



Landesbeauftragte
für Datenschutz
und Akteneinsicht

Tätigkeitsbericht Datenschutz 2023



Tätigkeitsbericht Datenschutz der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht

zum 31. Dezember 2023

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 2023 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: Besucherzentrum Bernau des UNESCO-Welt-
erbes „Das Bauhaus und seine Stätten in Weimar,
Dessau und Bernau“
Steimle Architekten BDA | Foto: Brigida González

Druck: Landesvermessung und Geobasisinformation
Brandenburg

Vorwort	7
----------------------	----------

Teil A: Bericht nach Artikel 59 Datenschutz-Grundverordnung

I	Schwerpunkte	13
1	Künstliche Intelligenz	13
1.1	Künstliche Intelligenz und Datenschutz	13
1.2	Mitwirkung bei der Prüfung von ChatGPT	17
1.3	KI-Handreichung des Bildungsministeriums für Schulen	18
2	Umsetzung des Onlinezugangsgesetzes zur Digitalisierung der Verwaltung	20
2.1	Orientierungshilfe zur Nachnutzung von Onlinediensten	20
2.2	Begleitung der OZG-Projekte im Themenfeld „Ein- und Auswanderung“	23
2.3	Ausgewählte Einzelprojekte	25
2.3.1	Energiepreispauschale für Studierende	25
2.3.2	Heizkosten: Härtefallhilfen für Privathaushalte	28
2.3.3	Förderung der Fortbildung zum beruflichen Aufstieg	30
2.3.4	Wohngeld	32
2.4	Novellierung des Onlinezugangsgesetzes	34
3	Betrieb von Facebook-Fanpages durch öffentliche Stellen	37

II	Datenschutzverstöße: Maßnahmen und Sanktionen	41
1	Geplante Videoüberwachung eines Stadtfestes	41
2	Videokameras in Ferienwohnanlagen	43
3	Umfangreiche Videoüberwachung in einem Produktionsbetrieb	48
4	Offenlegung hunderter E-Mail-Adressen bei der Versendung von Werbung	50
5	Unzulässige Datenverarbeitung einer Fahrerlaubnisbehörde nach Beantragung einer Parkerleichterung durch Schwerbehinderte und bei Umtausch des Führerscheins	52
6	Bericht der Bußgeldstelle	55
6.1	Aushang der Krankentage von Beschäftigten eines Lebensmittelgeschäfts	55
6.2	Unbefugte Datenabfragen in Krankenhäusern	56

6.3	Polizist nutzt Telefonnummer einer Anzeigerstatterin zur privaten Kontaktaufnahme	58
6.4	Mitgliederdaten eines Anglervereins im Internet abrufbar	59

III	Anlasslose Prüfungen	61
1	Einhaltung der Betroffenenrechte beim Versand von Newslettern	61
2	Prüfung von Webseiten auf Cookies, Tracking und eingebundene Drittdienste	64
3	Technisch-organisatorische Prüfung nach einem Angriff auf die IT-Infrastruktur der Landeshauptstadt Potsdam	67

IV	Ausgewählte Fälle	71
1	Datenleck bei einem Fahrzeughersteller – unsere Rolle im europäischen Aufsichtsverfahren	71
2	Herausgabe von Protokolldaten einer Bank	74
3	Ein Mailserver, zwei Sicherheitslücken und kein Backup	76
4	Verlust von Gesundheitsdaten bei Transport und Aufbewahrung	78
5	Mitteilung der Arbeitsunfähigkeit per E-Mail	81
6	Veröffentlichung von Alarmmeldungen der Feuerwehr im Internet	84

V	Ausgewählte Beratungen	87
1	Schutz personenbezogener Daten bei der E-Mail-Kommunikation	87
2	Das Standard-Datenschutzmodell – ein Werkzeug zur Erfüllung datenschutzrechtlicher Anforderungen	92
3	Melddatenerhebung zur Beteiligung von Kindern und Jugendlichen in Gemeindeangelegenheiten	96
4	Gesetz zur Modernisierung des Kommunalrechts	99
5	Kinder- und Jugendgesundheitsdienst-Verordnung	103
6	18. Jahrestreffen mit den behördlichen Datenschutzbeauftragten	106

VI	Zahlen und Fakten	107
1	Beschwerden	107

2	Beratungen	107
3	Videoüberwachung: Beschwerden und Beratungen	108
4	Meldungen von Datenschutzverletzungen	111
5	Abhilfemaßnahmen	114
5.1	Warnungen, Verwarnungen, Anweisungen und Anordnungen	114
5.2	Geldbußen	115
6	Europäische Verfahren	116
7	Förmliche Begleitung von Rechtsetzungsvorhaben	118

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

1	Gesetz zur Verhinderung von Gewalt gegen Frauen und häuslicher Gewalt	121
2	Digitalisierungsprojekte bei der Polizei	127
3	Lernplattform zur Sensibilisierung für Datenschutz	129
4	Kontrolle personengebundener und ermittlungsunterstützender Hinweise in Kriminalakten	130
5	Geschwindigkeitsübertretung: Abruf personenbezogener Daten aus der Elektronischen Einwohnerakte	134
6	Zahlen und Fakten	136

Teil C: Die Dienststelle

1	Öffentlichkeitsarbeit	141
2	Pressearbeit	145
3	Personal und Organisation der Dienststelle	148

Vorwort

Liebe Leserinnen, liebe Leser,

mit dem vorliegenden Tätigkeitsbericht möchte ich Sie über wichtige datenschutzrechtliche Themen sowie über ausgewählte Beratungs- und Beschwerdefälle informieren, mit denen meine Dienststelle im vergangenen Jahr befasst war.

Ein Thema, an dem 2023 niemand vorbeikam, ist die Künstliche Intelligenz (KI). Untrennbar damit verbunden ist ChatGPT, ein Produkt des amerikanischen Unternehmens OpenAI für die KI-basierte Generierung von Texten zu beliebigen Themen. ChatGPT hat sich in beeindruckender Geschwindigkeit seinen Weg nicht nur in Schulen, Universitäten, Verwaltung und Wirtschaft gebahnt. Seit der Integration in einen häufig genutzten Webbrowser ist es auch im Alltag vieler Internetnutzerinnen und -nutzer angekommen. Die große öffentliche Aufmerksamkeit – verbunden mit datenschutzrechtlichen Diskussionen (z. B. zur Verwendung von Trainingsdaten oder zur Nutzung durch Kinder) – war der Anlass für mich, das Unternehmen OpenAI gemeinsam mit Kolleginnen und Kollegen der anderen unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Umsetzung der Vorgaben der Datenschutz-Grundverordnung anzuhören. Weitere Aspekte des Schwerpunktthemas Künstliche Intelligenz in diesem Bericht sind die Schaffung einer europaweit gültigen Rechtsvorschrift zur Regulierung von KI-Systemen sowie eine erste Handreichung für den Einsatz textgenerierender KI-Systeme in brandenburgischen Schulen.

Wie schon in der Vergangenheit habe ich mich auch im Berichtsjahr ausführlich mit Fragen der Digitalisierung der Verwaltung und der Umsetzung des Onlinezugangsgesetzes befasst. Eigentlich sollten bis Ende 2022 knapp 600 Verwaltungsdienstleistungen in Bund und Ländern digital für Bürgerinnen und Bürger bereitstehen. Diese Zahl wurde mittlerweile zwar deutlich nach unten korrigiert; gleichwohl gab es im Berichtszeitraum eine ganze Reihe von Umsetzungsprojekten. Im zweiten Schwerpunktthema gebe ich einen Einblick in ausgewählte Projekte und informiere über meine Beratungstätigkeit für brandenburgische Verwaltungen.




