und organisatorischen Maßnahmen oder eine ggf. durchzuführende Datenschutz-Folgenabschätzung.

1.2 Standardisierter Prüfprozess für länderübergreifende EfA-Onlinedienste

Bei länderübergreifenden Onlinediensten, die nach dem Einer-für-Alle-Prinzip (EfA) realisiert werden, stellt sich häufig die Frage, wie datenschutzrechtliche Anforderungen im Prozess der Entwicklung und beim Betrieb dieser Dienste umgesetzt werden können. Gleichzeitig sollten die Datenschutzaufsichtsbehörden projektbegleitend die Anbieterinnen und Anbieter verschiedener länderübergreifender EfA-Onlinedienste einheitlich beraten bzw. die Dienste nach den gleichen Maßstäben bewerten. Vor diesem Hintergrund hat die o. g. Arbeitsgruppe der Datenschutzkonferenz im Berichtszeitraum einen „Standardisierten Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz (OZG)“ erarbeitet. Dieser wurde nach Erörterung im Arbeitskreis Verwaltung von der Konferenz zum Ende des Berichtszeitraums verabschiedet und veröffentlicht. Seine Anwendung ist allen Stellen, die derartige Onlinedienste entwickeln bzw. betreiben, empfohlen.

Kern des Dokuments ist eine strukturierte Handlungsanleitung zur Umsetzung der Vorgaben der Datenschutz-Grundverordnung (DS-GVO) und datenschutzrechtlicher Spezialnormen bei der Entwicklung oder grundlegenden Überarbeitung von länderübergreifenden EfA-Onlinediensten. Berücksichtigt wurden auch die Verordnung des Bundesministeriums für Digitales und Staatsmodernisierung

25 Siehe A V 1.3.2.

über Standards für den Onlinezugang zu Verwaltungsleistungen (Standardverordnung Onlinezugang, OZSV) sowie die in § 2 Absatz 2 OZSV referenzierte DIN SPEC 66336, die über die DIN Media GmbH bezogen werden kann. Dort werden als Teil der Qualitätskriterien eines Onlinedienstes zwar auch Datenschutzanforderungen definiert, jedoch keine konkreten Vorgaben getroffen, was genau zu welchem Zeitpunkt von den Verantwortlichen umzusetzen bzw. zu prüfen ist.

An dieser Stelle setzt der standardisierte Prüfprozess an. Er orientiert sich an den bei der Umsetzung von Digitalisierungsprojekten auf Ebene des Bundes und der Länder regelmäßig zur Anwendung kommenden Vorgaben des Projektmanagements. Den fünf klassischen Phasen des Projektmanagements (Initialisierung, Definition, Planung, Durchführung sowie Abschluss) werden jeweils Prozessschritte zugeordnet, in denen die wichtigsten datenschutzrechtlichen Fragen zu prüfen und zu klären sind. Für jeden Prozessschritt werden die durchzuführenden Aktivitäten beschrieben, einschlägige Rechtsvorschriften benannt und Hinweise auf weiterführende Veröffentlichungen der Datenschutzaufsichtsbehörden gegeben.

Der große Wert des standardisierten Prüfprozesses liegt darin, dass die strukturierte Durchführung des Entwicklungsvorhabens eines länderübergreifenden EfA-Onlinedienstes eng mit der Prüfung der Einhaltung bzw. der Umsetzung datenschutzrechtlicher und technisch-organisatorischer Anforderungen verzahnt wird. Darüber hinaus enthält ein Anhang des Prüfprozesses einen Vorschlag für die Struktur eines Datenschutzkonzeptes mit sich anschließender Datenschutz-Folgenabschätzung. Dieser erleichtert Verantwortlichen die Erfüllung ihrer Nachweis- und Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DS-GVO. Nach unserer Auffassung bietet der „Dreiklang“ aus Prozessorientierung, datenschutzrechtlichen Prüfinhalten und Dokumentationsempfehlung Verantwortlichen eine außerordentlich wertvolle Unterstützung und Handlungsanleitung, damit sie bei der Realisierung von länderübergreifenden EfA-Onlinediensten die gesetzlichen Vorgaben einhalten.

Der standardisierte Prüfprozess weist aber auch darüber hinaus: Wir werden ihn als Aufsichtsbehörde ebenso anwenden, um Umsetzungsprojekte im Kontext des Onlinezugangsgesetzes zu begleiten, zu beraten und zu prüfen. Wir sind uns in dieser Hinsicht mit vielen anderen Datenschutzaufsichtsbehörden in Deutschland einig, die ähnliche Absichten verfolgen. Dieses gemeinsame, abgestimmte

Vorgehen innerhalb der Datenschutzkonferenz dient nicht zuletzt einer einheitlichen und transparenten Beratungs- und Prüfpraxis in Bund und Ländern.

1.3 Zu einzelnen OZG-Projekten

1.3.1 Begleitung der Umsetzung von Onlinediensten im Themenfeld „Ein- und Auswanderung“

Das Ministerium des Innern und für Kommunales des Landes Brandenburg ist gemeinsam mit dem Auswärtigen Amt deutschlandweit federführend für die Umsetzung von länderübergreifenden Onlinediensten im OZG-Themenfeld „Ein- und Auswanderung“. Zu den dort nach dem Einer-für-Alle-Prinzip entwickelten Diensten gehören z. B. die elektronische Beantragung von Aufenthaltstiteln sowie von Aufenthaltskarten und aufenthaltsrelevanten Bescheinigungen.[26] Im Berichtszeitraum haben wir die datenschutzrechtliche Begleitung der Projekte, die unter dem Titel „Aufenthalt digital“ zusammengefasst und in mittlerweile 15 Bundesländern eingesetzt werden, fortgesetzt.

Positiv hervorzuheben ist, dass die Änderungen im Onlinezugangsgesetz, insbesondere die Ergänzung von § 8a OZG, von den Projektverantwortlichen rasch umgesetzt wurden. Eine Auswirkung der Novellierung des Gesetzes ist beispielsweise, dass das Ministerium nunmehr deutschlandweit allein für alle Anträge auf Aufenthaltstitel datenschutzrechtlich verantwortlich ist (sofern die Antragstellung über den Onlinedienst erfolgt). Dementsprechend wurden auch die bisher genutzten Vereinbarungen zur Auftragsverarbeitung nach Artikel 28 Datenschutz-Grundverordnung (DS-GVO) mit nachnutzenden Behörden nicht weiter verwendet und die datenschutzrechtlichen Dokumentationen an die neue Rechtslage angepasst. Das Ministerium beachtete auch unsere Hinweise zur Aktualisierung der Datenschutzerklärung bei den Onlinediensten und pflegte erforderliche Änderungen unverzüglich in die Webseiten ein.

Eine neue Entwicklung, die sich im Berichtszeitraum abzeichnete, ist der geplante Einsatz von Künstlicher Intelligenz (KI) bei der Prüfung

---

26 Tätigkeitsbericht Datenschutz 2023, A I 2.2.

von Anträgen. Eine KI-gestützte Komponente soll zunächst Antragstellerinnen und Antragsteller, später auch Sachbearbeiterinnen und Sachbearbeiter in den Ausländerbehörden unterstützen. Ziel ist, die Qualität der eingereichten Anträge zu erhöhen, ihre Vollständigkeit und Korrektheit zu sichern sowie den Kommunikationsaufwand zur Nachforderung von Unterlagen zu vermindern. Ähnlich wie beim KI-unterstützten Wohngeldverfahren[27] soll die eingesetzte KI hier die eingereichten Dokumente klassifizieren, Daten extrahieren sowie den Antrag auf Vollständigkeit und Konsistenz prüfen. Da beabsichtigt ist, dies bereits während der Antragstellung im Onlinedienst durchzuführen, können betroffene Personen bei Fehlern oder Unklarheiten unmittelbar eine Rückmeldung erhalten und zur Nachbesserung aufgefordert werden.

Aus datenschutzrechtlicher Sicht stellt sich u. a. die Frage, auf welcher Rechtsgrundlage die personenbezogenen Daten mittels Künstlicher Intelligenz verarbeitet werden. Eine ausdrückliche Erlaubnis fehlt aus unserer Sicht sowohl im brandenburgischen Landes- als auch im Bundes- oder Europarecht. Im Rahmen eines Vor-Ort-Gesprächs haben wir mit den Projektverantwortlichen weiterhin technische und organisatorische Maßnahmen erörtert, durch die mögliche Risiken für betroffene Personen bei der Datenverarbeitung minimiert werden können. Wir machten darauf aufmerksam, dass KI-spezifische Risiken (wie Halluzinationen, Voreingenommenheit oder Diskriminierung) besonders sorgfältig zu betrachten sind. Darüber hinaus empfahlen wir zu prüfen, ob eine Pseudonymisierung oder Anonymisierung der Daten hier sinnvoll eingesetzt werden kann. Und schließlich erinnerten wir daran, dass die KI lediglich als Hilfe und Unterstützung genutzt werden darf und die letzte Entscheidung stets ein Mensch bei der Bearbeitung zu treffen hat.

Wir werden die Gespräche fortführen, entsprechende datenschutzrechtliche Dokumentationen auswerten (sobald diese vorliegen) und dann eine abschließende Einschätzung vornehmen.

27 Siehe A I 3.

1.3.2 Nachnutzung der Rechnungseingangsplattform des Bundes

Im Berichtszeitraum bat uns das Ministerium der Finanzen und für Europa des Landes Brandenburg um eine datenschutzrechtliche Einschätzung einer Verwaltungsvereinbarung mit dem Bund zur Mitnutzung der OZG-konformen Rechnungseingangsplattform OZG-RE, deren Abschluss im Rahmen der Umsetzung der Richtlinie 2014/55/EU über die elektronische Rechnungsstellung bei öffentlichen Aufträgen geplant war. Die Richtlinie verpflichtet die Verwaltung, elektronische Rechnungen zu empfangen und zu verarbeiten, die der europäischen Norm für die elektronische Rechnungsstellung entsprechen. Bereits im Jahr 2019 hatte der Minister der Finanzen im Einvernehmen mit dem Minister des Innern und für Kommunales auf Grundlage des § 5 Absatz 2 Brandenburgisches E-Governmentgesetz die Verordnung über die elektronische Rechnungsstellung bei öffentlichen Aufträgen im Land Brandenburg (BbgERechV) erlassen. § 3 Absatz 2 i. V. m. § 4 Absatz 2 BbgERechV schreibt für Rechnungsempfängerinnen und -empfänger, die zur juristischen Person Land Brandenburg gehören, die Nutzung des vom Land zur Verfügung gestellten Verwaltungsportals für elektronisch ausgestellte und übermittelte Rechnungen vor.

Das Ministerium übersandte uns die Entwürfe der Verwaltungsvereinbarung sowie des Vertrags zur Auftragsdatenverarbeitung nach Artikel 28 Datenschutz-Grundverordnung (DS-GVO) für die Mitnutzung der vom Bund bereitgestellten Plattform. Geplant war die zeitnahe Unterzeichnung durch mehrere Länder einschließlich Brandenburg.

Im Zuge der Befassung mit der Anfrage stellten wir fest, dass es sich bei der OZG-konformen Rechnungseingangsplattform OZG-RE um einen länderübergreifenden Onlinedienst i. S. v. § 2 Nummer 8 Onlinezugangsgesetz (OZG) handelt. Betreiber ist das Beschaffungsamt des Bundesministeriums des Innern, das die Bundesdruckerei GmbH mit der technischen Dienstleistung beauftragt hat. Wegen der Kategorisierung als länderübergreifender Onlinedienst sind für die Plattform die Vorgaben von § 8a OZG zu beachten. Das Beschaffungsamt ist wegen § 8a Absatz 4 OZG allein datenschutzrechtlich verantwortlich für die Verarbeitung personenbezogener Daten auf der Plattform. Hierfür liefert § 8a Absatz 1 OZG eine Rechtsgrundlage. Diese erlaubt auch die Übermittlung der Rechnungen an die Rechnungs-

empfängerinnen und -empfänger, die ihrerseits für die weitere Verarbeitung datenschutzrechtlich allein verantwortlich sind.

Die vom Finanzministerium vorgelegten Unterlagen zeigten, dass die genannten gesetzlichen Vorschriften nicht beachtet wurden. Insbesondere sahen wir aufgrund der klaren Zuweisung der datenschutzrechtlichen Verantwortung keinen Raum für den Abschluss einer Vereinbarung zur Auftragsdatenverarbeitung nach Artikel 28 DS-GVO.[28] Nachdem wir das Ministerium über unsere Einschätzung informiert hatten, suchten wir den Austausch mit der Dienststelle der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie mit dem Datenschutzbeauftragten des Beschaffungsamts. Im Rahmen der Erörterung wurde Einigkeit darüber erzielt, dass vor der geplanten Unterzeichnung der Mitnutzungsvereinbarung eine Anpassung an die Vorgaben von § 8a OZG herbeizuführen war. Angemerkt sei an dieser Stelle, dass zwischen der initialen Kontaktaufnahme des brandenburgischen Finanzministeriums mit uns und dem geplanten Zeichnungstermin vor Ort im Bundesministerium für Digitales und Staatsmodernisierung lediglich 13 Tage lagen.

Das erreichte, äußerst erfreuliche Ergebnis zeigt, wie wichtig die frühzeitige Einbeziehung unserer datenschutzrechtlichen Expertise bei der Verwaltungsdigitalisierung ist. Trotz der kurzen Fristen konnte vermieden werden, dass Bund und Länder die ursprünglich vorgelegten, nicht rechtskonformen Vereinbarungen unterzeichnen und im Ergebnis eines aufsichtsrechtlichen Tätigwerdens hätten nachbessern müssen.

Im Nachgang wiesen wir das Finanzministerium ergänzend darauf hin, dass § 4 Absatz 4 BbgERechV zu ändern ist. Dort wurde ursprünglich festgelegt, dass dem Ministerium die Bereitstellung des Rechnungseingangsportals obliegt. Diese Vorgabe widerspricht den aktuellen Gegebenheiten und wie oben ausgeführt § 8a Absatz 4 OZG.

28 Siehe A V 1.1.

1.3.3 Nachnutzung des Onlinedienstes zur Förderung ehrenamtlicher Tätigkeit (Ehrenamtskarte)

Das Land Nordrhein-Westfalen ist bundesweit zuständig für die Entwicklung und Bereitstellung eines länderübergreifenden Onlinedienstes zur Förderung ehrenamtlicher Tätigkeit. Personen, die sich in besonderem Maße ehrenamtlich für das Gemeinwohl engagieren, können mit der sogenannten Ehrenamtskarte bestimmte Angebote öffentlicher, gemeinnütziger und privater Einrichtungen vergünstigt nutzen. Im Rahmen des Onlinedienstes können Bürgerinnen und Bürger mittels einer speziellen App eine Ehrenamtskarte beantragen, verlängern und bei den Vergünstigungspartnerinnen und -partnern vorzeigen. Das Angebot beinhaltet darüber hinaus ein Verwaltungsprogramm für die zuständigen Behörden in den Ländern, das dazu dient, z. B. Anträge zu bearbeiten, Nachrichten zum Ehrenamt zu versenden oder die Akzeptanzstellen der Ehrenamtskarte übersichtlich darzustellen.

Durch die Integration verschiedener Funktionen in der Software bestanden bei diesem Onlinedienst Unsicherheiten hinsichtlich der Anwendbarkeit der Regelungen von § 8a OZG, der Abgrenzung der datenschutzrechtlichen Verantwortlichkeit und der Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Sie konnten in der von der Datenschutzkonferenz eingerichteten Arbeitsgruppe zu Fragen der Umsetzung des Onlinezugangsgesetzes durch eine intensive Diskussion unter Beteiligung der nordrhein-westfälischen Datenschutzaufsichtsbehörde geklärt werden. Insbesondere wurde festgestellt, dass derjenige Teil der Software, der die Beantragung und Nutzung der Ehrenamtskarte durch Bürgerinnen und Bürger direkt betrifft (die App), als länderübergreifender Onlinedienst i. S. v. § 2 Nummer 8 OZG zu klassifizieren ist. Auf diesen Teil sind die Vorgaben von § 8a OZG anzuwenden, woraus in der Konsequenz eine zentrale, länderübergreifende datenschutzrechtliche Verantwortlichkeit der den Dienst anbietenden Behörde resultiert. Demgegenüber ist derjenige Teil der Software, durch den die Verwaltungsprozesse in den zuständigen Landes- bzw. Kommunalbehörden unterstützt werden und der ergänzende Funktionen (z. B. den Nachrichtendienst) enthält, als nachgelagertes Fachverfahren aufzufassen. Hier sind die jeweiligen lokalen Behörden eigenständig datenschutzrechtlich verantwortlich, da § 8a OZG nicht anwendbar ist.