Auch die Facebook-Fanpages beschäftigen die Aufsichtsbehörden seit Jahren. Sowohl der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als auch die Sächsische Datenschutz- und Transparenzbeauftragte haben bereits den Betrieb solcher Seiten gegenüber jeweils einer öffentlichen Stelle in ihrem Zuständigkeitsbereich untersagt; hiergegen gibt es Klagen vor den Verwaltungsgerichten. Im Berichtszeitraum hat auch meine Dienststelle ein Verwaltungsverfahren mit dem Ziel, eine Untersagung auszusprechen, eingeleitet. Hierüber informiere ich im dritten Schwerpunktthema. Allerdings änderte der Meta-Konzern zum Jahresende die Cookie-Richtlinie für Facebook und stellt so erstmals Besucherinnen und Besuchern von Fanpages deutlich mehr Informationen zur Verfügung. Auch bietet er nunmehr ein werbefreies Abo-Modell für zahlende Nutzerinnen und Nutzer an. Für das Aufsichtsverfahren resultieren aus der geänderten Sachlage neue Prüfungen und Verzögerungen.

Immer wieder erhält meine Dienststelle Beschwerden über den unbefugten Abruf und den Missbrauch personenbezogener Daten durch Beschäftigte. Im Bericht der Bußgeldstelle werden hierzu Beispiele aus dem Bereich der Polizei und aus Krankenhäusern geschildert. Die Fälle sind auf Grund der Sensibilität der dort verarbeiteten Daten besonders gravierend, sodass ich gegen die Beschäftigten Bußgelder verhängt habe.

Brisant ist darüber hinaus der Fall der unzulässigen Erhebung von Gesundheitsdaten durch die Fahrerlaubnisbehörde der Landeshauptstadt Potsdam. Sie hatte über einen längeren Zeitraum Anträge schwerbehinderter Menschen auf Parkerleichterungen zum Anlass genommen, bei diesen Personen zusätzliche medizinische Daten abzufragen und ihre Fahrtauglichkeit zu überprüfen. Diese rechtswidrige Praxis habe ich genauso sanktioniert wie den Aushang krankheitsbedingter Abwesenheitszeiten in einem Unternehmen als „erzieherische Maßnahme“ der Leitung gegenüber den Beschäftigten. Aufsichtsrechtliche Maßnahmen musste ich im Berichtszeitraum auch erneut gegenüber mehreren Verantwortlichen wegen unzulässiger Videoüberwachungen verhängen.

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

Ihre

A handwritten signature in black ink, reading "Dagmar Hartge". The script is cursive and fluid, with the first letters of the first and last names being capitalized and prominent.

Dagmar Hartge





Bericht nach Artikel 59 Datenschutz-Grundverordnung

I	Schwerpunkte	13
II	Datenschutzverstöße: Maßnahmen und Sanktionen	41
III	Anlasslose Prüfungen	61
IV	Ausgewählte Fälle	71
V	Ausgewählte Beratungen	87
VI	Zahlen und Fakten	107

I **Schwerpunkte**

1 **Künstliche Intelligenz**

1.1 **Künstliche Intelligenz und Datenschutz**

Die Grundlagen für Künstliche Intelligenz (KI) als Teilgebiet der Informatik wurden bereits in den 1950er Jahren geschaffen. Dank des technischen Fortschritts der letzten Jahre sind entsprechende Anwendungen wie die Gesichtserkennung bei Fotos, die Generierung von Texten z. B. mittels ChatGPT oder teilweise autonom fahrende Fahrzeuge heute für viele Menschen bereits Teil ihres täglichen Lebens. Nicht immer sind sich die Nutzerinnen und Nutzer dessen auch bewusst, da Künstliche Intelligenz gerade in IT-Systemen oftmals schleichend Einzug hält. Hierbei stehen in der Regel die bessere Unterstützung der Anwenderinnen und Anwender bei Routineaufgaben, die Erleichterung des Umgangs mit der Flut an Informationen oder das Empfehlen von Handlungen aufgrund bisherigen Verhaltens im Vordergrund.

Obwohl die Künstliche Intelligenz keine ganz junge Wissenschaftsdisziplin mehr ist, gibt es je nach Sichtweise und Zweck unterschiedliche Definitionen. Die folgende Begriffsbestimmung aus einer Mitteilung des Europäischen Parlaments¹ liefert allerdings einen guten Einblick in das Themenfeld:

„Künstliche Intelligenz ist die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren. KI ermöglicht es technischen Systemen, ihre Umwelt wahrzunehmen, mit dem Wahrgenommenen umzugehen und Probleme zu lösen, um ein bestimmtes Ziel zu erreichen. ... KI-Systeme sind in der

1 Mitteilung des Europäischen Parlaments „Was ist künstliche Intelligenz und wie wird sie genutzt?“ vom 14. September 2020, siehe <https://www.europarl.europa.eu/news/>.

Lage, ihr Handeln anzupassen, indem sie die Folgen früherer Aktionen analysieren und autonom arbeiten.“

Zu bekannten Teildisziplinen der KI gehören u. a. Mustererkennung, Wissensmodellierung, Expertensysteme, Maschinelles Lernen, Künstliche Neuronale Netze und Deep Learning.

Bei KI-Systemen werden in der Regel die Lern- oder Trainingsphase und die Phase der eigentlichen Nutzung oder Anwendung unterschieden. Während in der erstgenannten Phase das jeweilige System aus existierenden Daten Informationen anhäuft, Wissen extrahiert und Modelle bildet, steht in der letztgenannten Phase die Anwendung und Weiterentwicklung der Modelle, das Ableiten von Schlussfolgerungen oder das Empfehlen von Verhalten im Vordergrund. Oftmals gibt es eine Rückkopplung, sodass Ergebnisse und ggf. ihre Bewertungen in die Selbstveränderung des Systems einfließen.

Sowohl während des Trainings als auch während der Nutzung sind bei der Mehrzahl von KI-Systemen personenbezogene Daten von Bedeutung. Insofern ergeben sich enge Bezüge zum Datenschutz; datenschutzrechtliche Anforderungen sind in allen Phasen des Lebenszyklus eines solchen KI-Systems zu beachten und einzuhalten. Hierzu gehören insbesondere die transparente und nachvollziehbare Verarbeitung der personenbezogenen Daten, die Beachtung der Grundsätze der Zweckbindung und der Datenminimierung, die Bestimmung und Umsetzung technischer und organisatorischer Maßnahmen zur Beherrschung der Risiken für die Rechte und Freiheiten betroffener Personen sowie die Einhaltung der Nachweis- und Rechenschaftspflicht. Alle genannten Punkte bergen große Herausforderungen für die jeweils Verantwortlichen.

Bereits im April 2019 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) die „Hambacher Erklärung zur Künstlichen Intelligenz“. In dieser formulierten die Aufsichtsbehörden sieben wesentliche datenschutzrechtliche Anforderungen an die Entwicklung und den Betrieb von KI-Systemen. Die Konferenz fordert u. a., dass Künstliche Intelligenz Menschen nicht zum reinen Objekt machen darf, sie nur für verfassungsrechtlich legitimierte Zwecke einzusetzen ist, Diskriminierungen vermieden werden müssen und klare Verantwortlichkeiten festzulegen sind.

Die Hambacher Erklärung wurde im November 2019 um das „Positionspapier der Datenschutzkonferenz zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen“ ergänzt. Das Papier erläutert die zu ergreifenden technischen und organisatorischen Maßnahmen im Sinne von Artikel 25 und 32 Datenschutz-Grundverordnung entsprechend dem Lebenszyklus von KI-Systemen und bezogen auf die datenschutzrechtlichen Gewährleistungsziele des Standard-Datenschutzmodells² (Datenminimierung, Transparenz, Nichtverkettung, Interventionsbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit). Sie sind bei der Entwicklung, dem Betrieb und der Anwendung von KI-Systemen zu beachten.