Im Ergebnis der Diskussionen bestand unter den Datenschutzaufsichtsbehörden Einigkeit, dass die technische Gestaltung eines Dienstes zur Verwaltungsdigitalisierung, das Vorhandensein etwaiger Zusatzfunktionen oder das Design nicht dazu führen dürfen, die gesetzlichen Festlegungen von § 8a OZG zu umgehen. Das würde nicht nur eine Aufspaltung der datenschutzrechtlichen Verantwortung für denselben Dienst zwischen einer Vielzahl von nutzenden Behörden bedeuten, sondern auch den Abschluss entsprechend vieler Vereinbarungen zur Auftragsverarbeitung oder zur gemeinsamen Verantwortung erfordern. Genau dies sollte aber mit der gesetzlichen Neuregelung im Onlinezugangsgesetz vermieden werden. Diese gemeinsame Haltung der Aufsichtsbehörden für eine weite Auslegung der Begriffsdefinition zu Onlinediensten fand Eingang in die überarbeitete und ergänzte Version der Orientierungshilfe der Datenschutzkonferenz zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes.[29]

29 Siehe A V 1.1.

2 Einsatz von Microsoft 365 in der Landesverwaltung

Die Standard-PCs für Beschäftigte in der Landesverwaltung Brandenburg sind u. a. mit dem Microsoft Office-Paket für Büroanwendungen ausgestattet. Bereits seit vielen Jahren ist bekannt, dass der Hersteller ab Mitte Oktober 2025 keine weitere Unterstützung der verwendeten Produktversion anbietet. Eine Nutzung über den genannten Zeitpunkt hinaus birgt erhebliche, auch datenschutzrechtliche Risiken, da die enthaltenen Programme nicht mehr aktualisiert, Fehler nicht mehr bereinigt und Sicherheitslücken nicht mehr geschlossen werden. Im Berichtszeitraum musste die Landesverwaltung insofern eine Entscheidung für eine neue Version oder ein anderes Produkt treffen und den Wechsel dorthin vollziehen.

Über die beratende Mitgliedschaft im Gremium der IT-Beauftragten der Ressorts (RIO-Ausschuss) und durch direkte Kontakte mit dem Brandenburgischen IT-Dienstleister war unsere Behörde von Anfang an in die Planungen und Entscheidungsprozesse einbezogen. Bereits früh stand fest, dass der Wechsel zu einem Softwarepaket eines anderen Herstellers oder zu Open-Source-Lösungen (auch zur Stärkung der digitalen Souveränität der Landesverwaltung) wegen der Kürze der zur Verfügung stehenden Zeit keine realistische Option war. Hierzu hätten Marktsondierungen, Produktbewertungen und Tests wesentlich früher starten müssen. Im Rahmen einer Wirtschaftlichkeitsbetrachtung stellte der Brandenburgische IT-Dienstleister deshalb die verschiedenen Varianten für einen Wechsel zu aktuellen Microsoft-Produkten einander gegenüber. Die Entscheidung fiel letztlich zugunsten von Microsoft 365.

Hierzu hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) im November 2022 einstimmig den Beschluss gefasst, dass Verantwortliche auf Basis der damaligen, von Microsoft bereitgestellten Vertragsunterlagen keinen Nachweis für einen datenschutzrechtskonformen Betrieb von Microsoft 365 führen können.[30] Die einzel-

30 Tätigkeitsbericht Datenschutz 2022, A V 1.

nen Kritikpunkte, die dieser Bewertung zugrunde lagen, werden in dem umfangreichen Abschlussbericht der Arbeitsgruppe der Datenschutzkonferenz detailliert erläutert. Wir machten in unseren Gesprächen mit den Verantwortlichen der Landesverwaltung immer wieder auf die Feststellungen aufmerksam – zumal auch in den seit 2022 von Microsoft vorgenommenen Fortschreibungen des Vertrags keine wesentlichen Änderungen in Bezug auf die Kritikpunkte zu verzeichnen waren.

Für die brandenburgische Landesverwaltung wurde entschieden, Microsoft 365 in einer spezifischen Ausprägung zu betreiben: Datenschutzrechtlich verantwortlich sind (wie bisher auch) die einzelnen Behörden. Der Brandenburgische IT-Dienstleister fungiert als Auftragsverarbeiter. Er installiert und wartet ausgewählte Programme des Office-Pakets (wie Textverarbeitung, Tabellenkalkulation, E-Mail-Client) lokal auf den PCs der Beschäftigten. Sämtliche Cloud-Funktionen von Microsoft 365 werden zentral abgeschaltet und alle Daten (wie Schreiben, Präsentationen, Tabellen und E-Mails) ausschließlich im Rechenzentrum des Brandenburgischen IT-Dienstleisters gespeichert. Microsoft nimmt die Rolle eines Unterauftragnehmers der Auftragsverarbeitung ein. Die Funktion umfasst hier die Verwaltung der Login-Daten der Beschäftigten und der Lizenzen. Im Vergleich zu einer vollständig cloudbasierten Nutzung von Microsoft 365 ist dies zumindest eine datensparsame Einbeziehung von Microsoft; die inhaltlich relevanten Daten sollen im Land verbleiben.

Daneben führte der Brandenburgische IT-Dienstleister bereits frühzeitig auf Test-PCs und für typische Nutzungsszenarien umfangreiche Untersuchungen zu Datenübermittlungen durch, bei denen Komponenten des Microsoft 365-Pakets involviert sind und Daten zum Hersteller oder zu Dritten transferiert werden. Nur zwingend erforderliche Verbindungen (z. B. für die Lizenzprüfung) werden erlaubt, alle anderen zentral am Ausgang des Landesverwaltungsnetzes zum Internet blockiert. Durch diese Vorkehrungen sollen unkontrollierte Abflüsse von Daten aus der Landesverwaltung verhindert werden. Sie bauen auf entsprechenden Untersuchungen und Maßnahmen für Windows 10 und 11 als Betriebssystem der PCs auf. Auch werden alle sonst empfohlenen Sicherheitsmaßnahmen für die Endgeräte in enger Kooperation von verantwortlicher Landesbehörde und Brandenburgischem IT-Dienstleister umgesetzt.

Wir waren von Anfang an in die genannten Untersuchungen und die Ableitung der Maßnahmen eingebunden. Bereits gegen Ende des vergangenen Berichtszeitraums hatte unsere Behörde die Gelegenheit zu einem intensiven Austausch mit dem Brandenburgischen IT-Dienstleister hierzu. Schon damals machten wir darauf aufmerksam, dass die Umsetzung technischer und organisatorischer Maßnahmen nach Artikel 32 Datenschutz-Grundverordnung (DS-GVO) zur Minimierung möglicher Risiken nur ein Baustein der rechtskonformen Verarbeitung personenbezogener Daten ist. Daneben sind z. B. die Transparenz zu wahren (Artikel 5 Absatz 1 DS-GVO), die Rechte betroffener Personen zu gewährleisten (Artikel 12 ff. DS-GVO) oder vertragliche Regelungen mit Auftragsverarbeitern gesetzeskonform zu gestalten (Artikel 28 DS-GVO). Wir waren insofern gespannt, welche Vereinbarungen die Landesverwaltung mit Microsoft zur Auftragsverarbeitung treffen und ob sie die o. g. Kritikpunkte der Datenschutzkonferenz von 2022 durch den ausgehandelten Vertrag ausräumen würde.

Die Verhandlungen starteten im Frühjahr des Berichtszeitraums, der Abschluss erfolgte Mitte des Jahres. Federführend auf der Seite der Landesverwaltung war der Brandenburgische IT-Dienstleister, unterstützt durch eine Rechtsanwaltskanzlei. Entwürfe des Vertrags mit Microsoft zur Auftragsverarbeitung wurden uns regelmäßig zur Verfügung gestellt. Zur vorfinalen Version nahmen wir schriftlich gegenüber dem Brandenburgischen IT-Dienstleister Stellung und informierten im RIO-Ausschuss auch die Ressorts über die Bewertung. Unsere Kommentare fanden jedoch leider keine Berücksichtigung im weiteren Verfahren.

Basis des für die Landesverwaltung ausgehandelten Vertrages bildet das so genannte Data Protection Addendum in der Fassung von Januar 2023 – eine Vertragsergänzung zu den allgemeinen Nutzungsbedingungen für Produkte von Microsoft, mit der datenschutzrechtliche Festlegungen getroffen werden sollen. Zu den konkreten Vertragsinhalten hatten wir insbesondere die folgenden kritischen Anmerkungen:

- Mit dem Vertrag werden die wesentlichen Kritikpunkte der Datenschutzkonferenz aus dem Jahr 2022 nicht ausgeräumt. Vielmehr ergibt ein Vergleich der Vertragstexte, dass die betreffenden Stellen größtenteils unverändert aus der früheren Version übernommen wurden. Dies betrifft z. B. die Festlegung der

Kategorien personenbezogener Daten und betroffener Personen für die Auftragsverarbeitung, die Bindung von Microsoft als Dienstleister an Weisungen der Auftraggeber aus der Landesverwaltung, die Offenlegung personenbezogener Daten durch Microsoft für Dritte sowie die Löschung von Daten, die im Auftrag verarbeitet werden.

- Microsoft lässt sich im Vertrag das Recht einräumen, Daten aus der Auftragsverarbeitung für eigene, unternehmensinterne Zwecke zu verwenden. Da öffentliche Stellen im Land Brandenburg keine Rechtsgrundlage haben, hierfür personenbezogene Daten an Microsoft zu übermitteln, müssen diese Daten zuvor anonymisiert bzw. aggregiert werden. Der Vertrag enthält keine Aussagen dazu, wie die Prozesse der Anonymisierung bzw. Aggregation personenbezogener Daten gestaltet sind. Unklar ist auch, wie die Rollentrennung bei Microsoft intern (als Auftragsverarbeiter mit personenbezogenen Daten, für eigene Zwecke ohne personenbezogene Daten) geregelt ist.

- Der Vertrag spiegelt die beabsichtigte sehr eingeschränkte Dienstleistung, die Microsoft für die Landesverwaltung erbringen soll, nicht in ausreichendem Maße wider. Wir hätten erwartet, dass die Kategorien betroffener Personen auf Beschäftigte und die Kategorien personenbezogener Daten auf Login- und Lizenzinformationen begrenzt werden. Stattdessen finden sich im entsprechenden Vertragsanhang alle möglichen Gruppen betroffener Personen (z. B. Familienangehörige von Beschäftigten, „Kunden, Klienten, Patienten, Besucher, [...], minderjährige Personen oder [...], Kirchenmitarbeiter“) und alle möglichen Arten personenbezogener Daten (z. B. Stammdaten inkl. Adresse und Geburtsdatum auch von Familienmitgliedern, „Finanz- und Versicherungsinformationen, [...], Standortdaten, Fotos, Videos und Audio, [...], Personal- und Einstellungsdaten, [...], Daten zur Gesundheit“). Es drängt sich der Eindruck auf, dass etwas geregelt werden soll, was nicht geregelt werden muss, oder dass die Landesverwaltung sich die Option offenhalten will, doch umfassend die Cloud-Dienste von Microsoft zu nutzen.

- Der Vertrag enthält an verschiedenen Stellen Unklarheiten, Widersprüche und irrelevante Teile. Die Verständlichkeit, Transparenz und Handhabbarkeit des Vertrages ließen sich durch eine Überarbeitung bzw. Streichung erheblich verbessern.

Im Ergebnis erfüllt der vorliegende Vertrag aus unserer Sicht nicht die Anforderungen von Artikel 28 DS-GVO. Wir kommen insofern zu der gleichen Feststellung wie die Datenschutzkonferenz 2022: Auf Grundlage dieser Vereinbarung kann der Nachweis einer rechtskonformen Auftragsverarbeitung nicht erbracht werden. Dies gilt unabhängig davon, dass der Brandenburgische IT-Dienstleister auf technischer und organisatorischer Ebene eine Reihe von Maßnahmen umgesetzt hat, um die durch die Verarbeitung personenbezogener Daten auftretenden Risiken zu minimieren. Die Rechtswidrigkeit des Vertrages kann dadurch nicht geheilt werden.

Rechtskonformer Einsatz von Microsoft 365 fraglich

Der Brandenburgische IT-Dienstleister, unterstützt durch die erwähnte Anwaltskanzlei, teilte unsere Auffassung nicht. Insbesondere übersandte uns die Kanzlei eine umfangreiche Stellungnahme. Sie enthält Textbausteine, die offensichtlich auf andere Bundesländer Bezug nehmen, Erläuterungen zur Datenverarbeitung bei Microsoft, die jedoch keinen Eingang in den Vertrag fanden, sowie Empfehlungen für zusätzliche technische und organisatorische Maßnahmen, die im Land umgesetzt werden sollten. In der anschließenden Diskussion hierzu zeigte sich, dass Microsoft in den Vertragsverhandlungen nicht bereit war, Änderungen am Vertragstext vorzunehmen, die vom Brandenburgischen IT-Dienstleister gewünscht waren oder die unserer Kritik Rechnung getragen hätten. Die gleiche Erfahrung hatte einige Jahre zuvor auch schon die Arbeitsgruppe der Datenschutzkonferenz machen müssen. Mittlerweile ist Microsoft 365 in der oben beschriebenen spezifischen Ausprägung in den vom Brandenburgischen IT-Dienstleister betreuten Landesbehörden im Einsatz.

Gegen Ende des Berichtszeitraums waren zwei wesentliche Entwicklungen zu verzeichnen, die unter Umständen auch in eine Fortschreibung des Vertrags mit Microsoft für die brandenburgische Landesverwaltung einfließen könnten:

- Ein Verfahren des Europäischen Datenschutzbeauftragten gegen die Europäische Kommission zur Nutzung von Microsoft 365 durch die Kommission wurde beendet, nachdem die Kommission auf eine Verwarnung und eine Anordnung des Datenschutzbeauftragten reagierte und den Nachweis erbrachte, dass der Einsatz der Microsoft-Produkte dort rechtskonform erfolgt. Hintergrund seien sowohl Änderungen im Vertrag zur

Auftragsverarbeitung als auch in technischen Details der Verarbeitung. Wir haben den Europäischen Datenschutzbeauftragten gebeten, uns die entsprechenden Unterlagen im Rahmen der Zusammenarbeit zur Verfügung zu stellen.

- Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat seit dem vorangegangenen Berichtszeitraum selbst intensiv mit Microsoft verhandelt und mit dem Unternehmen u. a. spezifische Vertragsbedingungen für öffentliche Stellen, die Auftraggeber von Microsoft sind, abgesprochen. Ein entsprechender Abschlussbericht zu den Gesprächen liegt vor. Er zeigt die Punkte auf, die aus Sicht des Hessischen Beauftragten umzusetzen sind, damit die Nutzung von Microsoft 365 rechtskonform erfolgen kann.

Wir werden die entsprechenden Unterlagen – gemeinsam mit den Kolleginnen und Kollegen der anderen Datenschutzaufsichtsbehörden – auswerten und anschließend prüfen, welche Konsequenzen sich daraus für das Land Brandenburg ergeben.

3 Videoüberwachung öffentlich zugänglicher Räume durch Kommunen

Auch in diesem Berichtsjahr war die Videoüberwachung durch brandenburgische Städte und Gemeinden wiederholt Gegenstand unserer aufsichtsbehördlichen Beratungen und Prüfungen. Gleich in mehreren Fällen ging es um den Kameraeinsatz an Busbahnhöfen. Ziel war es u. a., Sachbeschädigungen an den Gebäuden und Straftaten auf dem Gelände zu verhindern. Außerdem beschäftigte uns die Überwachung eines geschützten Denkmals, das immer wieder Ziel von Vandalismus wurde. Die gefährdeten Objekte befanden sich im Eigentum oder Besitz der Kommunen selbst. Die Rechtslage stellt sich in solchen Fällen wie folgt dar:

Soweit die Kommunen als Ordnungsbehörden im Rahmen der nichtpolizeilichen Gefahrenabwehr auf der Grundlage des Ordnungsbehördengesetzes tätig werden, steht ihnen keine Rechtsgrundlage für die Videoüberwachung im öffentlichen Raum zur Verfügung. Die Videoüberwachung öffentlich zugänglicher Straßen und Plätze, auf denen vermehrt Straftaten drohen, ist den jeweils zuständigen Polizeibehörden im Rahmen der Gefahrenabwehr auf der Grundlage des Brandenburgischen Polizeigesetzes vorbehalten.

Beabsichtigen Städte und Gemeinden eine Videoüberwachung im Rahmen des allgemeinen Verwaltungshandelns, richtet sich deren Zulässigkeit nach § 28 Brandenburgisches Datenschutzgesetz (BbgDSG). Danach ist die Erhebung personenbezogener Daten mithilfe von optisch-elektronischen Einrichtungen (Videoüberwachung) und deren weitere Verarbeitung u. a. dann zulässig, wenn dies zum Schutz des Eigentums oder Besitzes erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen.

Nach unserer Erfahrung kann der präventive Schutz des Eigentums mit einer Videoüberwachung oftmals nicht erreicht werden. Angriffe werden sich durch den Einsatz von Kameras in der Regel nicht verhindern lassen. Ihre abschreckende Wirkung ist eher gering. Zudem treffen Täterinnen und Täter oft Vorkehrungen, um nicht erkannt zu werden, indem sie beispielsweise Masken bzw. Kapuzen tragen oder gar die Videotechnik außer Betrieb setzen.

Im Rahmen der Prüfung der Erforderlichkeit bedarf es einer konkreten Gefährdungslage. Dies lässt sich im Rahmen einer Einzelfallprüfung unter Berücksichtigung einschlägiger Vorfälle aus der Vergangenheit bewerten. Hat es erhebliche Angriffe oder Beschädigungen gegeben, empfiehlt es sich, darüber einen Nachweis zu führen – auch um später im Sinne der Rechenschaftspflicht nach Artikel 5 Absatz 2 Datenschutz-Grundverordnung (DS-GVO) die Erforderlichkeit der Maßnahme zu begründen. Aus diesem Nachweis sollte sich ergeben, wann und wo es zu welchem Ereignis gekommen ist und welcher Schaden damit verbunden war.

Zudem darf der Gemeinde kein milderes Mittel zur Verfügung stehen. Unter einem milderen Mittel versteht man Maßnahmen, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen als die Videoüberwachung. Dafür können u. a. die Sensibilisierung der Öffentlichkeit durch eingängige Plakate, eine gute Ausleuchtung oder die verstärkte Präsenz des Ordnungsamts, der Polizei bzw. eines Sicherheitsdienstes infrage kommen. Denkbar wäre auch die Einhausung baulicher Objekte oder die Einzäunung eines Geländes. Glasflächen können möglicherweise durch das Anbringen spezieller Folien gegen Graffiti und andere Beschädigungen geschützt werden. Verspricht dies im Einzelfall keinen Erfolg, muss die Gemeinde darlegen, warum solche Maßnahmen nicht ausreichen.

Hohe Hürden für Kameraüberwachung

Zulässig ist eine Videoüberwachung zudem nur dann, wenn keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. Wird beispielsweise das gesamte Areal eines Busbahnhofs überwacht, geraten zahllose Personen in den Erfassungsbereich der Kameras, die sich auf dem Gelände bewegen, um die öffentlichen Verkehrsmittel zu nutzen, oder sich dort aus anderen Gründen aufhalten. Sie geben keinen Anlass zur Überwachung und stehen in ihrer überwiegenden Mehrzahl in keinerlei Verdacht, die in Rede stehenden Taten zu begehen. Mit der Erhebung ihrer Daten durch die Videoüberwachung kann deshalb eine hohe Eingriffsintensität verbunden sein. Die Überbrückung von Wartezeiten auf dem Busbahnhof und die Kommunikation der Fahrgäste untereinander sind der Freizeit der betroffenen Personen zuzurechnen. Diese sollen sie grundsätzlich ungezwungen und frei von einem durch die Videoüberwachung möglicherweise erzeugten Überwachungsdruck verbringen können. Das Recht auf Achtung des

Privatlebens aus Artikel 7 Charta der Grundrechte der Europäischen Union fließt insofern in die Interessenabwägung ein. Eine großflächige Videoüberwachung durch die Städte und Gemeinden ist deshalb regelmäßig nicht datenschutzkonform. Dies gilt nicht nur für Busbahnhöfe, sondern für andere öffentlich zugängliche Plätze, Verkehrsflächen oder Parks. Beschränkt sich der Erfassungsbereich der Kameras ausschließlich auf die zu schützenden baulichen Anlagen und erfasst zufällige Passantinnen und Passanten im Regelfall nicht, könnte das Interesse der Gemeinde an der Videoüberwachung überwiegen.

Für die wenigen Konstellationen, in denen eine gemeindliche Videoüberwachung zulässig ist, müssen technische und organisatorische Maßnahmen nach Artikel 32 DS-GVO umgesetzt werden. Außerdem sind die Informationspflichten nach Artikel 12 ff. DS-GVO i. V. m. § 28 Absatz 2 BbgDSG zu erfüllen. Schließlich ist eine Freigabe nach § 4 BbgDSG zu erteilen. Die verantwortliche Gemeinde ist auch verpflichtet, in regelmäßigen Abständen zu überprüfen, ob die durch die Videoüberwachung vorgenommene Verarbeitung personenbezogener Daten weiterhin für die Erreichung der damit verfolgten Zwecke erforderlich ist.

Im Rahmen unserer Beratungen haben wir die Städte und Gemeinden auf diese Rechtslage hingewiesen und von einer großflächigen Videoüberwachung stets abgeraten. Soweit eine Videoüberwachung überhaupt zulässig war, konnten wir im Ergebnis unserer Prüfungen erreichen, dass die verantwortlichen Kommunen den Erfassungsbereich ihrer Kameras erheblich eingeschränkt haben.

4 Arzttermine nur über einen Dienstleister?

Ein Medizinisches Versorgungszentrum (MVZ) bot neben einer Online-Terminvereinbarung auch die telefonische Buchung von Arztterminen an. Von Letzterem machte ein Patient Gebrauch. Als er jedoch darum bat, für die weitere Dokumentation und Verwaltung seines Termins keinen Dienstleister einzuschalten, teilte das MVZ mit, ihm unter diesen Umständen keinen Behandlungsvertrag anbieten zu können. Er müsse den Dienstleister akzeptieren. Der Patient wies uns auf diesen Umstand hin; wir haben die Angelegenheit daraufhin überprüft.

Im Ergebnis stellte sich die Situation so dar, wie von dem Patienten geschildert: Zwar war es möglich, Termine telefonisch unmittelbar mit dem MVZ zu vereinbaren. Die weitere Verwaltung und Dokumentation der Termine erledigte dann aber trotzdem der Dienstleister. Datenschutzrechtlich geschah dies im Wege einer Auftragsverarbeitung nach Artikel 28 Datenschutz-Grundverordnung. In einem solchen Fall gilt die ärztliche Schweigepflicht auch für den Auftragsverarbeiter. Ein Anspruch auf eine alternative Terminverwaltung ohne dessen Einschaltung besteht unter diesen Voraussetzungen nicht. Auch ist der Einsatz des Dienstleisters nicht vom Einverständnis der Patientinnen und Patienten abhängig. Ihnen bleibt im Zweifel nur die Wahl eines anderen MVZ oder einer anderen Arztpraxis.

Den Fall haben wir zum Anlass genommen, auch das Internetangebot des MVZ zu überprüfen. Dabei stellten wir fest, dass Patientinnen und Patienten, die einen Termin vereinbaren wollten, durch das Anklicken der Online-Terminvereinbarung auf die Plattform des Dienstleisters weitergeleitet wurden. Dies war vorher nicht zu erkennen; über die Weiterleitung informierte das MVZ nicht. Nachdem sich Patientinnen oder Patienten auf einen Termin festgelegt hatten, eröffnete die Plattform nur zwei Wahlmöglichkeiten: Entweder man loggte sich in ein vorhandenes Konto ein oder registrierte ein neues Konto beim Dienstleister. Erforderlich war also ein Vertragsschluss zwischen dem Dienstleister und der Patientin oder dem Patienten. Datenschutzrechtlich lag deshalb – anders als bei der oben beschriebenen Terminverwaltung – keine Auftragsverarbeitung vor; der Dienstleister wurde bei der Online-Terminvereinbarung vielmehr eigenverantwortlich tätig. Wir konnten erreichen, dass das MVZ

sein Internetangebot so umgestaltet hat, dass die Weiterleitung auf die Plattform des Dienstleisters zwecks Online-Terminvereinbarung nunmehr von vornherein ersichtlich ist.

Außerdem haben wir den Vertrag über die Auftragsverarbeitung zwischen dem MVZ und dem Dienstleister geprüft. Entsprechend der Standard-Einstellung des Dienstleisters war darin vorgesehen, die Termindokumentation fünf Jahre lang zu speichern. Auf unsere Empfehlung hin hat das MVZ diese Frist auf ein Jahr reduziert. Einer weiteren Verkürzung stand das medizinische Erfordernis einer revisionssicheren Übertragung insbesondere nicht wahrgenommener Termine in die Patientenakte entgegen.

Schließlich konnten wir das MVZ davon überzeugen, für das Ausfüllen des Freifeldes „Anmerkungen der Gesundheitsfachkraft“ in der Termindokumentation anstelle eines Klartextes mit sensiblen Gesundheitsdaten künftig einen internen Code zu verwenden, um Risiken einer nicht erforderlichen Kenntnisnahme aufseiten des Dienstleisters zu vermindern. Solche Anmerkungen betrafen beispielsweise die konkrete, für den Termin vorgesehene Therapiemaßnahme, die Notwendigkeit der Teilnahme einer Begleitperson oder auch eine Angststörung in Bezug auf Arztbesuche.

5 Dürfen Banken Ausweise vollständig kopieren?

Regelmäßig erhalten wir Beschwerden betroffener Personen, die die Praxis von Kreditinstituten, amtliche Ausweisdokumente zur Erfüllung ihrer geldwäscherechtlichen Sorgfaltspflichten vollständig zu kopieren oder zu scannen, infrage stellen. Sie berufen sich dabei auf den Grundsatz der Datenminimierung aus der Datenschutz-Grundverordnung. Hiernach muss eine Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Die Verarbeitung irrelevanter personenbezogener Daten ist hingegen unzulässig.

Amtliche Lichtbildausweise enthalten eine Vielzahl personenbezogener Daten – wie das Lichtbild, die Körpergröße und Augenfarbe – welche für die Arbeit von Kreditinstituten zunächst irrelevant erscheinen. Folgt hieraus, dass betroffene Personen berechtigt bzw. Kreditinstitute verpflichtet sind, Kopien der Lichtbildausweise teilweise zu schwärzen?

Hierfür spricht insbesondere der Pflichtenkatalog des § 11 Absatz 1 und 4 Geldwäschegesetz (GwG). Danach sind Kreditinstitute verpflichtet, Vertragspartner, ggf. für diese auftretende Personen und wirtschaftlich Berechtigte, vor Begründung der Geschäftsbeziehung oder vor Durchführung der Transaktion zu identifizieren und hierfür konkrete personenbezogene Daten zu erheben. Das betrifft bei natürlichen Personen den vollständigen Namen, den Geburtsort, das Geburtsdatum, die Staatsangehörigkeit und die Wohnanschrift. Die Überprüfung dieser Daten erfolgt nach § 8 Absatz 2 Satz 1 und 2 sowie § 12 Absatz 1 Satz 1 Nummer 1 GwG grundsätzlich durch die Vorlage eines amtlichen Lichtbildausweises, welcher dann zu kopieren oder optisch digital zu erfassen ist. Da das Gesetz die Erhebung konkreter Daten anordnet, liegt der Schluss nahe, dass darüber hinausgehende Daten nicht erforderlich sind.

Dennoch sind Kreditinstitute berechtigt und verpflichtet, Ablichtungen amtlicher Lichtbildausweise der betroffenen Personen vollständig und ungeschwärzt zu verarbeiten. Dies folgt aus § 8 Absatz 2 Satz 2 GwG, welcher nicht etwa regelt, wie mit den personenbezogenen Daten aus § 11 Absatz 4 GwG zu verfahren ist, sondern eine

eigenständige spezialgesetzliche Rechtsgrundlage darstellt. Zwar ergibt sich die Vollständigkeit der Ablichtung nicht unmittelbar aus dem Wortlaut der Norm, allerdings stellt der Gesetzgeber in seiner Gesetzesbegründung zur Umsetzung der Vierten Geldwäscherichtlinie[31] ausdrücklich auf die Notwendigkeit der „Fertigung von vollständigen Kopien“ ab. Auch die Kommentarliteratur verneint einen Konflikt zwischen dem Grundsatz der Datenminimierung und der vollständigen Ablichtung. Sie lehnt ein Recht bzw. eine Pflicht zur Schwärzung in der Folge ab. Zudem verlangt die Bundesanstalt für Finanzdienstleistungsaufsicht, welche die Aufsicht über Kreditinstitute führt, die vollständige Ablichtung von Vorder- und Rückseite des Lichtbildausweises und fordert, dass „sämtliche Angaben gut erkennbar sein müssen“.[32]

31 Deutscher Bundestag, Gesetzentwurf der Bundesregierung für ein Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen, Drucksache 18/11555 vom 17. März 2017, Seite 114.

32 Bundesanstalt für Finanzdienstleistungsaufsicht, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (Stand: März 2025), Seite 82.

6 Einsatz von Gesichtserkennung am Flughafen BER

Am Flughafen Berlin Brandenburg (BER) gibt es für Fluggäste die Möglichkeit des so genannten Hands-Free Check-In. Gemeint ist damit der kontaktlose Zutritt zur Sicherheitskontrolle und zu ausgewählten anderen Flughafenbereichen per Gesichtserkennung und ohne das Vorzeigen bzw. Einscannen der Bordkarte. Auch Gepäckbanderolen können hierüber an bestimmten Stationen selbst ausgedruckt werden. Nach Darstellung des Verantwortlichen handelt es sich um eine reine Komfortfunktion für Passagierinnen und Passagiere. Die Nutzung ist freiwillig. Sie ersetzt keine Sicherheitskontrollen und dient auch nicht der Beeinflussung oder Steuerung des Passagierstroms im Flughafengebäude.

Voraussetzung für die Inanspruchnahme des Services ist zunächst, dass die Nutzerin bzw. der Nutzer auf dem Smartphone eine App installiert und sich dort registriert. Anbieter der App ist ein bayerisches Unternehmen. Im Zuge der Registrierung ist u. a. ein Frontalbild (Selfie) mit dem Smartphone aufzunehmen. Hieraus wird eine so genannte Referenzdatei berechnet, die Grundlage für den späteren Abgleich mit einem aktuellen Gesichtsbild ist. Sie wird in verschlüsselter Form auf dem Smartphone gespeichert. Entscheidet sich die Nutzerin bzw. der Nutzer, für einen bestimmten Flug die Komfortfunktion zu verwenden, lädt sie bzw. er die Bordkarte in die App. Diese wird anschließend zusammen mit der Referenzdatei zum bayerischen Anbieter übertragen und dort verschlüsselt abgelegt. 12 Stunden vor dem Abflug lädt der Anbieter die Referenzdatei in entschlüsselter Form in den Arbeitsspeicher des unter seiner Verantwortung betriebenen Servers; sie steht damit für die Gesichtserkennung zur Verfügung.

Am Flughafen BER existieren zwei Arten von Terminals, an denen der Dienst genutzt werden kann. Den ersten Typ betreibt das bayerische Unternehmen, das auch die App anbietet, selbst. Hier muss die Passagierin bzw. der Passagier eine Lichtschranke durchqueren und damit die im Terminal verbaute Kamera aktivieren. Sie nimmt anschließend ein aktuelles Foto des Gesichts auf. Aus dem Foto wird vor Ort eine Referenzdatei berechnet, verschlüsselt zum App-Anbieter geschickt und dort mit den Referenzdateien aus der Registrierung aller

derjenigen Nutzerinnen und Nutzer verglichen, die den Dienst gebucht und ihre Bordkarte hochgeladen haben. Bei Übereinstimmung liefert der Dienst die zu der gefundenen Person gehörende Bordkarteninformation zurück, womit der Zutritt zur Sicherheitskontrolle bzw. ausgewählten Bereichen gestattet wird. Den zweiten Typ von Terminals betreibt ein anderes Unternehmen. Nachdem die Nutzerin bzw. der Nutzer die Kamera über das Terminaldisplay eingeschaltet hat, ermittelt das System per Video ein geeignetes Gesichtsbild. Sollte dies nicht gelingen, stoppt die Videoaufnahme. Ansonsten wird das Bild verschlüsselt zum bayerischen Unternehmen gesendet, dort die Referenzdatei erzeugt und mit denjenigen aus der Registrierung wie im ersten Fall verglichen. Bei einer Übereinstimmung wird die Bordkarteninformation zurückgeliefert und für den Druck der Gepäckbanderole verwendet. Spätestens 12 Stunden nach dem geplanten Abflug werden alle Daten beim bayerischen Anbieter gelöscht.

Per Gesichtserkennung zu mehr Komfort?