Im April 2021 veröffentlichte die Europäische Kommission einen Vorschlag für eine „Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union“. Der Entwurf dieser sogenannten KI-Verordnung enthielt das Ziel, die mit der Technologie einhergehenden Gefahren einzudämmen und sicherzustellen, dass nur vertrauenswürdige KI-Systeme zum Einsatz kommen. Er verfolgte einen risikobasierten Ansatz: KI-Systeme, die eine Bedrohung für die Sicherheit, die Lebensgrundlagen und die Rechte der Bürgerinnen und Bürger darstellen, sollten verboten werden. Für KI-Systeme, deren Einsatz in bestimmten Bereichen ein hohes Risiko für die Gesundheit oder Sicherheit birgt oder eine Beeinträchtigung der Grundrechte (beispielsweise auf Privatsphäre, Nichtdiskriminierung oder Datenschutz) mit sich bringt, sollten strenge Vorgaben gelten, bevor sie eingesetzt werden können.

Das Gesetzgebungsverfahren dauerte zum Ende des Berichtszeitraums an – bis zuletzt verhandelten EU-Kommission, Europäischer Rat und Europäisches Parlament im Trilog die konkreten Formulierungen der finalen Fassung der KI-Verordnung. Letztlich konnte im Dezember 2023 Einigkeit erzielt werden. Die Abstimmung im Parlament ist für das Frühjahr 2024 geplant. Ähnlich wie bei der Datenschutz-Grundverordnung wird es einen Übergangszeitraum von 24 Monaten zwischen dem Inkrafttreten der KI-Verordnung und ihrem

2 Siehe AV 2.

Wirksamwerden geben. Im Anschluss gilt die Verordnung unmittelbar in der gesamten Europäischen Union und ist damit voraussichtlich weltweit das erste Gesetz zur Regulierung von Künstlicher Intelligenz.

Im Vorfeld der zu erwartenden rechtlichen Regelungen und um uns einen Überblick über die aktuelle Situation im Land zu verschaffen, befragten wir im Berichtszeitraum eine Auswahl von in Brandenburg ansässigen Unternehmen, die die Entwicklung bzw. den Betrieb oder die Anwendung von KI-Systemen in die Beschreibung ihrer Geschäftstätigkeit aufgenommen hatten. Unser Ziel war dabei

KI – Brandenburg muss sich rüsten

ausdrücklich nicht die Einleitung von aufsichtsrechtlichen Verfahren. Vielmehr wollten wir die Verantwortlichen für einen datenschutzkonformen Umgang mit personenbezogenen Daten im Umfeld ihrer KI-Systeme sensibilisieren und auf die bisherigen Veröffentlichungen, insbesondere auf die o. g. Pa-

piere der Datenschutzkonferenz, aufmerksam machen. Im Ergebnis war festzustellen, dass die befragten Unternehmen in der Regel keine personenbezogenen Daten mittels KI verarbeiteten, dies für die Zukunft jedoch nicht ausschlossen. In dieser Hinsicht waren sie für unsere Hinweise dankbar.

Eine analoge Umfrage starteten wir auch bei den kommunalen Spitzenverbänden des Landes. Hier standen die Absichten bzw. Erfahrungen der Landkreise, Städte und Gemeinden beim Einsatz von KI-Systemen im Vordergrund. Im Ergebnis war festzustellen, dass es zwar erste Überlegungen und auch Pilotprojekte gibt – etwa zur Verwendung von Chatbots in der Kommunikation mit Bürgerinnen und Bürgern. Von einer flächendeckenden oder routinemäßigen Nutzung ist die Kommunalverwaltung in Brandenburg allerdings noch weit entfernt.

Unsere Behörde wurde außerdem in den Prozess der Erstellung der brandenburgischen Landesstrategie zum Thema „Künstliche Intelligenz“ eingebunden. Federführend ist hierbei das Ministerium für Wissenschaft, Forschung und Kultur. Im Rahmen eines Experteninterviews und eines Workshops zum Handlungsfeld „KI in der Verwaltung“ war es uns möglich, wesentliche datenschutzrechtliche sowie technisch-organisatorische Aspekte in die Diskussion einzubringen.

1.2 Mitwirkung bei der Prüfung von ChatGPT

Generative KI-Systeme sind derzeit in aller Munde. Mit ihnen lassen sich zu entsprechenden Eingaben (Prompts) z. B. passende Antworttexte oder Bilder erzeugen. Ein Beispiel für einen textbasierten Generator ist das System ChatGPT des Unternehmens OpenAI mit Sitz in Kalifornien. Die Trainingsdaten entstammen u. a. Büchern und literarischen Textsammlungen, Nachschlagewerken, Internetveröffentlichungen, Fachtexten und publizierten Briefwechseln. Bewertungen der generierten Antworten durch Nutzerinnen und Nutzer sowie Rückkopplungen fließen in die Weiterentwicklung des Systems ein.

Ende des ersten Quartals 2023 untersagte die italienische Datenschutzaufsichtsbehörde den Betrieb von ChatGPT in ihrem Zuständigkeitsbereich. Die Behörde hatte datenschutzrechtliche Mängel in Bezug auf die Transparenz und Rechtmäßigkeit der Verarbeitung personenbezogener Daten sowie hinsichtlich der Altersverifikation und der Einwilligung durch Minderjährige festgestellt. Nicht zuletzt diese Entwicklungen führten dazu, dass sich auch die anderen europäischen und speziell die deutschen Datenschutzaufsichtsbehörden intensiver mit ChatGPT beschäftigten. Auf europäischer Ebene wurde eine eigenständige Arbeitsgruppe eingerichtet; in Deutschland führte die seit 2019 existierende Taskforce „Künstliche Intelligenz“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz), an der auch unsere Behörde beteiligt ist, ihre Arbeiten fort.

In Abstimmung mit den europäischen Aufsichtsbehörden erstellte die Taskforce der Datenschutzkonferenz zunächst einen Fragebogen, der insbesondere die Themenbereiche Rechtsgrundlagen der Verarbeitung personenbezogener Daten, technische und organisatorische Maßnahmen sowie besonderer Schutz von Kindern und Jugendlichen umfasste. Die deutschen Aufsichtsbehörden forderten das Unternehmen OpenAI anschließend im Rahmen von Anhörungen auf, zu den einzelnen Fragen Stellung zu nehmen. Da OpenAI zu diesem Zeitpunkt keine Niederlassung in der Europäischen Union hatte und auch kein Vertreter gemäß Artikel 27 Datenschutz-Grundverordnung zu ermitteln war, ergab sich eine datenschutzrechtliche Prüf- und Kontrollzuständigkeit für jede einzelne Behörde.

Die Antworten von OpenAI im Rahmen der Anhörung lieferten nicht in allen Punkten Klarheit. Insofern ergänzten die deutschen Auf-

sichtsbehörden ihre Fragen und baten um eine zweite Stellungnahme. Die Antwortfrist wurde auf Bitten des Unternehmens verlängert und endete gegen Ende des Berichtszeitraums. Eine Auswertung der Antworten konnte deshalb bis zum Redaktionsschluss dieses Berichts nicht erfolgen. Allerdings hat OpenAI inzwischen eine europäische Niederlassung in Irland eröffnet. Damit wird die datenschutzrechtliche Prüf- und Kontrollzuständigkeit auf die irische Aufsichtsbehörde übergehen.

1.3 KI-Handreichung des Bildungsministeriums für Schulen

Spätestens mit dem Boom von text- bzw. bildgenerierenden Anwendungen der Künstlichen Intelligenz (KI) wurde das Thema für viele Menschen unmittelbar greifbar – auch in ihrem Alltag. Gerade textgenerierende KI-Anwendungen sind scheinbar in der Lage, auf beliebige Eingaben von Nutzerinnen und Nutzern (Prompts) fundiert zu antworten. Der Generator nutzt jeweils ein Sprachmodell, das im Vorfeld mit unzähligen Texten trainiert wurde, und erzeugt seine Reaktion auf der Basis mathematischer Wahrscheinlichkeiten. Die Antworten der KI sind deshalb nicht in jedem Fall korrekt und ihr Zustandekommen lässt sich (wenn überhaupt) nur schwer nachvollziehen. Ein hohes Maß an Medienkompetenz ist für den verantwortungsvollen Umgang gerade mit generativen KI-Anwendungen unerlässlich. Es ist daher richtig, wenn sich Schülerinnen und Schüler frühzeitig mit dem Thema Künstliche Intelligenz im Allgemeinen und textgenerierende KI-Anwendungen im Speziellen auch im Unterricht kritisch auseinandersetzen. Nur so können sie einen sachgerechten Umgang erlernen und die Grenzen bzw. Gefahren dieser Anwendungen besser einschätzen.