Aus datenschutzrechtlicher Sicht ist festzuhalten, dass für die beschriebenen Prozesse zwei verschiedene Unternehmen verantwortlich sind: Die Flughafen Berlin Brandenburg GmbH ist verantwortlich für den Betrieb der Terminals im Flughafengebäude, die Erfassung der Gesichtsbilder vor Ort, die Übermittlung zum bayerischen Anbieter und die Bordkartenverarbeitung. Sie ist auch Auftraggeberin entsprechender Auftragsverarbeitungen. Das Unternehmen in Bayern ist hingegen verantwortlich für die App auf dem Smartphone, die Buchung des Dienstes durch Kundinnen und Kunden sowie den Abgleich der Referenzdateien. Es verfolgt eigene Geschäftszwecke. Die zu Grunde liegende Technologie soll unabhängig von der Nutzung am Flughafen BER auch an anderen Orten für das komfortable Einchecken Verwendung finden, z. B. in Hotels, Spaßbädern oder Freizeitparks. Insofern beschränkt sich auch die Zuständigkeit unserer Dienststelle auf die Datenverarbeitung am Flughafen.

Derzeit prüfen wir, inwiefern die beschriebene Verarbeitung personenbezogener Daten am Flughafen BER den Anforderungen der Datenschutz-Grundverordnung (DS-GVO) gerecht wird und welche technischen bzw. organisatorischen Maßnahmen für einen rechtskonformen Betrieb umzusetzen sind. Hierzu stehen wir mit den Verantwortlichen der Flughafen Berlin Brandenburg GmbH im Austausch. Schwerpunkte der Untersuchungen sind u. a. Fragen der Kategorisierung der personenbezogenen Daten als biometrische Daten

i. S. v. Artikel 4 Nummer 14 DS-GVO und die Rechtsgrundlagen der Datenverarbeitung (im konkreten Fall die Einwilligung und deren ausdrückliche Erteilung). Weiterhin befassen wir uns mit der Verarbeitung von Daten unbeteiligter Dritter (z. B. im Hintergrund von Bildaufnahmen befindliche Personen) sowie der Verbesserung der Transparenz der Datenverarbeitung durch Information betroffener Personen. Im Rahmen eines Vor-Ort-Besuches haben wir der Flughafen Berlin Brandenburg GmbH einige Hinweise zu diesen Punkten gegeben, die zum Teil bereits umgesetzt wurden.

7 Datenschutz am Empfang und in Servicezentren

Wer kennt es nicht, dieses ungute Gefühl, am Empfangstresen einer Arztpraxis oder bei der Beratung im Servicezentrum einer Versicherung oder einer Behörde über persönliche Details zu sprechen und zu wissen, dass Personen im nahen Wartebereich oder am Tisch nebenan diese Informationen zur Kenntnis nehmen und ggf. weitertragen können? Die Wahrung der Vertraulichkeit spielt für viele Patientinnen und Patienten, Kundinnen und Kunden sowie Bürgerinnen und Bürger in diesem Zusammenhang eine große Rolle. Sie kritisieren oftmals zu Recht, dass Verantwortliche zu unbekümmert mit diesem Thema umgehen.

So erreichten uns im Berichtszeitraum erneut einige Beschwerden und Anfragen, in denen betroffene Personen ihren Befürchtungen Ausdruck verliehen und unzureichende Maßnahmen zum Schutz ihrer Rechte monierten. In mehreren Fällen machten sie uns darauf aufmerksam, dass in den von ihnen besuchten Arzt- oder Physiotherapiepraxen der Abstand zwischen Empfang und Wartebereich zu gering oder keine räumliche Abtrennung vorhanden war. Dialoge mit der Empfangskraft, bei denen der Name, das Geburtsdatum und gesundheitliche Beschwerden genannt oder sogar der Hergang eines Unfalls beschrieben werden sollten, offenbarten sensible Informationen für Unbeteiligte. In einem speziellen Fall kam hinzu, dass der Empfangstresen mehrfach für einige Minuten unbesetzt war und der Bildschirm des Praxiscomputers auch von nicht befugten Personen eingesehen werden konnte.

In Bezug auf die Servicestelle einer Krankenversicherung beschwerte sich ein Kunde bei uns, dass er bereits eineinhalb Jahre zuvor regelmäßig vor Ort war und dabei Gespräche anderer Versicherter oder ihrer Angehörigen mit dem Servicepersonal mitbekam. Dabei erfuhr er ungewollt allerlei zu Krebserkrankungen betroffener Personen, zu Versicherungsschulden, Einkommenshöhen und möglichen Tilgungsraten oder zu Privatangelegenheiten der Beschäftigten. Der „Schutz“ zwischen dem Warte- und dem Beratungsbereich bestand nach seiner Schilderung aus zwei Blumenkübeln. Nach einer mündlichen Beschwerde direkt bei der Leitung der Servicestelle erhielt er eine Entschuldigung mit dem Hinweis auf die noch zu vervollständi-

gende Büroeinrichtung und die Möglichkeit, vertrauliche Gespräche in einem Nebenraum zu führen. Ein erneuter Besuch im Berichtszeitraum zeigte jedoch, dass sich in den seit der ersten Kritik vergangenen Monaten nichts Wesentliches verändert hatte. Daraufhin informierte er unsere Behörde.

Aus datenschutzrechtlicher Sicht sind Verantwortliche verpflichtet, Artikel 32 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) einzuhalten. Sie müssen danach unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Nach Buchstabe b der genannten Regelung ist u. a. die Vertraulichkeit im Zusammenhang mit der Verarbeitung personenbezogener Daten sicherzustellen.

Wer hört mit?

Werden wie in den vorliegenden Fällen Gesundheitsdaten – eine besondere Kategorie personenbezogener Daten gemäß Artikel 9 Absatz 1 DS-GVO – verarbeitet, können die Risiken durch eine unbefugte Offenbarung, Kenntnisnahme und ggf. Nutzung dieser Daten besonders schwer wiegen. Inhaberinnen und Inhaber von medizinischen Einrichtungen sowie Organisationen, die Dienstleistungen im Gesundheitsbereich erbringen, müssen deshalb besonderes Augenmerk und spezielle Sorgfalt auf die Umsetzung geeigneter und angemessener Datenschutzmaßnahmen richten. Finanzielle Erwägungen können bei der Auswahl und Umsetzung der Maßnahmen zwar eine Rolle spielen – jedoch nur insoweit, als dass aus mehreren gleich geeigneten Maßnahmen eine kostengünstige genutzt werden kann. Wegen fehlender Finanzmittel auf erforderliche Maßnahmen zu verzichten, ist genauso wenig eine Option wie der Hinweis des Arztes gegenüber einer Beschwerdeführerin, sie würde sich durch die Einsichtnahme in fremde Patientendaten auf einem ungeschützten Monitor strafbar machen.

In den uns vorliegenden Anfragen und Beschwerdefällen haben wir den Verantwortlichen dringend empfohlen, durch bauliche, technische oder organisatorische Maßnahmen die Vertraulichkeit sicherzustellen. Wenn räumlich separate Empfangs- und Wartebereiche nicht zu realisieren sind, können beispielsweise transportable Zwi-

schenwände eine optische und akustische Abgrenzung ermöglichen. Abstandsgebote für Patientinnen und Patienten vor dem Tresen, Diskretionszonen, geschlossene Türen und Fenster, eine generelle Reduzierung der Gesprächslautstärke oder leise Hintergrundmusik erschweren Unbefugten das Mithören. Hinweise darauf, dass vertrauliche Daten nicht am Empfang preisgegeben werden müssen oder hierfür auch ein separater Raum aufgesucht werden kann, zeigen Patientinnen und Patienten bzw. Kundinnen und Kunden, dass die Verantwortlichen ihre Befürchtungen ernst nehmen. Vertrauen und Zufriedenheit entstehen in diesem Fall durch angemessenes Handeln. Hierzu gehört auch die Selbstverständlichkeit, bei Abwesenheit den Bildschirm des Computers zu sperren und durch geeignete Aufstellung oder Sichtschutzfolie Einblicke unbefugter Personen auf den Monitor und eine Kenntnisnahme der Daten anderer Patientinnen und Patienten zu verhindern.

In keinem Fall wiederholten sich die Beschwerden. Wir gehen deshalb davon aus, dass die Verantwortlichen unseren Empfehlungen gefolgt sind. Bei der oben erwähnten Servicestelle einer Krankenversicherung mussten wir durch einen Vor-Ort-Besuch mit Nachdruck auf die räumliche Umgestaltung drängen. Sie dauerte insgesamt etwas länger, da auch brand- und arbeitsschutzrechtliche Aspekte zu berücksichtigen waren.

8 20. Jahrestreffen mit den behördlichen Datenschutzbeauftragten

Auch im Berichtsjahr führten wir das regelmäßige Treffen mit den Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Gemeinden durch. Intention dieser ganztägigen Veranstaltung ist es, die Datenschutzbeauftragten bei der Erfüllung ihrer anspruchsvollen Aufgaben nach Artikel 39 der Datenschutz-Grundverordnung zu unterstützen und den Informationsaustausch zu fördern. Darüber hinaus erhalten aber auch wir einen aktuellen Einblick in die Problemfelder der kommunalen Verwaltungen und können so entsprechende Hilfestellungen geben sowie die Datenschutzbeauftragten über aktuelle Entwicklungen informieren.

Einer der Schwerpunkte der Veranstaltung war die Videoüberwachung durch öffentliche Stellen. Wir verzeichnen ein zunehmendes Interesse kommunaler Verantwortlicher, insbesondere öffentlich zugängliche Räume, wie z. B. Fahrradstellplätze oder Busbahnhöfe, zu überwachen. Dies ist jedoch nur unter engen rechtlichen Voraussetzungen zulässig.[33] Da die Datenschutzbeauftragten immer öfter den Einsatz Künstlicher Intelligenz durch öffentliche Stellen datenschutzrechtlich bewerten müssen, wurde auch dieses Thema lebhaft diskutiert. Der aktuelle Stand der Einführung von Microsoft 365 in der Landes- und Kommunalverwaltung und die hierfür geltenden datenschutzrechtlichen Anforderungen waren ebenso Gegenstand der Erörterungen wie verschiedene Fragestellungen und Entwicklungen aus dem Umfeld des Onlinezugangsgesetzes.[34]

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

---

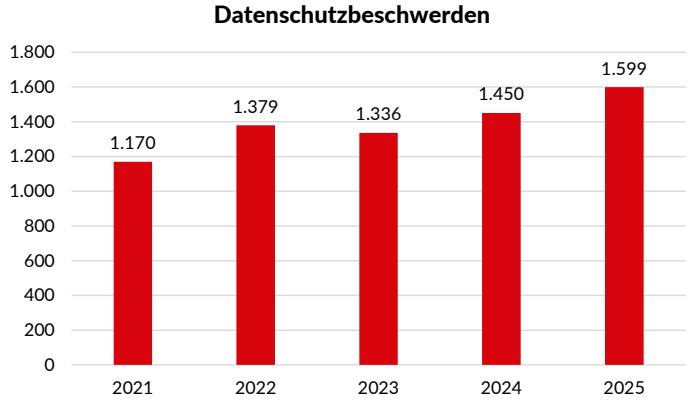
33 Siehe A V 3.

34 Siehe A V 2 und A V 1.

VI Zahlen und Fakten

1 Beschwerden

Im Berichtszeitraum gingen bei der Landesbeauftragten 1.599 schriftliche Beschwerden gemäß Artikel 77 Datenschutz-Grundverordnung ein. Damit hat sich die Anzahl gegenüber dem Vorjahr um mehr als 10 % 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.



Außerdem erreichte uns eine Reihe von Eingaben, deren Datenschutzbezug fraglich und zunächst zu prüfen war. Die Absenderinnen und Absender hatten diese breit an verschiedene Behörden gestreut, zum Teil waren 20 Stellen gleichzeitig angeschrieben worden. Beispielsweise erhielten wir im Berichtsjahr 231 E-Mails eines einzelnen Beschwerdeführers, von denen lediglich 8 in unsere Zuständigkeit fielen und in die Statistik eingingen.

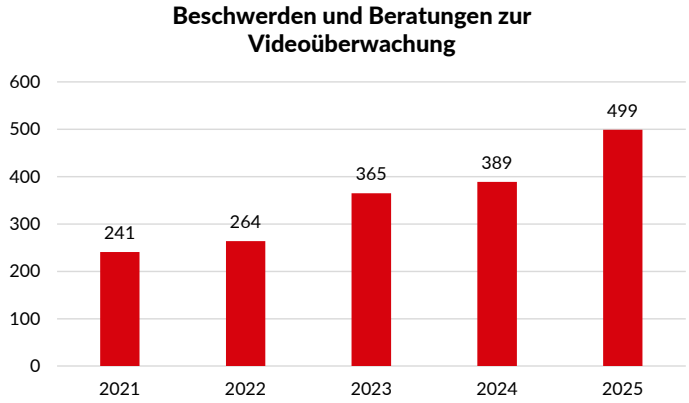
2 Beratungen

Neben Beschwerden registrierte die Landesbeauftragte im Berichtsjahr auch 477 Anfragen zu Datenschutzthemen, was einen leichten Anstieg gegenüber dem Vorjahr bedeutet. Sie unterstützte betroffene Personen, Verantwortliche im öffentlichen und nicht öffentlichen Bereich sowie die Landesregierung bei Rechtsetzungsverfahren durch schriftliche Stellungnahmen, Hinweise und Anmerkungen. Hinzu kommt eine Vielzahl telefonischer Anfragen und Beratungen, die nicht statistisch erfasst werden.

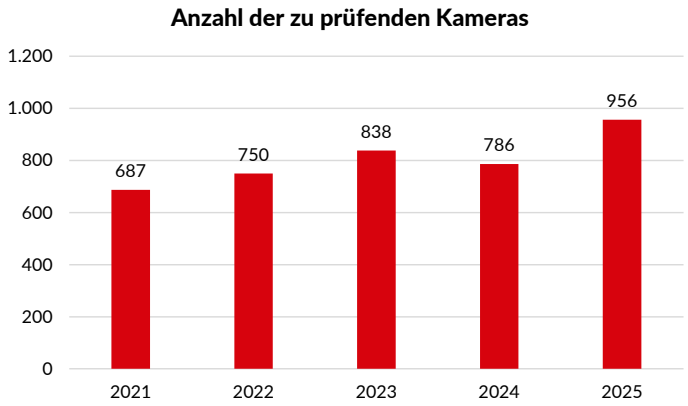
3 Videoüberwachung: Beschwerden und Beratungen

Im Berichtsjahr stellte die Landesbeauftragte erneut einen Anstieg von Beschwerden und Beratungsanfragen fest, die sich auf die Videoüberwachung durch Privatpersonen, Unternehmen und öffentliche Stellen bezogen. Ähnlich wie im Vorjahr beschwerten sich Bürgerinnen und Bürger vorwiegend über in der Nachbarschaft installierte Videokameras. In der Regel erwecken diese Kameras den Eindruck, weitreichende Einblicke in private Rückzugsorte wie Gärten, Terrassen oder Wohnhäuser zu ermöglichen. Darüber hinaus fühlen sich oft auch Passantinnen und Passanten sowie andere Verkehrsteilnehmerinnen und -teilnehmer im öffentlichen Raum zu Unrecht beobachtet. Weitere wesentliche Schwerpunkte unserer Tätigkeit waren die datenschutzrechtliche Überprüfung von Videokameras in Freizeitstätten wie auf Campingplätzen, auf Fahrgastschiffen oder in Fitnessstudios. Hinzu kamen intensive Beratungen kommunaler Stellen zu Anforderungen für eine rechtmäßige Videoüberwachung, beispielsweise an Busbahnhöfen und an vermüllten Orten.

Im Jahr 2025 erreichten uns 431 Beschwerden. Verglichen mit dem Vorjahr, in dem es 330 Beschwerden waren, ist somit ein erheblicher Zuwachs zu verzeichnen. Darüber hinaus führten wir 68 Beratungen durch (nach 59 Beratungen im Vorjahr).

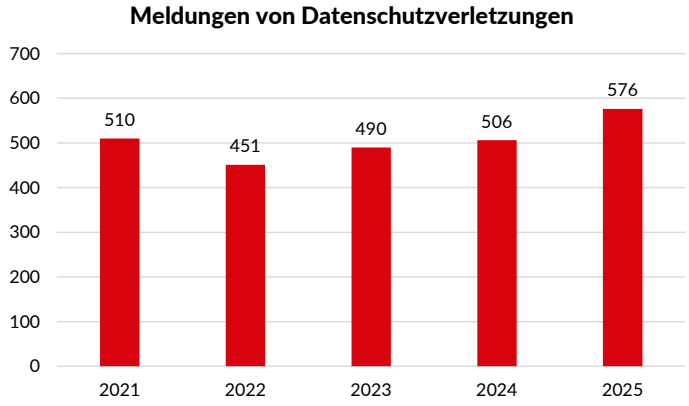


Da eine datenschutzrechtliche Bewertung einer Videoüberwachung stets eine Einzelfallprüfung erforderlich macht, ist jede Kamera einzeln auf ihre rechtliche Zulässigkeit sowie auf technisch-organisatorische Maßnahmen zu kontrollieren. Im Berichtsjahr überprüften wir 956 Videokameras, in dem Jahr zuvor waren es 786.