Das Themenfeld KI war im Berichtszeitraum auch für viele Schulen Neuland und sorgte bei Schulleitungen sowie Lehrkräften für große Verunsicherung. Daher war es wichtig, dass das Ministerium für Bildung, Jugend und Sport frühzeitig einen „Handlungsleitfaden zur Nutzung von textgenerierenden KI-Anwendungen an Schulen im Land Brandenburg“³ erarbeitete. Es gab damit einen ersten Rahmen für die Schulen vor, um die Auseinandersetzung mit KI-Anwendun-

3 https://mbjs.brandenburg.de/sixcms/media.php/140/handlungsleitfaden_zur_nutzung_von_textgenerierenden_ki-systemen.pdf

gen im Unterricht zu ermöglichen und gleichzeitig dafür Sorge zu tragen, dass der Einsatz nicht ungeregt erfolgt.

Der Handlungsleitfaden beleuchtet neben allgemeinen Fragen zum Begriff, zur Funktion und zur Leistungsfähigkeit textgenerierender KI-Anwendungen auch mögliche Einsatzszenarien, Risiken sowie rechtliche Voraussetzungen für den schulischen Einsatz. Die sehr komplexe Frage der Umsetzung datenschutzrechtlicher Anforderungen beim Einsatz von KI-Anwendungen in Schulen wird im Leitfaden jedoch nur ansatzweise betrachtet. Die Hinweise sehen insbesondere vor, dass keine personenbezogenen Daten in den Prompts enthalten sein dürfen. Außerdem sollten die Schülerinnen und Schüler im schulischen Kontext keine privaten und somit personalisierten Zugänge zu KI-Anwendungen nutzen.

Die Tatsache, dass das Ministerium mit diesen ersten Empfehlungen auf das generelle datenschutzrechtliche Problem beim Einsatz textgenerierender KI-Anwendungen aufmerksam macht, begrüßen wir. Allerdings sehen wir Handlungsbedarf, den Schulen mit darüber hinausgehenden Hinweisen, Empfehlungen und Vorgaben datenschutzrechtlich zur Seite zu stehen.

Aus diesem Grund nahmen wir mit den Verantwortlichen im Ministerium Kontakt auf und vereinbarten, Fortschreibungen und Ergänzungen des Handlungsleitfadens für Schulen künftig gemeinsam zu erarbeiten. Da KI-Anwendungen auch weiterhin eine erhebliche Rolle in der Gesellschaft spielen werden, muss vor allem die junge Generation für einen sachgerechten und kritischen Umgang mit Künstlicher Intelligenz sensibilisiert werden, datenschutzrechtliche und technische Herausforderungen sowie Risiken der Technologie kennen und auch den Einsatz von Mitteln zur Wahrung des Rechts auf informationelle Selbstbestimmung erlernen. Klar ist auch, dass die Auseinandersetzung mit KI-Anwendungen im Unterricht nicht verboten werden sollte. Ganz im Gegenteil: Schulen müssen bestmöglich unterstützt werden, um für die verschiedenen Einsatzszenarien einen differenzierten, auch datenschutzrechtlich abgesicherten Rahmen schaffen zu können. Nur so können sie ihrem Bildungsauftrag nachkommen.

Unterricht auch künstlich intelligent

2 Umsetzung des Onlinezugangsgesetzes zur Digitalisierung der Verwaltung

2.1 Orientierungshilfe zur Nachnutzung von Onlinediensten

Mit dem Onlinezugangsgesetz (OZG) schuf der Bundesgesetzgeber die Rahmenbedingungen dafür, dass die öffentliche Verwaltung ihre Dienstleistungen Bürgerinnen und Bürgern sowie Unternehmen auch elektronisch anbietet.⁴ Eine wesentliche Rolle bei der Umsetzung des Gesetzes sollte das „Einer für Alle“-Prinzip (EfA) spielen: Geplant war, dass jede der insgesamt knapp 600 identifizierten Verwaltungsdienstleistungen einem von 14 Themenfeldern zugeordnet, durch ein Bundesland zentral entwickelt und anschließend deutschlandweit zur Nachnutzung durch Bund, Länder und Kommunen bereitgestellt wird. Dieser Ansatz verfolgte das Ziel, den Entwicklungsaufwand für einzelne Behörden erheblich zu reduzieren und die Anzahl und Dichte der Dienstleistungsangebote zu erhöhen.

Auch wenn Umfang und Tempo bei der Umsetzung des OZG deutschlandweit Anlass zur Kritik geben, unterbreiteten verschiedene Themenfeldführer bzw. umsetzende Länder im Berichtszeitraum den Verantwortlichen im Land Brandenburg eine Reihe von Nachnutzungsangeboten für EfA-Onlinedienste. Oftmals erreichten unsere Behörde anschließend hierzu entsprechende Beratungsanfragen aus den brandenburgischen Verwaltungen. Auffällig war, dass sich in vielen Nachnutzungsprojekten auf Landes- und kommunaler Ebene ähnliche bzw. wiederkehrende datenschutzrechtliche Herausforderungen stellten. Insofern rückten hinsichtlich der Nachnutzung Fragen zur datenschutzrechtlichen Bewertung der EfA-Onlinedienste sowie zur praktischen Umsetzung der Projekte in den Blick der Landesbeauftragten.

Gerade kleinere, mit begrenzten Ressourcen ausgestattete Verwaltungen wünschten sich Orientierung und Hilfestellung bei den mitunter vielfältigen datenschutzrechtlichen und technischen Aktivitäten im Zuge der Einführung neuer Onlinedienste. Aber auch

4 Tätigkeitsbericht Datenschutz 2021, A I 1.

Landesministerien, die kommunale OZG-Projekte zur Nachnutzung von EFA-Onlinediensten koordinieren, wandten sich an uns. Mit dem für das landesweite OZG-Monitoring zuständigen Referat im Ministerium des Innern und für Kommunales erörterten wir daraufhin Möglichkeiten der Einbeziehung unserer Behörde bei konkreten Projekten. Im Ergebnis erarbeiteten wir eine Orientierungshilfe mit allgemeinen, unterstützenden datenschutzrechtlichen Hinweisen zur Nachnutzung von EFA-Onlinediensten für alle öffentlichen Stellen im Land.

Die Orientierungshilfe enthält zum einen Ausführungen zum Zusammenwirken der nachnutzenden Stellen mit dem jeweiligen Themenfeldführer. Insbesondere ist davon auszugehen, dass in dessen Verantwortung wesentliche Teile der aus Datenschutzsicht für einen rechtskonformen Betrieb des EFA-Onlinedienstes erforderlichen Dokumentation erarbeitet und der nachnutzenden Behörde zur Verfügung gestellt werden. Diese muss die Unterlagen mindestens auf Vollständigkeit und Plausibilität prüfen. Gegebenenfalls sind die Dokumente auch fortzuschreiben und lokale Anpassungen vorzunehmen. Eine nachnutzende Stelle kann ihrer datenschutzrechtlichen Nachweispflicht nur dann eigenständig nachkommen, wenn sie ein vollständiges Datenschutzkonzept bestehend aus zentral vom Themenfeldführer erarbeiteten Unterlagen und Anpassungen entsprechend der örtlichen Gegebenheiten und Festlegungen vorhält und bei Bedarf fortschreibt.

**Einer für alle –
eigene Aufgaben
bleiben**

Zum anderen werden in der Orientierungshilfe Probleme, die erfahrungsgemäß häufig bei der Nachnutzung von EFA-Onlinediensten auftreten, erörtert sowie praktikable Lösungsmöglichkeiten aufgezeigt. Dies beinhaltet etwa die in diesem Kontext oftmals schwierige Bestimmung der datenschutzrechtlichen Verantwortlichkeiten. Hieran ist insbesondere die Einhaltung der datenschutzrechtlichen Pflichten geknüpft, z. B. der Nachweis- und Rechenschaftspflicht, der Pflicht zur Gewährleistung der Betroffenenrechte oder der Pflichten bei Datenschutzverletzungen. Darüber hinaus geben wir Hinweise zur Auftragsverarbeitung, da EFA-Onlinedienste in der Regel nicht ohne (oft mehrere) Dienstleisterinnen und Dienstleister umgesetzt werden. In der Orientierungshilfe thematisieren wir landesspezifische datenschutzrechtliche Besonderheiten und bieten praktische Hilfestellungen z. B. zur Ermittlung von Risiken der Datenverarbei-



tion, zur Schwellwertanalyse, zur Datenschutz-Folgenabschätzung, zur Umsetzung von technischen und organisatorischen Maßnahmen sowie zum Verzeichnis von Verarbeitungstätigkeiten.

Gegenwärtig gehen wir davon aus, dass – ähnlich wie bei EfA-Onlinediensten mit dem Land Brandenburg als Themenfeldführer⁵ – die jeweils zuständigen Datenschutzaufsichtsbehörden diejenigen Projekte für EfA-Onlinedienste, die unter der Themenfeldführerschaft ihres Bundeslandes durchgeführt werden, aus datenschutzrechtlicher Sicht begleiten, beraten und ggf. auch prüfen. Ist dies der Fall, orientieren wir uns an den dort erzielten Ergebnissen und berücksichtigen diese bei unserer datenschutzrechtlichen Bewertung des jeweiligen Dienstes. Einerseits wäre es nicht zu vermitteln, dass unterschiedliche Aufsichtsbehörden in Deutschland zu unterschiedlichen Ergebnissen der Bewertung kommen, andererseits verfügt unsere Behörde nicht über die personellen und zeitlichen Ressourcen, jeden einzelnen EfA-Onlinedienst vollständig tiefgehend selbst zu prüfen. Ein entsprechender Austausch zu Anforderungen an und Ergebnissen bei der Umsetzung von EfA-Onlinediensten findet im Arbeitskreis „Verwaltung“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder statt, der unter unserem Co-Vorsitz steht.

Das Ministerium des Innern und für Kommunales übermittelte unsere Orientierungshilfe zusammen mit einem erläuternden Anschreiben an die OZG-Koordinatorinnen und -Koordinatoren der Staatskanzlei sowie der Ministerien, die kommunalen Spitzenverbände, den Brandenburgischen IT-Dienstleister, die Kommunale Arbeitsgemeinschaft „Technikunterstützte Informationsverarbeitung im Land Brandenburg“ und den Zweckverband Digitale Kommunen. Beschäftigte unserer Behörde haben die Inhalte zudem in Videokonferenzen vorgestellt, so z. B. beim „OZG-Koordinierenden-Austausch“ für die Landesverwaltung und bei der „Kommunalen OZG-Sprechstunde“ für die Landkreise, Städte und Gemeinden.

Bei datenschutzrechtlichen Unklarheiten oder Schwierigkeiten im Kontext von Umsetzungsprojekten zur Nachnutzung von EfA-Onlinediensten liefert die Orientierungshilfe unserer Behörde Hinweise

5 Siehe A I 2.2.

und Empfehlungen. Sie kann gleichzeitig als Arbeitsmittel dienen, um nach der Einführung eines solchen Dienstes das Datenschutzniveau aufrechtzuerhalten bzw. zu verbessern und das jeweilige Datenschutzkonzept kontinuierlich fortzuschreiben. Im Hinblick auf die geplante Novellierung des Onlinezugangsgesetzes⁶ werden wir uns erneut mit dem Dokument befassen und notwendige Anpassungen an neue gesetzliche Rahmenbedingungen vornehmen.

2.2 Begleitung der OZG-Projekte im Themenfeld „Ein- und Auswanderung“

Das Ministerium des Innern und für Kommunales des Landes Brandenburg ist deutschlandweit Themenfeldführer für Projekte zur Umsetzung des Onlinezugangsgesetzes (OZG) im Themenfeld „Ein- und Auswanderung“. Es entwickelt entsprechende Onlinedienste nach dem „Einer für Alle“-Prinzip (EfA), die auf kommunaler Ebene nachgenutzt werden können. Gegen Ende des Berichtszeitraums waren einzelne Dienste in über 140 Ausländerbehörden deutschlandweit im Einsatz.

Von Beginn an wurde unsere Behörde bei der Konzipierung und Umsetzung der Dienste einbezogen.⁷ Unsere datenschutzrechtliche Beratungstätigkeit setzten wir auch im Berichtszeitraum fort. Im Mittelpunkt standen dabei erneut die EfA-Onlinedienste „Aufenthaltstitel“ sowie „Aufenthaltskarten und aufenthaltsrelevante Bescheinigungen“. Unser Fokus richtete sich auf die umfangreiche datenschutzrechtliche und technische Dokumentation im Projekt, insbesondere das Datenschutzkonzept mit seinen verschiedenen Anlagen und die Betrachtungen zur Informationssicherheit.

Da im Rahmen der Entwicklung der genannten EfA-Onlinedienste die Dokumentationen bislang separat erstellt und gepflegt wurden, legten die Projektverantwortlichen besonderen Wert auf die Konsolidierung der getrennt vorliegenden Unterlagen. Dies ermöglichte es, Redundanzen und Inkonsistenzen zu beseitigen bzw. zu vermeiden – z. B. bei der Beschreibung der Datenkategorien, der Schutzbedarfsfeststellung, der Datenschutz-Folgenabschätzung und der Ableitung

6 Siehe A I 2.4.

7 Tätigkeitsberichte Datenschutz 2020, A V 1.2, sowie 2021, A I 1.2.

von technischen und organisatorischen Maßnahmen. Wir empfehlen jedoch, die Muster für bestimmte Dokumente, wie Datenschutzerklärungen oder das Verzeichnis der Verarbeitungstätigkeiten, auch weiterhin separat vorzuhalten. Im Hinblick auf die Datenschutzerklärungen wird für betroffene Personen so die Nachvollziehbarkeit und Transparenz der Datenverarbeitung erhöht, da Informationen zu verschiedenen Onlinediensten auch getrennt voneinander in verschiedenen Datenschutzerklärungen angeboten werden. Bezüglich des Verzeichnisses der Verarbeitungstätigkeiten ist ohnehin davon auszugehen, dass für unterschiedliche Verarbeitungstätigkeiten (hier: Antragsstrecken in Onlinediensten) unterschiedliche Verzeichniseinträge bestehen, die separat gepflegt und ggf. fortgeschrieben werden.

Mit dem Ministerium des Innern und für Kommunales erörterten wir darüber hinaus die verfahrensspezifischen Protokollierungen innerhalb der entwickelten Onlinedienste. Wir legten hierbei Wert auf eine detaillierte Beschreibung der Zwecke und Inhalte der Protokollierung, der möglichen Zugriffe auf Protokolle, der Protokollauswertungen sowie auf eine angemessene Aufbewahrungsfrist. Die Projektverantwortlichen sagten zu, entsprechende Präzisierungen in den Dokumenten vorzunehmen.

Als weiteren Diskussionspunkt thematisierte das Ministerium den sog. Rückkanal für Onlinedienste: Dieser gehört zur vollständigen Digitalisierung der Verwaltungsleistung und soll der zuständigen Ausländerbehörde ermöglichen, Informationen auf digitalem Weg an Antragstellerinnen und Antragsteller zu übermitteln (z. B. um über den Sachstand des Verfahrens zu informieren, Antragsunterlagen nachzufordern oder Unklarheiten im Antrag zu beseitigen). Während auf der technischen Plattform, auf der die Onlinedienste webbasiert angeboten werden, in der Regel alle Antragsdaten unmittelbar nach ihrer Übermittlung an die zuständige Ausländerbehörde gelöscht werden, müssen dort bei bestimmten Antragstellungen für den Rückkanal spezifische technische Informationen langfristig zwischengespeichert werden. Diese Informationen sind zumindest personenbeziehbar. Es scheint (auch aus Sicht des Ministeriums) jedoch fraglich, ob für eine solche Zwischenspeicherung gegenwärtig eine tragfähige Rechtsgrundlage existiert.