4 Meldungen von Datenschutzverletzungen

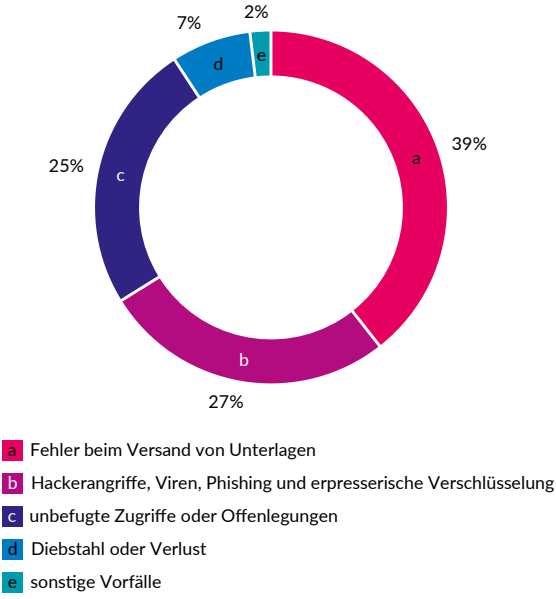
Artikel 33 Datenschutz-Grundverordnung verpflichtet den Verantwortlichen, eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, an die zuständige Datenschutzaufsichtsbehörde zu melden. Die Meldepflicht entfällt nur, 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 576 Meldungen von Datenschutzverletzungen. Das bedeutet eine Steigerung gegenüber dem Vorjahr, in welchem 506 Meldungen eingingen. Die Datenschutzverletzungen passierten sowohl im öffentlichen (271 Meldungen) als auch im nicht öffentlichen Bereich (305 Meldungen). Beachtlich ist, dass die Zahl der Meldungen durch öffentliche Stellen geringfügig sank, während die Zahl der Meldungen durch nicht öffentliche Stellen um ca. 30 % stieg. Allerdings ge-

ben diese Zahlen nur Auskunft über die Meldungen und nicht über die tatsächliche Zahl der Datenschutzverletzungen.

Art der gemeldeten Datenschutzverletzung



Sehr viele Meldungen betrafen den Fehlversand von Unterlagen (insgesamt 227 Fälle). Hiervon umfasst waren sowohl Fehlkuvertierungen von Briefpost, versehentlicher E-Mail-Versand an einen offenen Verteilerkreis, Namensverwechslungen oder die Beifügung von Unterlagen unbeteiligter Dritter. Eine erhebliche Anzahl der gemeldeten Datenschutzverletzungen beruhte auf technischen Mängeln (154 Fälle) und bezog sich insofern auf z. B. Hackerangriffe, Virenbefall, Phishing und erpresserische Verschlüsselungen von Datensätzen. 142 Fälle betrafen unbefugte Zugriffe oder Offenlegungen bis hin zu unzulässigen Veröffentlichungen. Ein Abhandenkommen physischer Datenträger, etwa durch Diebstähle aus Räumen des Verantwortlichen oder durch Verlust auf dem Postweg, wurde der Landesbeauftragten in 42 Fällen gemeldet. Lediglich 11 Meldungen wurden der Kategorie „Sonstiges“ zugeordnet.

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 in 15 Fällen etwa bei erfolgreichen Hackerangriffen, in deren Verlauf Datenbestände verschlüsselt und so dem Zugriff der eigentlich Befugten entzogen wurden, beim Verlust eines Wählerverzeichnisses in einem Wahllokal, bei einer unvollständigen Datenmigration im Rahmen eines Updates sowie bei der Weitergabe personenbezogener Daten wahlberechtigter Kinder und Jugendlicher innerhalb einer Stadtverwaltung.

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 2 Warnungen, 14 Verwarnungen und 2 Anordnungen aus, wobei sich 3 Verwarnungen gegen öffentliche Stellen richteten. Hinzu kommen die im folgenden Abschnitt behandelten Bußgeldverfahren.

5.2 Geldbußen

Im Berichtszeitraum wurden der Bußgeldstelle der Landesbeauftragten 40 Sachverhalte wegen Verstößen gegen datenschutzrechtliche Vorgaben zur Kenntnis gegeben. Die Verfahren wurden zu einem großen Teil, nämlich in 32 Fällen, von den zuständigen Polizeibehörden oder Staatsanwaltschaften an die Bußgeldstelle weitergeleitet. Insgesamt 8 Sachverhalte haben aufsichtsbehördlich tätige Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten oder andere Aufsichtsbehörden mangels eigener Zuständigkeit an die Bußgeldstelle abgegeben.

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

Gegenüber 9 Verantwortlichen verhängte die Landesbeauftragte wegen der festgestellten datenschutzrechtlichen Verstöße insgesamt 25 Geldbußen. Ihre Gesamtsumme betrug knapp 109.000 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 2.654 einzelne Benachrichtigungen aus dem Binnenmarkt-Informationssystem, hinsichtlich derer sie das Ergreifen von Maßnahmen zu prüfen hatte.

Von allen eingegangen Benachrichtigungen prüften wir gemäß Artikel 56 DS-GVO in 1.215 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. In 35 Fällen initiierten wir aufgrund eingegangener Beschwerden selbst eine solche Prüfung. 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 69 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 Niederlassung in Brandenburg hatten und keine erheblichen Auswirkungen auf Brandenburgerinnen und Brandenburger festzustellen waren.

In 1.313 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 abermals das gegenseitige Amtshilfeverfahren zwischen der Nationalen Kommission für den Datenschutz (CNPD) des Großherzogtums Luxemburg und der Landesbeauftragten. Dies 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 verfügte das Unternehmen im Berichtsjahr über eine unselbstständige Zweigniederlassung, sodass wir die sachnächste Aufsichtsbehörde innerhalb Deutschlands gemäß § 19 Absatz 2 Satz 1 Bundesdatenschutzgesetz waren. Beschwerden gegen PayPal wurden deswegen von anderen deutschen Aufsichtsbehörden weitergereicht und bei uns zentralisiert. Diese wurden im Rahmen der gegenseitigen Amtshilfe an die CNPD übermittelt und im engen Austausch bearbeitet.

Im Berichtsjahr gingen zu PayPal ca. 100 Beschwerden und weitere Anfragen bei der Landesbeauftragten ein. Damit ist die Zahl wieder angestiegen, im Vergleich zum Vorjahr hat sie sich mehr als verdoppelt.

Durch den Umzug der bisher in Brandenburg ansässigen Zweigniederlassung des Unternehmens PayPal nach Berlin geht die Zuständigkeit im folgenden Berichtszeitraum auf die Berliner Beauftragte für Datenschutz und Informationsfreiheit über.

7 Förmliche Begleitung von Rechtsetzungsvorhaben

Aus den zahlreichen Beratungen ist die Begleitung rechtsetzender Maßnahmen durch die Landesbeauftragte besonders hervorzuheben. Insgesamt wurden wir im Berichtszeitraum 31 Mal an der Erstellung oder Änderung von Gesetzen, Verordnungen, Satzungen oder Verwaltungsvorschriften beteiligt, prüften die vorgelegten Entwürfe und nahmen in aller Regel Stellung.

Die rechtliche Grundlage zur Beteiligung der Landesbeauftragten folgt aus § 18 Absatz 5 Satz 1 Brandenburgisches Datenschutzgesetz. Danach ist sie 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 Netzwerkspeicher des Staatsschutzes schutzlos im Internet

Die Abteilung Zentraler Staatsschutz/Terrorismusbekämpfung im Landeskriminalamt kümmert sich um die Analyse und Auswertung aller staatsschutzrelevanten Delikte im Land Brandenburg und führt Ermittlungsverfahren bei Landes-, Friedens- und Hochverrat sowie in Fällen der Bildung einer terroristischen Vereinigung. In diesem Zusammenhang sammeln die dortigen Beschäftigten auch große Mengen an personenbezogenen oder personenbeziehbaren Daten, z. B. aus öffentlich zugänglichen Bereichen des Internets. Sie recherchieren entweder selbst oder erhalten die Daten von anderen, etwa vom Bundeskriminalamt. Zur Ablage dieser Daten hat das Landeskriminalamt einen eigenen, vom internen Polizeinetz getrennten Netzwerkspeicher eingerichtet.

Im Berichtszeitraum informierte uns die Polizei in einer als vorsorglich gekennzeichneten Meldung gemäß § 29 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) über die Verletzung der Sicherheit personenbezogener Daten bei einem polizeilichen, im Internet erreichbaren Network Attached Storage (NAS). Die dort installierte Software diente zum damaligen Zeitpunkt auch der elektronischen Entgegennahme von Bürgerhinweisen zu einem Brand mit zwei Toten. Ein Nutzer hatte der Polizei zuvor gemeldet, dass über den Verweis auf das Hinweisportal, der in einer Pressemitteilung verbreitet wurde, jedermann die Anmeldeseite des NAS-Administrators aufrufen könne. Die Polizei teilte mit, eine Datenschutzverletzung bzw. ein Informationssicherheitsvorfall sei zu diesem Zeitpunkt nicht erkennbar, eine detaillierte Bewertung des Falles werde aber noch erfolgen und ggf. entsprechend nachberichtet.

Bei der Untersuchung stellte sich zunächst heraus, dass es sich bei dem in der Meldung erwähnten System um den oben beschriebenen Netzwerkspeicher der Abteilung Staatsschutz des Landeskriminalamts handelte, der zum damaligen Zeitpunkt auch als Speicher für Bürgerhinweise eingesetzt wurde. Im Gegensatz zur Ersteinschätzung des Vorfalls zeigte sich in der weiteren Analyse aber, dass es zu gravierenden Versäumnissen bei der Umsetzung technischer und organisatorischer Maßnahmen gekommen war, die die Vertraulichkeit,

Integrität und Verfügbarkeit der gespeicherten Daten bedrohten. Außerdem warf der Fall ein Licht auf den mangelnden Überblick der Polizei über die von den einzelnen Dienststellen unter eigener Ägide betriebenen Systeme und damit einhergehend auf den Sicherheitszustand der von der Polizei betriebenen Hard- und Software und der verarbeiteten hochsensiblen Daten insgesamt.

Es zeigte sich nämlich, dass der Netzwerkspeicher ohne Firewall oder weiteren Schutz vermutlich bereits seit 2021 mittels eines DSL-Anschlusses des Landeskriminalamts direkt mit dem Internet verbunden war. Die Beschaffung und der Betrieb der entsprechenden Informationstechnik erfolgten eigenständig durch das Landeskriminalamt. Zwar war das Login des Administrators mit einem ausreichend langen Passwort geschützt und seine Standardzugriffsrechte eingeschränkt. Festgestellt wurde jedoch, dass das NAS-Betriebssystem zum Zeitpunkt der o. g. Meldung bereits seit vielen Monaten nicht aktualisiert worden war. Während dieses Zeitraums hatte der Hersteller für das betroffene Modell Informationen zu einer Reihe von Sicherheitslücken veröffentlicht, von denen mindestens zwei als kritisch und eine als hoch risikoreich eingestuft waren. Risikoverstärkend kam hinzu, dass das NAS zu einem späteren Zeitpunkt mit einem Funknetz verbunden wurde, das ebenfalls unsicher konfiguriert war und damit ein weiteres mögliches Einfallstor für unberechtigte Zugriffe auf das NAS bot. Ein entsprechender, unbemerkter Zugriff durch unbefugte Dritte aus dem Internet auf die gespeicherten Daten konnte daher nicht ausgeschlossen werden.

Sorglosigkeit gefährdet Sicherheit

Weder für die Datenverarbeitungen unter Nutzung des NAS noch für das verbundene Funknetz wurden die vorgeschriebenen Freigabeprozesse ordnungsgemäß durchlaufen. Datenschutzrechtlich erforderliche Dokumente wie ein Verzeichnis der Verarbeitungstätigkeiten oder ein Sicherheitskonzept lagen nicht vor. Die Systemprotokolle des NAS gaben keine Auskunft darüber, welche Daten wann von wem erstellt, gelesen, bearbeitet oder gespeichert wurden. Im Ergebnis war es daher nicht möglich, einen Zugriff unberechtigter Personen auszuschließen.

Eine Verbindung des Netzwerkspeichers zum geschützten internen Polizeinetz bestand zwar zu keinem Zeitpunkt. Auch handelte es sich bei dem größten Teil der betroffenen personenbezogenen Daten um öffentlich zugängliche Daten aus dem Internet. Allerdings

wurden daneben auch ein Passwort zu einem Server des Bundeskriminalamts in unverschlüsselter Form und weitere nicht öffentliche, hochsensible Daten auf dem Speicher gesichert – diese hätten ausschließlich im internen Polizeinetz verarbeitet werden dürfen. Die datenschutzrechtliche Sensibilität sowohl der öffentlichen als auch der nicht öffentlichen Daten ergibt sich aus dem jeweiligen Sachzusammenhang. Grundsätzlich kann aber schon allein die Tatsache, dass die Staatsschutzabteilung des Landeskriminalamts diese Daten gespeichert hat und damit ein polizeiliches Interesse zu erkennen gibt, selbst bei öffentlich zugänglichen Daten zu einer Erhöhung der Risiken für die Rechtsgüter der betroffenen Personen führen. Dies gilt umso mehr für Daten, die niemals auf dem NAS mit Internetzugang hätten gespeichert werden dürfen.

Die Polizei ist nach den datenschutzrechtlichen Vorschriften verpflichtet, ihre Informationssicherheit nach dem Stand der Technik auszugestalten. Die internen Vorgaben und Verfahren zur Inbetriebnahme von Informations- und Kommunikationsdiensten, die über die Jahre erneuert und an die technischen Gegebenheiten angepasst worden sind, enthalten auch detaillierte Bestimmungen zum Vorgehen bei der Einführung oder bei Änderungen von IT-Services. Insbesondere können damit die Anforderungen aus den hier maßgeblichen Standards des Bundesamts für Sicherheit in der Informationstechnik grundsätzlich umgesetzt werden. Es ist allerdings festzustellen, dass diese Vorgaben die vorliegende Datenschutzverletzung nicht verhinderten, da die in Rede stehende IT-Technik unter Umgehung des Anforderungsmanagements ohne ordnungsgemäßen Freigabeprozess und – davon muss ausgegangen werden – mit Wissen und Billigung der jeweiligen lokalen Leitungspersonen beschafft und betrieben wurde. Dies blieb offenbar auch beim Informationssicherheitsmanagement der Polizei unbemerkt.

Im Ergebnis war festzustellen, dass es über einen längeren Zeitraum Mängel bei der Umsetzung der Informationssicherheit im Polizeipräsidium gab, wodurch sich das Risiko, dass unbefugte Dritte Zugang zu hochsensiblen personenbezogenen Daten erlangen, deutlich erhöhte. Diese Mängel hat die Landesbeauftragte gemäß § 36 Absatz 2 BbgPJMDSG beanstandet. Um ähnliche Vorfälle künftig zu vermeiden, wurden folgende Maßnahmen empfohlen:

- Umsetzung zentral kontrollierbarer Internetzugänge für die Polizeidienststellen,

- Überprüfung und ggf. Überarbeitung der Befugnisse der lokalen Informationssicherheitskoordinatoren,

- Durchführung spezieller Sensibilisierungsveranstaltungen und Datenschutzschulungen für Führungskräfte der Polizei,

- Fortschreibung des Informationssicherheitskonzeptes der Polizei dahingehend, dass sämtliche im Polizeipräsidium verwendeten Betriebsmittel und Geräte erfasst sowie entsprechend der Vorgaben behandelt werden.

Die Polizei hat unabhängig von der Beanstandung erkannt, dass sie hinsichtlich der Kontrolle der Informationssicherheit in den einzelnen Dienststellen verstärkt Maßnahmen ergreifen muss. Dazu hat sie ein Konzept zur Implementierung zentral kontrollierbarer Internetzugänge für die ganze Behörde erstellt. Parallel erarbeitet sie grundlegende Regelungen für den strategischen und operativen Datenschutz und die Informationssicherheit. Zudem werden die Aufgaben der für die Informationssicherheitskoordination, die Digitalisierungskoordination (eine neu geschaffene Rolle) und das Datenschutzmanagement in den Dienststellen zuständigen Personen konkretisiert und abgegrenzt. Fachaufsicht und Kommunikationswege werden präzisiert. Außerdem wird das Managementwerkzeug für das Rahmensicherheitskonzept neu aufgestellt, um zu einer besseren, prozessorientierten Umsetzung des IT-Grundschutzes nach den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik zu gelangen.