Wir werden die Umsetzung der EfA-Onlinedienste im OZG-Themenfeld „Ein- und Auswanderung“ und insbesondere das zuletzt genann-

te Problem weiter mit den Projektverantwortlichen erörtern. Dabei wird es auch wesentlich darauf ankommen, welche neuen bzw. geänderten rechtlichen Vorgaben der Bundesgesetzgeber mit der Novellierung des Onlinezugangsgesetzes treffen wird.⁸

2.3 Ausgewählte Einzelprojekte

2.3.1 Energiepreispauschale für Studierende

Der völkerrechtswidrige Angriffskrieg Russlands gegen die Ukraine hat auch globale Auswirkungen. Für die deutsche Bevölkerung und Wirtschaft machte sich dies u. a. durch gestiegene Energiepreise unmittelbar bemerkbar. Um für eine finanzielle Entlastung der eigenen Bevölkerung zu sorgen, beschloss der Bundestag gezielte Maßnahmen. So trat am 21. Dezember 2022 das Studierenden-Energiepreispauschalengesetz in Kraft. Dessen Ziel war es, durch einmalige Zahlung einer Energiepreispauschale in Höhe von 200 Euro einen schnellen und unbürokratischen Ausgleich für die gestiegenen Energiekosten bereitzustellen. Die Hilfeleistung richtete sich vor allem an Studentinnen und Studenten, die am 1. Dezember 2022 an deutschen Hochschulen immatrikuliert waren. Aber auch Schülerinnen und Schüler von Berufsfachschulen, Fach- und Fachoberschulen bestimmter Bildungsgänge waren für die Einmalzahlung antragsberechtigt. Die entsprechenden Anträge waren bis zum 30. September 2023 zu stellen.

Die Bundesländer wurden mit der Durchführung des Gesetzes beauftragt. Um trotz des hohen Zeitdrucks eine zügige und bundesweit einheitliche Lösung zu erarbeiten, bildeten sie gemeinsam mit dem Bund eine Arbeitsgruppe. Neben rechtlichen Vorgaben wie einer Muster-Rechtsverordnung und einer Verwaltungsvereinbarung entwarf die Arbeitsgruppe auch konkrete Prozesse und technische Umsetzungen für die Antrags-, Bewilligungs- und Auszahlungsverfahren.

Im Einzelnen war geplant, in jedem Bundesland zentrale Stellen für die Bearbeitung und Bewilligung der Anträge einzurichten. Die im Gesetz genannten Ausbildungsstätten mussten Listen aller Antrags-

8 Siehe A I 2.4.



berechtigten erstellen, die mindestens deren Namen, Vornamen und Geburtsdatum enthalten. Eine zentral zur Verfügung gestellte Software, der sogenannte Zugangscodegenerator, diente dazu, die Datensätze in den Listen zu verschlüsseln. Auch hierfür waren die Ausbildungsstätten zuständig. Der Zugangscodegenerator erzeugte zunächst für alle Antragsberechtigten jeweils einen individuellen Zugangscode und eine PIN. Die einzelnen Datensätze wurden anschließend um die jeweilige PIN erweitert und dann mit Hilfe des individuellen Zugangscode verschlüsselt. Jede Ausbildungsstätte musste den Antragsberechtigten ihren individuellen Zugangscode und ggf. auch die optionale PIN (für ein bestimmtes Authentisierungsverfahren) übermitteln. Die Listen mit den verschlüsselten Datensätzen wurden anschließend an die zentralen Stellen der jeweiligen Länder für die Bearbeitung der Anträge übersandt.

Auf der zentral eingerichteten Antragsplattform konnten Studierende im Anschluss die Anträge für die Einmalzahlung stellen. Neben dem durch die Ausbildungsstätten generierten Zugangscode benötigten sie hierfür ein BundID-Konto. Falls ein solches Konto mit der Vertrauensstufe „Basisregistrierung“ (d. h. ohne die eID-Funktion des Personalausweises, nur mit Benutzername oder E-Mail-Adresse und Passwort) verwendet wurde, war die PIN als zusätzlicher Faktor für die Authentisierung erforderlich. Durch die Angabe des Zugangscode bei der Antragstellung konnte die zuständige Bewilligungsstelle den zugehörigen Datensatz der antragstellenden Person, welcher ihr bislang nur verschlüsselt vorlag, entschlüsseln und den Antrag bearbeiten. Darüber hinaus erfolgte ein bundesweiter Abgleich der Anträge auf Dopplungen, um Mehrfachauszahlungen zu vermeiden. Nach der Bearbeitung wurden die Bescheide elektronisch per E-Mail übermittelt und im Fall der Bewilligung die Pauschale ausgezahlt.

Datenschutzaufsichtsbehörden waren in der o. g. Arbeitsgruppe nicht vertreten. Allerdings wandten sich einzelne Mitglieder aus den Ländern mit der Bitte um Beratung an ihre zuständige Aufsichtsbehörde. Nach einem kurzen Informationsaustausch beauftragte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) ihren Arbeitskreis „Verwaltung“ unter Vorsitz von Baden-Württemberg und Brandenburg mit der Erarbeitung einer Stellungnahme. Diese lag nach kurzer Zeit und intensiver interner Abstimmung vor; sie wurde von der Konferenz angenommen.

In der Stellungnahme benannte die Datenschutzkonferenz einige gravierende datenschutzrechtliche Mängel. Insbesondere führte sie aus, dass das Studierenden-Energiepreispauschalengesetz keine tragfähige Ermächtigung für die Länder enthielt, Rechtsverordnungen zur Legitimierung der Datenverarbeitung zu erlassen. Ohne eine passende Rechtsgrundlage blieben auch die Zuweisung der datenschutzrechtlichen Verantwortung für die zentrale Antragsplattform sowie der Abgleich der Antragsdaten auf Dopplungen. Darüber hinaus befasste sich die Konferenz mit einigen technisch-organisatorischen Fragen und zeigte Verbesserungsmöglichkeiten bei der Gestaltung des Antrags- und Bewilligungsverfahrens auf. Diese konnten im Projekt wegen des hohen Zeitdrucks nur teilweise Berücksichtigung finden.

Positiv hervorzuheben ist, dass der ursprüngliche Ansatz, die Daten der Antragsberechtigten pauschal gegenüber der Bewilligungsstelle offenzulegen, verworfen und stattdessen das oben beschriebene kryptografische Verfahren eingeführt wurde. Dies hatte zur Folge, dass die Bewilligungsstelle von den Ausbildungsstätten zunächst nur verschlüsselte Datensätze aller Antragsberechtigten erhielt. Für das Entschlüsseln eines konkreten Datensatzes benötigte sie den entsprechenden Zugangscodes, der ihr erst bei der Antragstellung mitgeteilt wurde. Durch dieses Vorgehen wurde das Risiko reduziert, dass die Bewilligungsstelle Daten von Personen zur Kenntnis nimmt, die zwar antragsberechtigt sind, aber keinen Antrag stellen. Der Kern des Problems blieb aber auch bei dieser Lösung bestehen: Personenbezogene Daten aller Antragsberechtigten quasi „auf Vorrat“ zu speichern (auch in verschlüsselter Form), ohne dass tatsächlich entsprechende Anträge vorlagen, war nicht erforderlich. Eine bessere Lösung wäre gewesen, erst nach Eingang eines Antrags den verschlüsselten Datensatz zu übermitteln. Der großen Eile geschuldet, schien jedoch das implementierte Verfahren hinnehmbar, da eine unbefugte Kenntnisnahme der Daten durch die Bewilligungsstelle faktisch verhindert wurde.