Wir begrüßen diese Maßnahmen der Polizei und werden uns über deren Umsetzung berichten lassen. Nachholbedarf besteht gleichwohl weiterhin bei speziell auf Führungskräfte ausgerichteten Schulungs- und Sensibilisierungsmaßnahmen zu Datenschutz und Informationssicherheit. Dies hat die Landesbeauftragte gegenüber dem Polizeipräsidenten deutlich gemacht und behält sich kritische Nachfragen vor.

2 Speicherung im Schengener Informationssystem

Im Berichtsjahr erreichte uns die Beschwerde eines pakistanischen Staatsbürgers zu einer von ihm als unrechtmäßig angesehenen Personenausschreibung im Schengener Informationssystem (SIS). Dieses dient den Sicherheitsbehörden der sogenannten Schengener Staaten[35] zur automatisierten Personen- und Sachfahndung innerhalb des Schengen-Raums. Der Beschwerdeführer hielt sich in Portugal auf und hatte dort einen Antrag auf Aufenthaltserlaubnis bei der für Fragen des legalen Aufenthalts zuständigen Agentur für Integration, Migration und Asyl (Agência para a Integração, Migrações e Asilo, AIMA) gestellt. Der Aufenthaltstitel wurde jedoch unter Hinweis auf den SIS-Eintrag einer brandenburgischen Ausländerbehörde versagt. Der Betroffene, der sich bereits geraume Zeit in Portugal aufhielt, konnte sich nicht erklären, weshalb eine Ausschreibung im SIS zu ihm bestand. Er war bereits mehrfach erfolglos mit Löschungsersuchen an die deutsche Behörde herangetreten, bevor er sich schließlich mit der Bitte an uns wandte, ihn dabei zu unterstützen.

Die Sachverhaltsaufklärung war langwierig und wurde dadurch erschwert, dass ein Teil der übersandten Unterlagen in portugiesischer Sprache verfasst war. Unsere Recherchen bei der zuständigen Ausländerbehörde ergaben, dass gegen den Betroffenen keine polizeiliche Personenausschreibung zur Verhütung, Ermittlung oder Verfolgung von Straftaten vorlag. Vielmehr hatte der Beschwerdeführer in Deutschland einen Asylantrag gestellt, der vom Bundesamt für Migration und Flüchtlinge (BAMF) abgelehnt worden war. Nach ebenfalls erfolgloser Asylklage war das Verfahren unanfechtbar abgeschlossen. Da gegen ihn kein Einreise- oder Aufenthaltsverbot verhängt wurde, war er auch nicht zur Fahndung und Festnahme ausgeschrieben worden. Wie in diesen Fällen üblich, erteilte die Ausländerbehörde dem Beschwerdeführer eine Duldung. Die Duldung ist kein Aufenthaltstitel, sondern gewährt einer ausreisepflichtigen

35 Zu den Schengener Staaten gehören alle EU-Länder mit Ausnahme von Irland und teilweise Zypern. Darüber hinaus zählen Island, Liechtenstein, Norwegen und die Schweiz dazu.

Person die vorübergehende Aussetzung der Abschiebung. Sie ist in der Regel mit einer Wohnsitzauflage bzw. räumlichen Beschränkung verbunden. Nach bestandskräftigem Asylverfahren löst das BAMF jedoch bei Drittstaatsangehörigen im SIS eine Ausschreibung zur Rückkehr aus. Deren Zweck ist es zu überprüfen, ob die betroffene Person ihrer Verpflichtung zur Ausreise nachgekommen ist. Rechtsgrundlage dafür ist Artikel 3 der Verordnung (EU) 2018/1860 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger.

Verlässt die ausreisepflichtige Person ihren Aufenthaltsort im Asylantragsstaat, muss sie die Ausländerbehörde informieren. Der Beschwerdeführer hatte dies nach Auskunft der brandenburgischen Ausländerbehörde unterlassen, als er sich nach Portugal begab, sodass die Eintragung zurecht bestehen blieb. Sobald sich eine ausgeschriebene Person in einem anderen Schengen–Mitgliedstaat bei der dort zuständigen Ausländerbehörde meldet und einen Aufenthaltstitel beantragt, wird die Ausschreibung bekannt. Erwägt dieser Staat, der antragstellenden Person einen Aufenthaltstitel oder ein Visum für längerfristigen Aufenthalt zu erteilen, muss er den ausschreibenden Staat nach Artikel 9 Absatz 2 Verordnung (EU) 2018/1860 unverzüglich davon unterrichten. Erst dann kann die bisher zuständige Ausländerbehörde die Ausschreibung löschen.

Pingpong um Löschung

Diese Unterrichtung, die über interne Kommunikationskanäle des SIS erfolgt (gemäß Verordnungstext: Austausch von Zusatzinformationen), hatte die AIMA unterlassen. Die Ausländerbehörde in Brandenburg wusste offiziell nicht, dass sich der ehemalige Asylbewerber tatsächlich in Portugal aufhielt und dort einen legalen Aufenthaltstitel erhalten sollte. Ohne diesen behördlichen Nachweis wollte sie die Ausschreibung nicht löschen. Wir erläuterten dem Beschwerdeführer die Situation und legten ihm nahe, dass er – mangels unserer Zuständigkeit – die AIMA auffordern sollte, eine Anfrage an die brandenburgische Ausländerbehörde zu richten. Andernfalls könne er nur selbst alle Dokumente mitsamt der Fallnummer zur Antragstellung an die deutsche Behörde senden und darum bitten, dass diese die Kommunikation mit der portugiesischen Behörde aufnimmt. Der Beschwerdeführer beklagte jedoch, dass die AIMA dies verweigere und ihn auffordere, selbst die Löschung zu veranlassen.

Da die Ausschreibung ihren Ursprung in Deutschland hatte und rechtmäßig war, wäre der Sachverhalt auch kein Fall für den portugiesischen Datenschutzbeauftragten (Comissão Nacional de Protecção de Dados, CNPD) gewesen. Obwohl uns die brandenburgische Ausländerbehörde signalisiert hatte, dass sie eine offizielle Mitteilung aus Portugal benötige, entschieden wir – auf Wunsch des Beschwerdeführers – die uns bekannt gewordenen Details, den Schriftverkehr und die Kontaktinformationen der AIMA an die Ausländerbehörde zu übermitteln. Damit sollte eine Verständigung ermöglicht werden, ob die Ausschreibung gelöscht werden kann.

Wie wir zwischenzeitlich festgestellt haben, war diese Strategie nicht erfolgreich. Wir haben uns daher mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ausgetauscht. Dabei wurde bekannt, dass die Schwierigkeiten beim Austausch von Zusatzinformationen zwischen Schengen –Staaten kein Einzelfall sind, sondern auch in Spanien, Belgien und den Niederlanden vergleichbare Problematiken auftreten. Viele betroffene Drittstaatsangehörige können einen möglicherweise bestehenden Löschanspruch nicht realisieren. Um die Ursache dieses Problems zu beheben, hat die Vertreterin der Bundesbeauftragten den Sachverhalt im Aufsichtsgremium für das SIS, dem Coordinated Supervision Committee, vorgetragen, das aus nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten besteht. Wie schnell Abhilfe erfolgt, bleibt abzuwarten.

3 Übersendung von Daten aus dem Ermittlungsverfahren per E-Mail

Ein Hotel informierte uns darüber, dass ein Polizeibediensteter im Zuge eines Ermittlungsverfahrens eine E-Mail an ein zentrales, für mehrere Beschäftigte zugängliches E-Mail-Postfach gesandt hatte. Darin schilderte er, dass gegen einen namentlich benannten Mitarbeiter des Hotels ein Ermittlungsverfahren geführt werde, und bat um weitere Daten des Tatverdächtigen.

Wir bewerteten dies als unzulässige Datenverarbeitung. Der Polizist hätte zunächst beim Hotel anfragen müssen, welche Personen dort für die Bearbeitung polizeilicher Anfragen zu Beschäftigten zuständig sind. Anschließend hätte er sich ausschließlich an die vom Hotel benannte Stelle wenden dürfen, damit nur diejenigen Personen von dem Auskunftsverlangen Kenntnis erlangt hätten, die dafür zuständig waren.

Spätestens beim E-Mail-Versand hätte der Polizeibedienstete geeignete technische und organisatorische Maßnahmen nach §§ 17 und 20 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz ergreifen müssen, um die personenbezogenen Daten des Tatverdächtigen während der elektronischen Übermittlung zu schützen. Denkbar wären hier beispielsweise die Ende-zu-Ende-Verschlüsselung der E-Mail, die Verschlüsselung eines an die E-Mail angehängten Dokuments oder anderweitige, ggf. in Absprache mit der zuständigen Stelle zu treffende technische Sicherungsmaßnahmen gewesen. Sollte hierdurch dem Schutzbedarf nicht angemessen Rechnung getragen werden können, dürfen die personenbezogenen Daten einer oder eines Tatverdächtigen nicht elektronisch übermittelt werden.

Wir informierten die Polizei Brandenburg über den Sachverhalt und wiesen auf die Rechtslage hin. Außerdem regten wir an, geeignete Maßnahmen zu treffen, um die Polizeibediensteten für den Umgang mit per E-Mail gestellten Auskunftsverlangen zu sensibilisieren.

4 Wahrnehmung des datenschutzrechtlichen Auskunftsrechts gegenüber der Polizei

Im Berichtszeitraum fragten uns mehrere betroffene Personen, wie sie herausfinden können, ob und wenn ja, welche Daten die Polizei über sie speichert. Unsere Antwort lautete kurzgefasst: Jedermann hat gegenüber der Polizei Brandenburg einen datenschutzrechtlichen Auskunftsanspruch, mit dem diese Fragen geklärt werden können.

Der Auskunftsanspruch richtet sich nach § 71 Brandenburgisches Polizeigesetz i. V. m. § 40 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz und setzt einen Antrag der betroffenen Person voraus. Die Polizei muss grundsätzlich Auskunft über die gespeicherten personenbezogenen Daten und deren Kategorien, die Herkunft der Daten, die Zwecke und die Rechtsgrundlage der Verarbeitung, die Empfängerinnen bzw. Empfänger oder die Kategorien von Empfängerinnen bzw. Empfängern, denen die Daten offengelegt worden sind, und die Speicherdauer, hilfsweise die Kriterien für deren Festlegung, erteilen. Darüber hinaus muss sie die betroffene Person über ihr Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten und das Recht, die Landesbeauftragte anzurufen, unterrichten und Angaben zu deren Erreichbarkeit bereitstellen. In bestimmten Fällen, beispielsweise wenn die personenbezogenen Daten vom Verfassungsschutz oder einer Staatsanwaltschaft stammen, darf die Polizei die Auskunft nur erteilen, wenn die jeweilige Ursprungsbehörde zugestimmt hat.

Der Auskunftsanspruch gilt nicht uneingeschränkt. Die Polizei kann bei Vorliegen bestimmter Voraussetzungen von einer Auskunftserteilung absehen, sie aufschieben oder einschränken. Hierüber muss sie die betroffene Person grundsätzlich unter Angabe von Gründen unterrichten. Die Mitteilung der Gründe ist nur dann nicht erforderlich, wenn dadurch der Zweck, dessentwegen die Auskunft nicht oder nicht vollständig erteilt wurde, gefährdet werden würde. In diesem Fall ist die betroffene Person darauf hinzuweisen, dass sie ihr Recht auf Auskunft auch über die Landesbeauftragte ausüben kann. Soweit gesetzlich zulässig, muss die Polizei Letzterer die begehrte Auskunft erteilen. Anschließend informiert die Landesbeauftragte die betroffene Person darüber, dass sie das Auskunftsrecht für sie

wahrgenommen hat. Im Berichtszeitraum ist ein solcher Fall nicht an uns herangetragen worden.

Die Auskunft ist gebührenfrei und muss von der Polizei innerhalb einer angemessenen Zeitspanne erteilt werden, die aber von verschiedenen Kriterien (z. B. Ressourcen, Rechercheaufwand, etc.) abhängig sein kann. Zur Verifizierung des Auskunftsersuchens fordert die Polizei regelmäßig eine Kopie des Personalausweises an und akzeptiert hierbei Schwärzungen der für die Identifizierung nicht erforderlichen Angaben.

Der Europäische Datenschutzausschuss arbeitet derzeit an Leitlinien zum Auskunftsrecht im Anwendungsbereich der Richtlinie (EU) 2016/680 (JI-Richtlinie). Dadurch soll auf europäischer Ebene eine Harmonisierung der Auslegung der Rechtsvorschriften erreicht werden. Die Leitlinien werden nach ihrer Fertigstellung auch in unserem Internetangebot veröffentlicht.

5 Datenlöschung nach Einstellung des Ermittlungsverfahrens

Ein Beschwerdeführer teilte uns mit, dass im Jahr 2022 gegen ihn ein Ermittlungsverfahren wegen Nötigung und Beleidigung durch die zuständige Staatsanwaltschaft eingeleitet, aber bereits nach zwei Wochen mangels hinreichenden Tatverdachts gemäß § 170 Absatz 2 Strafprozessordnung (StPO) eingestellt wurde. Im Anschluss hatte er sich an die für das Verfahren zuständige Polizeidirektion gewandt und beantragt, seine Daten zu löschen. Eine Reaktion erfolgte nicht. Erst im Jahr 2025 fragte der Beschwerdeführer erneut bei einer Polizeidienststelle nach und erfuhr, dass seine Daten weiterhin gespeichert waren. Per Bescheid teilte die Polizei nach nochmaliger Prüfung schließlich mit, die Daten gelöscht zu haben, weil kein Restverdacht mehr bestand.

Von der Staatsanwaltschaft erfuhr der Beschwerdeführer, dass die Löschungen dort automatisiert erfolgten, sein Vorgang jedoch fünf Jahre gespeichert bliebe. In seiner Beschwerde bei uns berief er sich auf die Regelungen für Justizbehörden, wonach Einträge in das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) innerhalb von zwei Jahren nach Erledigung des Verfahrens zu löschen sind. Nicht nachvollziehbar war für ihn auch die dazu scheinbar im Widerspruch stehende gesetzlich vorgesehene dreijährige Frist, nach der die Staatsanwaltschaft prüfen muss, ob eine Notwendigkeit besteht, Daten weiter zu speichern (§ 489 Absatz 3 Nummer 3 StPO). Nunmehr beantragte der Beschwerdeführer erneut die Löschung aller im Zusammenhang mit diesem Vorgang stehenden personenbezogenen Daten bei der Staatsanwaltschaft und bat uns um eine Erläuterung der Rechtslage.

Zur Datenspeicherung bei der Polizei erläuterten wir Folgendes:

Die Polizei ist berechtigt, rechtmäßig erlangte personenbezogene Daten in Akten oder Dateien zu speichern und zu nutzen, soweit dies zur Erfüllung ihrer Aufgaben, zur zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist. Für die für Zwecke der Aufklärung und Prävention suchfähig im Auskunftsverfahren POLAS gespeicherten polizeilichen Daten gilt, dass die Polizei diese nur löschen muss, wenn sich der gegen die betroffene Person be-

stehende Verdacht einer Straftat anhand der polizeilichen Unterlagen nicht mehr begründen lässt. Ein Restverdacht, wie er besonders bei Einstellungen gemäß § 170 Absatz 2 StPO häufig besteht, genügt gemäß § 47 Absatz 2 Satz 1 Nummer 1 i. V. m. § 39 Absatz 2 Satz 5 Brandenburgisches Polizeigesetz für die weitere Speicherung. Die Speicherfrist ist systemseitig auf zunächst 13 Monate festgelegt. Die Entscheidung der Staatsanwaltschaft, ein Ermittlungsverfahren einzustellen, begründet deshalb noch keinen Rechtsanspruch auf Löschung der bei der Polizei im Zusammenhang mit dem eingestellten Verfahren gespeicherten Daten. Die Unterlagen (Kriminalakte und Datenspeicherung) müssen jedoch in regelmäßigen Abständen nach Ablauf von Prüffristen, die bei jeder Ersterfassung und bei jeder Aufbewahrungsverlängerung neu festzulegen sind, dahingehend geprüft werden, ob der Restverdacht noch besteht und ob die Daten für die Polizeiarbeit noch erforderlich sind. Eine Prüfung erfolgt auch im Einzelfall, wenn die betroffene Person einen Antrag auf Löschung stellt. Eine zunächst festgelegte Speicherfrist kann sich auch dadurch verlängern, dass vor Ablauf der Prüffrist der Polizei ein weiteres Verfahren gegen die betroffene Person bekannt wird. In diesem Fall werden die bis dahin gespeicherten Daten so lange vorgehalten, bis für alle Eintragungen, auch die zuletzt hinzugekommene, die Löschungsvoraussetzungen vorliegen.