Ein weiterer Kritikpunkt an der Umsetzung betraf das Verfahren zur Authentisierung der Antragstellerinnen und Antragsteller. Für sie bestand der Zwang, ein BundID-Konto zu nutzen. Diese Vorgabe wäre sinnvoll gewesen für Studierende, die bereits über ein solches Konto mit dem Vertrauensniveau „substanziell“ oder „hoch“ verfügten. Für alle anderen Fälle hätte es mindestens eine gleichwertige Alternative ohne Verwendung der BundID gegeben: Denn ein herkömmliches

Nutzerkonto mit E-Mail-Adresse und Passwort (wie man es z. B. von Online-Shops kennt) hätte das gleiche Vertrauens- und Sicherheitsniveau erreicht wie die „Basisregistrierung“ eines BundID-Kontos, bei der die sich registrierende Person auf eine Bestätigung ihrer persönlichen Daten über die eID-Funktion des Personalausweises verzichtet. Im Antragsverfahren für die Einmalzahlung war vorgeschrieben, dass bei Verwendung eines BundID-Kontos mit der Vertrauensstufe „Basisregistrierung“ zusätzlich eine Authentisierung über die durch die Ausbildungsstätte erzeugte PIN vorzunehmen war. Diese Verfahrensweise hätte jedoch auch bei einem herkömmlichen Nutzerkonto ohne BundID umgesetzt werden können.

Im Ergebnis ist festzustellen, dass eine rechtzeitige und umfassende Einbindung der Datenschutzaufsichtsbehörden die beschriebenen datenschutzrechtlichen Defizite hätte verhindern können. Auch wenn im vorliegenden Fall die Pläne zur Zahlung der Energiepauschale zu unterstützen waren und ein hoher Zeitdruck bei der praktischen Umsetzung bestand, müssen in derartigen Projekten die datenschutzrechtlichen bzw. technischen Anforderungen in vollem Umfang erfüllt sowie die Rechte und Freiheiten der betroffenen Personen stets gewährleistet werden.

Auch schnelle Hilfe nur mit Datenschutz

2.3.2 Heizkosten: Härtefallhilfen für Privathaushalte

Die globalen Auswirkungen des völkerrechtswidrigen Angriffskriegs Russlands gegen die Ukraine stellen Deutschland vor große Herausforderungen. Mit verschiedenen Maßnahmepaketen sollten Bürgerinnen und Bürger u. a. wegen der stark gestiegenen Energiepreise entlastet werden. In diesem Rahmen forderte der Bundestag im Dezember 2022 die Bundesregierung per Beschluss auf, diejenigen privaten Haushalte, die sogenannte nicht leitungsgebundene Energieträger (wie Heizöl, Pellets, Kohle oder Flüssiggas) nutzen und besondere Preiserhöhungen zu verkraften hatten, durch finanzielle Hilfen zu unterstützen. Der Bund stellte für die Härtefallhilfen die Finanzmittel zur Verfügung. Die Umsetzung oblag den Ländern.

13 Bundesländer einschließlich Brandenburg schlossen sich daraufhin zusammen, um für das Projekt eine gemeinsame technische Lösung im Sinne des Einer-für-Alle-Prinzips (EfA) zu nutzen. Das Ministerium für Wirtschaft, Arbeit und Energie beauftragte die Investitionsbank des Landes Brandenburg (ILB), als brandenburgische

Bewilligungsstelle zu agieren und hierbei auf die zentrale technische Lösung der Länder als Antrags- und Bewilligungsplattform zurückzugreifen. Da die ILB bei der geplanten Umsetzung datenschutzrechtliche Bedenken hatte, wandte sie sich mit der Bitte um Beratung an uns. Dabei gab es enge zeitliche Restriktionen: Schon im Mai 2023 sollte die technische Lösung verfügbar sein; alle Anträge waren durch die betroffenen Haushalte bis zum 20. Oktober 2023 einzureichen – vorzugsweise über die elektronische Plattform.

Zunächst erörterten wir gemeinsam mit der ILB, welche personenbezogenen Daten für eine Antragstellung tatsächlich erforderlich waren. Ein wesentliches Problem bestand darin, dass aufgrund des Zeitdrucks bei der länderübergreifenden Umsetzung die Dokumente und Handlungsvorgaben teilweise inkonsistente oder gar widersprüchliche Informationen bzgl. des Antragsverfahrens enthielten. Wir machten die ILB frühzeitig darauf aufmerksam, damit sie für die notwendige Klarheit sorgen konnte. Ein weiteres Thema, das in diesem Zusammenhang erörtert wurde, war die Erstellung von Personalausweiskopien. Der Bund hatte vorgegeben, dass im Rahmen der digitalen Antragstellung eine Identitätsprüfung zur Betrugsprävention durchgeführt wird. Hierfür sollten die Antragstellerinnen und Antragsteller jeweils ein Foto der Vorder- und der Rückseite des Personalausweises sowie ein Foto von sich selbst mit der Personalausweisvorderseite auf die Antragsplattform hochladen. Mit der ILB stimmten wir ab, dass auch die Möglichkeit vorzusehen war, Anträge mit teilweise geschwärzten Ausweisdaten zu stellen. Hierfür musste abgeklärt werden, welche Daten des Personalausweises in jedem Fall erforderlich waren, damit auf mögliche Schwärzungen überflüssiger Daten hingewiesen werden konnte. Zu begrüßen ist, dass neben der digitalen eine gleichwertige postalische Antragstellung ermöglicht wurde, welche aufgrund des geringeren Betrugsrisikos ganz ohne Personalausweiskopien auskam und somit eine datensparsamere Alternative darstellte.

Da zu erwarten war, dass die ILB als Bewilligungsstelle Unterlagen für unvollständige Anträge nachfordert und Bescheide an die antragstellenden Haushalte übermittelt, besprachen wir datenschutzrechtliche Anforderungen für diese nachgelagerte Kommunikation. Unkritisch war der Fall der postalischen Antragstellung, da hier die weitere Kommunikation ausschließlich postalisch abgewickelt werden sollte. Im Fall eines digital gestellten Antrags war dagegen die E-Mail-Kommunikation vorgesehen, um Unterlagen nachzufordern

und Bescheide zu versenden. Wir wiesen darauf hin, dass die ILB keine E-Mails mit sensiblen Inhalten ohne Ende-zu-Ende-Verschlüsselung verschicken darf. Die Bank sagte zu, entsprechende Textbausteine datensparsam und möglichst ohne sensible Inhalte zu erstellen. Für den Fall der Nachforderung von Unterlagen durch die ILB besprachen wir, den antragstellenden Personen die Möglichkeit einzuräumen, die Unterlagen per Ende-zu-Ende-verschlüsselter E-Mail zu übersenden. Weil sie einen solchen Kommunikationsweg bereits bei den Corona-Hilfen umgesetzt hatte, gingen wir davon aus, dass die ILB hiermit keine Schwierigkeiten haben würde.

Bei der Auszahlung der Härtefallhilfen kam es auf eine möglichst schnelle Entlastung der privaten Haushalte an; die Umsetzung des Projekts erfolgte deshalb unter enormem Zeitdruck. Dies hatte zur Folge, dass trotz der datenschutzrechtlichen Bedenken der ILB und unserer frühen Einbeziehung nicht alle datenschutzrechtlichen Aspekte abschließend geklärt werden konnten. So ließ sich die komplexe Frage der Abgrenzung der datenschutzrechtlichen Verantwortlichkeit beim Einsatz des EfA-Dienstes aufgrund des hohen Abstimmungsbedarfs zwischen den Ländern und der Kürze der Zeit nicht vollumfänglich und rechtlich sauber lösen. Letztendlich resultierte daraus, dass die ILB ausschließlich für die Bearbeitung und Bescheidung der Anträge datenschutzrechtlich verantwortlich war, nicht jedoch für die Entgegennahme des Antrags, die Identitätsprüfung und die Auszahlung. Gleichwohl gelang es, Verbesserungen bei der Gestaltung des zentralen Antragsverfahrens und den von der ILB in eigener Regie durchgeführten Verarbeitungsschritten zu erwirken.