Zur Datenspeicherung bei der Staatsanwaltschaft erläuterten wir Folgendes:

Für die bei der Staatsanwaltschaft gespeicherten Daten regelt § 489 StPO Details zur Löschung. Nach Absatz 1 Nummer 1 der Vorschrift sind die für Zwecke eines Strafverfahrens gespeicherten Daten mit der Erledigung des Verfahrens zu löschen, soweit die Speicherung nicht für Zwecke künftiger Strafverfahren und der Vorgangsverwaltung zulässig ist. Auch für die im Zuge des Ermittlungsverfahrens bei der Staatsanwaltschaft gespeicherten Daten gilt, dass die Notwendigkeit weiterer Speicherung regelmäßig zu überprüfen ist und hierfür angemessene Fristen vorzusehen sind. In § 489 Absatz 3 StPO sind Überprüfungsfristen für staatsanwaltliche Daten festgelegt, die zu Zwecken künftiger Strafverfahren gespeichert werden können. Dabei wird zwischen den Betroffenen und der Art der Verfahrenseinstellung unterschieden. Die von dem Beschwerdeführer zitierte Frist von drei Jahren bezieht sich auf eine „nicht nur vorläufige“ Verfahrenseinstellung, d. h. eine endgültige Einstellung. Eine solche lag im Beschwerdefall nicht vor.

Nach § 170 Absatz 2 Satz 1 StPO ist ein Verfahren einzustellen, wenn die Ermittlungen keinen genügenden Anlass zur Erhebung der öffentlichen Klage gegeben haben. Dies kann der Fall sein, wenn aufgrund der unzureichenden Beweislage ernsthafte Zweifel an der Täterschaft bestehen oder aber, wenn eine wichtige Voraussetzung für die Strafverfolgung fehlt oder ein sogenanntes Verfahrenshindernis vorliegt. Sind jene dauerhaft und nicht behebbar, wirkt die Einstellung endgültig. Stellt die Staatsanwaltschaft das Verfahren dagegen mangels hinreichenden Tatverdachts ein, so gilt dies nicht als „endgültige Einstellung“. Wenn nachträglich Tatsachen festgestellt werden, dass der Betroffene das Delikt begangen haben könnte, kann das Verfahren bis zum Eintritt der gesetzlichen Verfolgungsverjährung wieder aufgenommen werden. Erst mit Eintritt der Verjährung ist es als endgültig erledigt anzusehen. Die maßgebliche Verjährungsfrist beträgt für das hier relevante Delikt der Nötigung gemäß § 78 Absatz 3 Nummer 4 StGB fünf Jahre. Danach könnte das Ermittlungsverfahren trotz Tatverdachts nicht mehr aufgenommen werden und die Daten wären grundsätzlich zu löschen. Wir erläuterten dem Beschwerdeführer daher den aus dem Gesetzestext nicht unmittelbar erkennbaren Unterschied.

Löschvorschriften: Komplexe Rechtslage

Vor allem die Speicherung für Zwecke der Vorgangsverwaltung erlaubt oftmals längere Speicherfristen. Mit Ablauf der Aufbewahrungsfristen für die Papierakte werden diese und die dazugehörigen Daten im staatsanwaltschaftlichen Vorgangsverfahren MESTA gelöscht. Die Aufbewahrungsfristen richten sich nach dem Brandenburgischen Justiz-Schriftgutaufbewahrungsgesetz und Anlage 1 der Verordnung über die Aufbewahrung von Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden. In Letzterer ist für Strafakten mit sonstigen Angelegenheiten, in denen das Verfahren eingestellt ist, und sonstige Akten eine Aufbewahrungsfrist von fünf Jahren vorgesehen.

Die Auskunft der Staatsanwaltschaft, dass der Vorgang erst nach fünf Jahren gelöscht werden sollte, war daher zutreffend. Eine Datenschutzverletzung, konnten wir nicht feststellen.

Davon unabhängig bestehen Regelungen für das vom Bundesamt für Justiz geführte ZStV. Eine verpflichtende Löschung nach zwei Jahren erfolgt dort gemäß § 494 Absatz 2 Satz 2 StPO nur, wenn das

Verfahren gegen den Beschuldigten nicht nur vorläufig eingestellt wurde, sondern endgültig. Im Ergebnis stellten wir daher fest, dass die Voraussetzungen für die genannte Speicherfrist von zwei Jahren beim ZStV ebenfalls nicht vorlagen.

6 Bedeutung der KI-Verordnung für die Strafverfolgung

Am 2. Februar 2025 wurden verschiedene Vorschriften der Verordnung über Künstliche Intelligenz (KI-Verordnung, KI-VO) wirksam. Seitdem müssen Anbieterinnen und Anbieter sowie Betreiberinnen und Betreiber von KI-Systemen gemäß Artikel 4 KI-VO sicherstellen, dass alle Personen, die mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen. Darüber hinaus verbietet Artikel 5 KI-VO bestimmte Praktiken im KI-Bereich.[36]

Im Kontext der polizeilichen Nutzung untersagt Artikel 5 Absatz 1 Buchstabe d KI-VO beispielsweise den Einsatz eines KI-Systems, das ausschließlich auf der Grundlage des Profilings einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften das Risiko, dass diese Person eine Straftat begehen wird, bewertet oder vorhersagt (sogenanntes „Predictive Policing“). Ebenso ist es nach Buchstabe e der Vorschrift untersagt, ein KI-System zu verwenden, das ungezielt Gesichtsbilder aus dem Internet oder aus Aufnahmen von Überwachungskameras ausliest (sogenanntes „Scraping“), um daraus eine Gesichtserkennungsdatenbank zu erstellen oder eine solche zu erweitern.

Für die Strafverfolgung gibt es Ausnahmen von diesem grundsätzlichen Verbot, wenn strenge Voraussetzungen eingehalten und eng umrissene Zwecke verfolgt werden. Beispielsweise ist es gemäß Artikel 5 Absatz 1 Buchstabe h KI-VO zulässig, biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken zu verwenden, wenn und soweit dies unbedingt erforderlich ist, um die nachfolgenden Ziele zu erreichen:

- gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen,

36 Siehe A I.

- Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags,

- Aufspüren oder Identifizieren einer Person, die der Begehung einer schweren Straftat verdächtigt wird, um gegen diese Person strafrechtliche Ermittlungen, Strafverfahren oder Strafvollstreckung durchzuführen.

Unter den Begriff des biometrischen Fernidentifizierungssystems fällt nach der Definition in Artikel 3 Nummer 41 KI-VO ein KI-System, das „dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren." Dazu gehören etwa die Erkennung anhand des Ganges, der Sprache und – besonders praxisrelevant – des Gesichts. Erfolgt die Identifizierung nicht unmittelbar, sondern mit zeitlicher Verzögerung, spricht man von nachträglicher bzw. retrograder Fernidentifizierung.

Biometrische Echtzeit-Fernidentifizierungssysteme dürfen nur zur Bestätigung der Identität der verdächtigen Personen eingesetzt werden. Dabei müssen sowohl die Art der Situation als auch die Folgen der Verwendung des Systems für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden. Die genannten Voraussetzungen eines erlaubten Einsatzes beziehen sich ausschließlich auf die Echtzeit-Fernidentifizierung, d. h. eine nachträgliche Fernidentifizierung bezogen auf öffentlich zugängliche Räume für o. g. Zwecke ist nicht untersagt. Darüber hinaus gilt das grundsätzliche Verbot auch nicht für nicht öffentlich zugängliche Räume, z. B. Arbeitsplätze oder im Online-Bereich.

Weitere Voraussetzungen für den Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme sind nach der KI-Verordnung u. a., dass die Strafverfolgungsbehörde eine Grundrechte-Folgenabschätzung gefertigt und das System in der EU-Datenbank registriert hat. Vor der Verwendung des Systems muss die Strafverfolgungsbehörde grundsätzlich eine Genehmigung der zuständigen Stelle, die durch das nationale Recht der Mitgliedsstaaten festgelegt wird, einholen. Jede Verwendung eines solchen Systems muss zudem der zuständigen Marktüberwachungsbehörde und der zuständigen Datenschutz-

behörde mitgeteilt werden. Die Mitgliedstaaten können im Einklang mit dem Unionsrecht strengere Rechtsvorschriften für die Verwendung biometrischer Fernidentifizierungssysteme erlassen.

Am 2. August 2025 wurden weitere Vorschriften der KI-VO mit Pflichten zur Dokumentation und Risikobewertung wirksam, die Anbieterinnen und Anbieter von KI-Modellen mit allgemeinem Verwendungszweck einhalten müssen. Außerdem wurden Vorschriften zu Sanktionen eingeführt.

7 Rechtsgrundlage für eine automatisierte Datenanalyse

In mehreren Bundesländern wurden oder werden derzeit die Polizeigesetze u.a. mit dem Ziel reformiert, Polizeibehörden Datenverarbeitungen mittels Künstlicher Intelligenz zu ermöglichen. Insbesondere die automatisierte Datenanalyse steht dabei im Fokus. Dadurch können große Mengen personenbezogener Datensätze ausgewertet und verknüpft werden. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat hierzu im September 2025 eine Entschließung verabschiedet.[37] Darin fordert sie, dass solche Analysewerkzeuge nur bei schwerwiegenden Verletzungen von Rechtsgütern und unter Beachtung enger Verfahrensvoraussetzungen eingesetzt werden dürfen. Hierfür bedarf es einer spezifischen Rechtsgrundlage in den Polizeigesetzen, da die bestehenden Normen für die Besonderheiten der komplexen Analysemittel derzeit nicht ausreichen. Von einer Analyse können nicht nur potenzielle Straftäterinnen und Straftäter betroffen sein, sondern auch Zeuginnen und Zeugen, Sachverständige und Geschädigte. Vor allem für diejenigen Personen, die keinen Anlass für Ermittlungen gegeben haben, deren personenbezogene Daten aber dennoch durch die automatisierte Datenanalyse verarbeitet werden, ist der Eingriff in ihre Grundrechte besonders schwerwiegend.

Bei der Erarbeitung neuer Rechtsgrundlagen müssen auch die Vorgaben des Bundesverfassungsgerichts beachtet werden. Dieses hat in seinem Urteil vom 16. Februar 2023[38] ausgeführt, dass sich die Schwere des mit der automatisierten Datenanalyse verbundenen Grundrechtseingriffs insbesondere nach Art und Umfang der verarbeiteten personenbezogenen Daten und der Auswahl der Analysemethode bemisst. Wenn viele Personen, die keinen Anlass zur Straf-

37 Entschließung „Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten!“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 17. September 2025.

38 Urteil des Bundesverfassungsgerichts vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20.

tatermittlung geben, von der Datenauswertung betroffen sind oder in die Datenanalyse verschiedene, ursprünglich zu anderen Zwecken geführte Datensammlungen einbezogen werden, ist regelmäßig von einem besonderen Gewicht des Grundrechtseingriffs auszugehen. Gleiches gilt, wenn eine KI für die automatisierte Datenanalyse genutzt wird. Ein solch schwerwiegender Grundrechtseingriff ist nur dann zulässig, wenn er dem Schutz wichtiger Rechtsgüter dient und unter streng definierten weiteren Voraussetzungen erfolgt. Hierzu gehört auch eine sachgerechte Ausgestaltung der Kontrolle durch die Datenschutzaufsicht.

Bei der Auswahl geeigneter Analysewerkzeuge ist auch das Gebot der digitalen Souveränität des Staates zu beachten. Sollten Analysesysteme verwendet werden, die von anderen Staaten oder privaten Akteuren entwickelt wurden, kann dies Risiken im Hinblick auf eine unbemerkte Manipulation oder einen unbemerkten Zugriff auf die verwendeten personenbezogenen Daten bergen.[39]

Für Brandenburg ist eine Novellierung des Polizeigesetzes angekündigt. Es bleibt abzuwarten, wie die Vorgaben für eine automatisierte Datenanalyse umgesetzt werden.

39 Urteil des Bundesverfassungsgerichts vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn 100.

8 Zahlen und Fakten

Im Berichtszeitraum gingen bei der Landesbeauftragten insgesamt 31 Beschwerden von Bürgerinnen und Bürgern über die Datenverarbeitung bei der Polizei und den Staatsanwaltschaften ein. Zwei Beschwerden befassten sich darüber hinaus mit der Zulässigkeit der Datenverarbeitung durch Justizvollzugsanstalten. Diese Fälle werden, da sie im Bereich der Strafvollstreckung liegen, ebenfalls von der Richtlinie (EU) 2016/680 (JI-Richtlinie) erfasst.

Von den 31 Beschwerden richtete sich der überwiegende Teil gegen die Polizei. Nur ein kleiner Teil betraf die Staatsanwaltschaften des Landes Brandenburg. Inhaltlich gab es eine große Vielfalt an Fallgestaltungen. So wurden wir in einigen Fällen um Unterstützung gebeten, Protokolldatenabfragen bei der Polizei zu veranlassen. Gegenstand mehrerer Verfahren war das Begehren betroffener Personen, Auskunft über die zu ihnen bei der Polizei gespeicherten Daten zu erhalten. In anderen Fällen hegten die Beschwerdeführerinnen und Beschwerdeführer den Verdacht, dass die Polizei ihre personenbezogenen Daten unbefugt an Dritte übermittelt haben könnte, und wandten sich deshalb an uns. Auch trugen betroffene Personen die Vermutung der falschen Zuordnung von personenbezogenen Daten durch die Polizei bzw. daraus resultierende Berichtigungsbegehren an uns heran.

In 21 Fällen bearbeiteten wir Anfragen von Bürgerinnen und Bürgern. Eine solche liegt u. a. dann vor, wenn die Person nicht selbst von der Datenverarbeitung durch die Polizei oder Staatsanwaltschaft betroffen und somit nicht beschwert sein kann oder wenn es sich um eine allgemein gehaltene Frage handelt, die uns losgelöst von einem konkreten Beschwerdefall erreicht. Hierunter fallen auch Abgrenzungsfragen, in denen wir die Unterschiede zwischen datenschutzrechtlichen und verfahrensrechtlichen Auskunfts- und Akteneinsichtsansprüchen erläuterten. Zusätzlich berieten wir auch telefonisch, ohne dies statistisch zu erfassen.

Wir begleiteten im Berichtszeitraum drei polizeirechtliche Rechtsetzungsvorhaben mittels Stellungnahmen und Beratungen und standen dabei im Austausch mit dem zuständigen Referat im Ministerium des Innern und für Kommunales des Landes Brandenburg.

Gemäß § 29 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) bzw. § 65 Bundesdatenschutzgesetz sind die Polizei, Staatsanwaltschaften und Justizvollzugsbehörden verpflichtet, uns Verletzungen der Sicherheit personenbezogener Daten zu melden. Dies geschah im Berichtszeitraum in 29 Fällen. Meldungen erhielten wir vom Zentraldienst der Polizei und dem Polizeipräsidium. Inhaltlich ging es u. a. um den Fehlversand von Unterlagen, beispielsweise durch fehlerhafte Kuvertierung von Briefen oder Verwechslungen von Personen. Auch die unberechtigte Kenntnisnahme von personenbezogenen Daten durch Dritte wurde uns gemeldet.

In einem Fall sprachen wir eine Beanstandung gemäß § 36 Absatz 2 BbgPJMDSG gegenüber der Polizei aus.[40]

40 Siehe B I.

Die Dienststelle

1 Öffentlichkeitsarbeit

In jedem Jahr führt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz), zu deren Mitgliedern die Landesbeauftragte zählt, eine zentrale Veranstaltung anlässlich des am 28. Januar gefeierten Europäischen Datenschutztags durch. Im Berichtsjahr trug diese Veranstaltung den Titel „Digitalisierung um jeden Preis? Kein Zwang zur Preisgabe personenbezogener Daten“. Vor rund 150 Gästen sprachen Vertreterinnen und Vertreter aus Journalismus, Zivilgesellschaft, Wissenschaft und Wirtschaft über die Frage nach den Folgen weitreichender Digitalisierung für den Zugang zu Waren und Diensten sowie zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten bei rein digitalem Zugang. Ausgerichtet wurde die Veranstaltung in der Hessischen Landesvertretung in Berlin vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit als Vorgänger des Konferenzvorsitzes im Jahr 2025.

In jedem zweiten Herbst dreht sich in einer der Städte Brandenburgs ein ganzes Wochenende lang alles um die Vorzüge und Qualitäten des Landes und seiner Bewohnerinnen und Bewohner, denn dann ist Brandenburg-Tag, das offizielle Landesfest. Nachdem 2023 ins südliche Finsterwalde geladen worden war, erhielt im Berichtsjahr die im nordwestlichen Landeszipfel gelegene Rolandstadt Perleberg Gelegenheit, sich als Ausrichterstadt zu beweisen. Rund 80.000 Personen begaben sich am Wochenende vom 12. bis 14. September dorthin und informierten und amüsierten sich an den Ständen der vielen Ausstellerinnen und Aussteller. Darunter fand sich auch dieses Mal wieder die Landesbeauftragte. Mit Schautafeln und einem Rätsel „KI-Wortsuche“ in zwei Schwierigkeitsstufen bot sie den Besucherinnen und Besuchern ihres Standes die Möglichkeit zur Auseinandersetzung mit dem aktuell viel diskutierten Thema „Künstliche Intelligenz“ (KI). Im Fokus standen dabei natürlich Aspekte des Datenschutzes. Eine Schautafel informierte über Datenschutz-Risiken beim Einsatz von KI-Chatbots und zeigte Wege auf, wie diesen begegnet werden kann. Eine andere Tafel richtete sich an beruflich mit KI befasste Personen – wie Entwicklerinnen und Entwickler, aber auch Entscheidungsträgerinnen und -träger, die einen KI-Einsatz erwägen – und widmete sich daher auch Fragen der Konzeption und Implementierung von KI-Anwendungen. Das Rätsel bestand im Auf-

finden zentraler Begriffe des Themenfeldes KI in einem Buchstabengitter. Während die leichte Variante die zu suchenden Wörter bereits mit an die Hand gab, galt es im Fall der schwierigeren Fassung, die Wörter zunächst selbst zu ermitteln, indem Sätze zu vervollständigen waren. Wer die Aufgabe erfolgreich meisterte, erhielt als Anerkennung eine Kleinigkeit mit Datenschutzbezug.

Diejenigen, die sich über Datenschutz oder Akteneinsicht informieren möchten, finden bei der Landesbeauftragten ein vielfältiges Angebot an Informationsmaterial in gedruckter oder digitaler Form. Erhältlich sind beispielsweise wichtige Rechtstexte in Broschürenform, aber auch Faltblätter, die einen schnellen Überblick zu Themen mit starkem Alltagsbezug liefern. Als zentrales Regelwerk des Datenschutzrechts ist die Datenschutz-Grundverordnung Teil des Broschürenangebots; von den Faltblättern widmet sich eines dem in der Beschwerdebearbeitung häufig wiederkehrenden Thema der Videoüberwachung im nachbarschaftlichen Kontext. Im Fall beider Veröffentlichungen ging der Vorrat im Berichtsjahr zur Neige, sodass ein erneuter Druck erforderlich wurde. Während das Faltblatt keiner inhaltlichen Änderungen bedurfte, musste die Broschüre, die zuletzt im Jahr 2020 gedruckt worden war, entsprechend der Berichtigung der Datenschutz-Grundverordnung vom 4. März 2021 angepasst werden. Das Faltblatt wurde daher im Oktober des Berichtsjahres in 4., unveränderter Auflage veröffentlicht, die Broschüre bereits im März als 3., aktualisierte Auflage.

Als reine Netzpublikation bietet die Landesbeauftragte u. a. Handreichungen an, die sich mit häufig gestellten Fragen sowohl von Bürgerinnen und Bürgern als auch von Verantwortlichen befassen. Drei dieser Handreichungen wurden im Berichtsjahr aktualisiert, nämlich „Datenschutzbeauftragte – rechtliche Anforderungen“, „Meldung von Datenschutzverletzungen in Brandenburg“ sowie „Technische und organisatorische Maßnahmen zur Umsetzung des Datenschutzes bei Heimarbeit“. Alle Dateien wurden zudem in ein neues, barrierefreies Format überführt. Überarbeitungen zur Verbesserung der Barrierefreiheit fanden daneben auch über die gesamte Breite des Internetangebots hinweg statt. So wurden im Zuge dieser Arbeiten etwa auch die Musterschreiben für Bürgerinnen und Bürger zur Verwendung gegenüber Behörden, Unternehmen, Vereinen und sonstigen Daten verarbeitenden Stellen neu geschaffen.

Als weitere, strukturelle Veränderung im Internetangebot der Landesbeauftragten ist für das Berichtsjahr die Einführung eines neuen Themenschwerpunktes festzuhalten: Dem Thema KI ist dank seiner Aktualität und Bedeutung nunmehr eine eigene Seite gewidmet, die ausgewählte Dokumente und Positionen insbesondere der Datenschutzaufsichtsbehörden aus Deutschland und der Europäischen Union zusammenstellt, um Orientierung und Hilfestellung auf diesem Gebiet zu geben. Als lebende Sammlung wird die Seite auf alle künftigen Entwicklungen mit inhaltlichen Anpassungen reagieren, um diesen Anspruch weiterhin erfüllen zu können. Verzichtet wird im Gegenzug auf den Themenschwerpunkt „Internationaler Datenverkehr".

Der Gerichtshof der Europäischen Union entscheidet in vielen Fällen über grundlegende Fragen zur Auslegung der Datenschutz-Grundverordnung. Den Urteilen kommt für die Datenschutzpraxis daher eine hohe Bedeutung zu. Vor diesem Hintergrund führt die Landesbeauftragte auf einer weiteren Schwerpunktseite eine Liste ausgewählter Entscheidungen des Gerichtshofs, die gleichsam ständig fortgeschrieben wird. Auch im Berichtsjahr wurde diese Liste abermals erweitert. Die hinzugefügten Urteile betreffen die Zulässigkeit von Geschlechtsabfragen beim Fahrkartenkauf, die Frage, wann die Inanspruchnahme der Aufsichtsbehörden für Beschwerdezwecke als exzessiv bewertet werden kann, die maximale Bußgeldhöhe bei Zugehörigkeit des betreffenden Unternehmens zu einem Konzern, das Auskunftsrecht bei automatisierter Bonitätsberechnung und die Präzisierung des Begriffs „personenbezogene Daten" im Kontext der Pseudonymisierung.

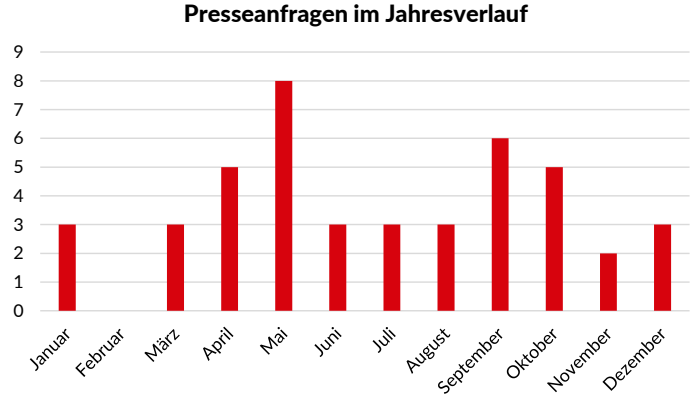
In Orientierungshilfen und Anwendungshinweisen gibt die Datenschutzkonferenz Antworten auf wichtige Fragen zu Auslegung und Umsetzung datenschutzrechtlicher Vorschriften. Als Konferenzmitglied wirkt die Landesbeauftragte an der Erarbeitung derartiger Papiere mit. Im Berichtsjahr wurde dieses Angebot um folgende Dokumente erweitert: eine „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen", „Anwendungshinweise zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken", eine Orientierungshilfe „Datenschutzrechtliche Besonderheiten generativer KI-Systeme mit RAG-Methode", eine Handlungsanleitung „Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei

EfA-Onlinediensten nach Onlinezugangsgesetz (OZG)“ und eine „Orientierungshilfe zur Zusammenarbeit mehrerer Aufsichtsbehörden im Rahmen von § 5 GDNG“. Zudem wurden 2 existierende Papiere überarbeitet und mit neuer Versionsnummer veröffentlicht, nämlich die „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ als Version 3.0 und die „Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG)“ als Version 1.1. Alle genannten Papiere sind im Internetangebot der Landesbeauftragten abrufbar.

Einheitlichkeit in der Anwendung der EU-Datenschutzvorschriften ist das vornehmliche Ziel des Europäischen Datenschutzausschusses (EDSA). Hierfür gibt der EDSA u. a. 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. Im Berichtsjahr wurde die Sammlung ergänzt um die „Leitlinien 02/2024 zu Artikel 48 DSGVO“. Außerdem wurde im Falle der „Leitlinien 03/2022 zu irreführenden Gestaltungsmustern auf Benutzeroberflächen von Social-Media-Plattformen“ die englische Fassung durch die deutsche Übersetzung ersetzt.

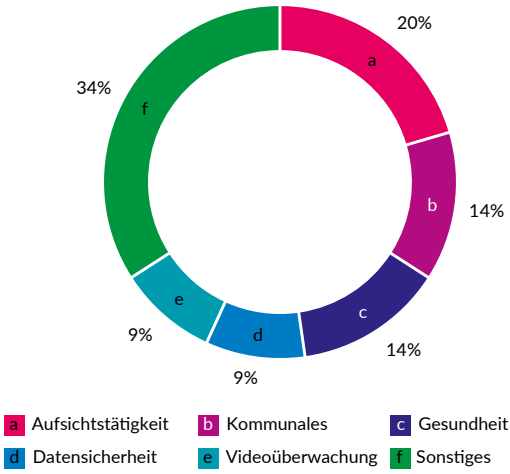
2 Pressearbeit

Im Berichtszeitraum haben wir 44 Medienanfragen zum Datenschutz erhalten. Das war ca. ein Fünftel weniger als im Vorjahr. Im monatlichen Vergleich erreichten uns die meisten Anfragen im Mai und September.



Wie bereits im Vorjahr war kein klarer thematischer Schwerpunkt der Anfragen zu erkennen. Häufig wurden wir nach unserer Aufsichtstätigkeit gefragt. Das betraf beispielsweise die Organisation der Datenschutzaufsicht, die Sanktionspraxis der Landesbeauftragten sowie statistische Angaben zu Beschwerden, Meldungen von Datenschutzverletzungen oder Bußgeldern. Datenschutzrelevante Gesichtspunkte im Zusammenhang mit dem Gesundheitswesen sowie mit originär kommunalen Aufgaben rangierten an zweiter Stelle, während Aspekte zur Datensicherheit und zur Videoüberwachung sich den dritten Rang teilten. Die übrigen Anfragen ließen sich derartigen Schwerpunkten nicht eindeutig zuordnen.

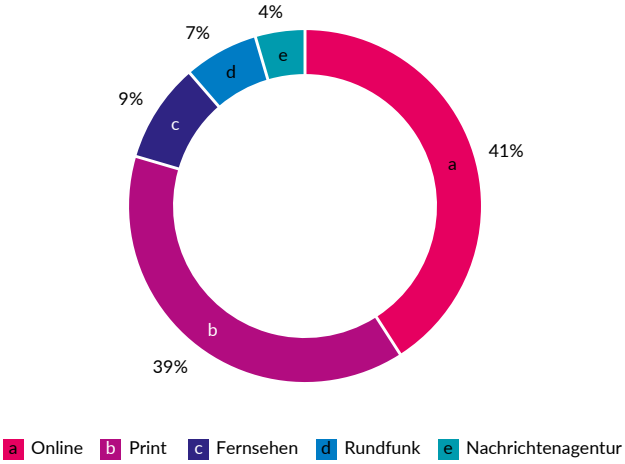
Schwerpunkte der Presseanfragen



Hinsichtlich der datenschutzrechtlich Verantwortlichen richteten sich die Presseanfragen zu 41 % auf die Datenverarbeitung durch öffentliche Stellen. 39 % bezogen sich auf Unternehmen und andere nicht öffentliche Stellen.

Erstmals stellten Anfragen, die voraussichtlich in einer Online-Berichterstattung münden sollten, den größten Anteil an allen Medienanfragen. Er betrug 41 %. Nur mit geringem Abstand folgten Anliegen von Journalistinnen und Journalisten, die in Print-Medien berichteten, nämlich 39 %. Die restlichen Anteile betrafen das Fernsehen, den Hörfunk oder Nachrichtenagenturen. Die Abgrenzung zwischen den einzelnen Arten der Medien bleibt allerdings weiterhin schwer, da viele ihre Berichterstattung inzwischen in unterschiedlicher Form anbieten.

Welche Medien stellen Presseanfragen?



Jeweils etwa die Hälfte der Anfragen stammten von regionalen Medien – also aus den Ländern Brandenburg und Berlin – und von Journalistinnen und Journalisten aus anderen Bundesländern bzw. von solchen, die bundesweit tätig waren. Internationale Presseanfragen fielen im Berichtszeitraum kaum ins Gewicht.

3 Personal und Organisation der Dienststelle

Mit dem Wirksamwerden der europäischen Verordnung über Künstliche Intelligenz im Berichtsjahr ergaben sich für meine Dienststelle neue Aufgaben, insbesondere in Bezug auf die Verarbeitung personenbezogener Daten in KI-Systemen. Der Landtag Brandenburg bewilligte in diesem Zusammenhang für den Doppelhaushalt 2025/2026 dankenswerterweise zwei neue Stellen. Eine dieser Stellen konnte noch im Berichtszeitraum mit einem Informatiker besetzt werden; das Bewerbungsverfahren für die zweite Stelle, die im Bereich Recht angesiedelt ist, wurde ebenfalls erfolgreich abgeschlossen.

Dessen ungeachtet blieb die Personalsituation der Dienststelle auch im Berichtsjahr angespannt. Betroffen waren mit den Bereichen Recht, Technik und Organisation sowie Verwaltung und dem Justiziariat alle Teile der Behörde. Insgesamt waren sieben Stellen vakant und die Bemühungen zur Wiederbesetzung nur zum Teil erfolgreich. In fünf Fällen gelang dies, teilweise jedoch erst nach mehreren Ausschreibungen. Den langjährigen Leiter des Bereichs Recht meiner Dienststelle verabschiedete ich am Ende des Berichtsjahrs in den wohlverdienten Ruhestand. Seine Nachfolgerin konnte bereits einige Monate zuvor gefunden werden.

Auch waren wieder Mutterschutz- und Elternzeiten, verschiedene Arbeitszeitverkürzungen und lange krankheitsbedingte Ausfallzeiten zu kompensieren. Erfreulicherweise gelang es zumindest teilweise, hierfür befristete Vertretungen zu finden.

Für eine recht kleine Behörde mit nur 46 Stellen sind eine hohe Personalfluktuation, ein nicht unwesentlicher Anteil an Teilzeitbeschäftigungen und häufige sowie langfristige Abwesenheiten eine große Herausforderung und Belastung. Die schwierige Personalsituation führt auch dazu, dass Beschwerdeführerinnen und Beschwerdeführer sowie Beratung suchende Personen bei der Bearbeitung ihrer Anliegen oft viel Geduld mitbringen müssen. Klar ist leider, dass die Vertretungen den Personalausfall nicht vollständig ausgleichen können. Wie schon in den Vorjahren möchte ich mich bei allen Mitarbeiterinnen und Mitarbeitern meiner Dienststelle für die geleistete Mehrarbeit und die großen Anstrengungen, trotz aller Schwierigkei-

ten so bürgerfreundlich und zügig wie möglich zu arbeiten, herzlich bedanken.

Eine Entspannung ist auch in Zukunft kaum zu erwarten. Dies liegt nicht zuletzt daran, dass in der Region eine Reihe attraktiver Arbeitgeberinnen und Arbeitgeber um Beschäftigte werben. So hat auch meine Dienststelle bereits mehrfach Mitarbeiterinnen und Mitarbeiter an diese verloren.

Wie bereits im letzten Tätigkeitsbericht dargestellt, plante der Brandenburgische Landesbetrieb für Liegenschaften und Bauen seit einiger Zeit, meiner Behörde in einem Nachbargebäude auf der Liegenschaft in Kleinmachnow zusätzliche Büroräume bereitzustellen. Die Sanierung wurde nunmehr abgeschlossen. Der Dienststelle stehen damit fünf neue Büros, ein großer Besprechungsraum sowie einige Funktionsräume zur Verfügung. Sie sind barrierefrei und über einen Fahrstuhl auch per Rollstuhl zu erreichen. Die bislang angespannte Raumsituation konnte dadurch entschärft werden.

Bedauerlich ist, dass sich auch im Berichtsjahr die Möglichkeiten zur Mittagsverpflegung nicht verbessert haben. Dem benachbarten Julius-Kühn-Institut gelang es trotz mehrfacher Versuche nicht, die dortige Kantine neu zu verpachten. Andere Angebote gibt es nur in begrenzter Zahl und in größerer Entfernung. Die Attraktivität des Behördenstandorts Kleinmachnow leidet darunter.

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