2.3.3 Förderung der Fortbildung zum beruflichen Aufstieg

Das Aufstiegsfortbildungsförderungsgesetz (AFBG) regelt die finanzielle Unterstützung von Menschen, die sich für ihr berufliches Fortkommen qualifizieren möchten. Insgesamt wird die Vorbereitung auf über 700 Abschlüsse, z. B. in Meister- oder Fachwirtkursen, gefördert. Zur Beantragung dieser staatlichen Leistung entwickelte das Land Sachsen-Anhalt als Themenfeldführer im Projekt „AFBG Digital“ ein webbasiertes Antragsportal, über das bundesweit Förderanträge eingereicht werden können. Das Portal wird durch einen externen IT-Dienstleister betrieben. Der Dienst selbst folgt dem „Einer für

Alle“-Prinzip – einem Grundgedanken des Onlinezugangsgesetzes (OZG) und der Verwaltungsdigitalisierung.⁹

In Brandenburg koordiniert das Ministerium für Wissenschaft, Forschung und Kultur die Einführung dieses EfA-Onlinedienstes. Datenschutzrechtlich verantwortlich sind die kommunalen Ämter für Ausbildungsförderung der Landkreise und kreisfreien Städte. Sie nehmen die Anträge entgegen, bearbeiten sie und entscheiden über die Förderung. Hierbei nutzen sie das Antragsportal und weitere Softwarekomponenten, die von dem o. g. IT-Dienstleister betrieben werden.

Wir wurden in diesem Zusammenhang durch das Ministerium um Beratung zu Fragen der Auftragsverarbeitung gebeten. Grundsätzlich ist jede einen EfA-Onlinedienst nachnutzende Stelle (hier die Ämter für Ausbildungsförderung) aufgrund ihrer datenschutzrechtlichen Verantwortlichkeit verpflichtet, die gesetzlichen Anforderungen der Auftragsverarbeitung zu erfüllen und einen entsprechenden Vertrag mit dem IT-Dienstleister abzuschließen. Im konkreten Fall wurde zusammen mit dem Dienstangebot auch ein Mustervertrag bereitgestellt, demzufolge allerdings das nachnutzende Bundesland – für Brandenburg das Wissenschaftsministerium – den Vertrag als Auftraggeber abschließen sollte. Dadurch ergibt sich jedoch die Problematik, dass den rechtlich verbindlich geregelten Einflussmöglichkeiten der eigentlich verantwortlichen Ämter für Ausbildungsförderung nicht angemessen Rechnung getragen wird.

Wir empfehlen deshalb, eine Kette von Auftragsverarbeitungsverträgen umzusetzen: Zwar kann das Ministerium einen Auftragsverarbeitungsvertrag mit dem IT-Dienstleister schließen. Es agiert aber seinerseits nicht als datenschutzrechtlich Verantwortlicher der Datenverarbeitung, sondern lediglich stellvertretend für die jeweils zuständigen Ämter für Ausbildungsförderung und ist insoweit selbst deren Auftragnehmer. Die Ämter ihrerseits schließen entsprechende Auftragsvertragsverträge mit dem Ministerium und können so mittelbar Einfluss auf die Dienstleistung beim IT-Dienstleister nehmen. Ein Vorteil dieser Lösung ist, dass der IT-Dienstleister nicht

⁹ Siehe A I 2.1.

mit jedem Amt einzeln einen Auftragsverarbeitungsvertrag abschließen muss, sondern eine Bündelung auf Länderebene stattfindet.

Inwieweit mit der geplanten Novellierung des Onlinezugangsgesetzes eine Neubewertung der Sachlage erforderlich wird, bleibt abzuwarten. Das parlamentarische Verfahren hierzu war zum Redaktionsschluss des Berichts noch nicht abgeschlossen. Es deutet sich jedoch bereits an, dass im Gesetz neue, spezifische Regelungen zur datenschutzrechtlichen Verantwortlichkeit des Betreibers bzw. der Betreiberin eines EfA-Onlinedienstes geschaffen werden.¹⁰

2.3.4 Wohngeld

Das Wohngeld ist eine finanzielle staatliche Unterstützung, die einkommensschwachen Personen hilft, ihre Kosten für Mietwohnungen oder selbst genutztes Wohneigentum zu tragen. Ein Onlinedienst zur Beantragung von Wohngeld wurde in den vergangenen Jahren unter der Themenfeldführung des Landes Schleswig-Holstein entwickelt. Das entsprechende Projekt ist Teil der Umsetzung des Onlinezugangsgesetzes (OZG) und folgt dem „Einer für Alle“-Prinzip (EfA).¹¹ Der Verfahrensbetrieb wird durch einen externen IT-Dienstleister übernommen.

In Brandenburg koordiniert das Ministerium für Infrastruktur und Landesplanung die Einführung dieses EfA-Onlinedienstes. Datenschutzrechtlich verantwortlich sind die kommunalen Wohngeldstellen in den Landkreisen und kreisfreien Städten. Im Berichtszeitraum wandte sich eine Reihe von behördlichen Datenschutzbeauftragten der Kommunen mit der Bitte um datenschutzrechtliche Stellungnahme bzw. Einschätzung zu verschiedenen Themenkomplexen an unsere Behörde.

In erster Linie ging es darum, Klarheit über die datenschutzrechtliche Verantwortlichkeit für den Onlinedienst zu schaffen. Darauf aufbauend wurden Fragen zur Ausgestaltung der (schriftlichen) Vereinbarungen, die zwischen den Beteiligten zu schließen waren, thematisiert. Und letztlich mussten die Beziehungen zwischen den

¹⁰ Siehe A I 2.4.

¹¹ Siehe A I 2.1.

allgemeinen datenschutzrechtlichen und den speziellen sozialrechtlichen Vorschriften beachtet werden. In mehreren Besprechungen mit den kommunalen Datenschutzbeauftragten, dem Ministerium und dem Themenfeldführer in Schleswig-Holstein erörterten wir die damit zusammenhängenden Aspekte. Allerdings gelangten wir bis zum Ende des Berichtszeitraums nicht in jedem Punkt zu einer abschließenden Lösung.

Ursprünglich war vom Themenfeldführer vorgesehen, dass die Wohngeldstellen Verträge zur Auftragsverarbeitung nach Artikel 28 Datenschutz-Grundverordnung (DS-GVO) mit dem in Anspruch genommenen IT-Dienstleister schließen. Das wäre auch aus unserer Sicht eine rechtlich tragfähige Lösung gewesen, die sowohl die datenschutzrechtlichen als auch die sozialrechtlichen Vorschriften berücksichtigt. Im Projektverlauf wurde die Variante jedoch verworfen und stattdessen eine gemeinsame Verantwortung nach Artikel 26 DS-GVO zwischen dem Themenfeldführer und den jeweiligen kommunalen Wohngeldstellen präferiert. Dies würde nach unserer Auffassung jedoch im Widerspruch zu den Vorschriften des Wohngeldgesetzes und der entsprechenden Durchführungsverordnung des Landes Brandenburg stehen. Nach diesen Vorschriften sind allein die Wohngeldstellen für die Durchführung des Wohngeldgesetzes zuständig – also auch für die damit verbundene Verarbeitung personenbezogener Daten. Eine datenschutzrechtliche Verantwortung des Themenfeldführers ergibt sich daraus mangels Aufgabenzuweisung nicht.

Analog stehen wir der mit der Umsetzung des EfA-Onlinedienstes einhergehenden Trennung des Verfahrens zur Beantragung von Wohngeld vom Verfahren zur Bearbeitung und Bescheidung der Anträge kritisch gegenüber. Diese Einschätzung gilt gerade aus Sicht der betroffenen Personen und der Wahrung des Sozialgeheimnisses. Dem Themenfeldführer fehlt aus unserer Sicht schon eine tragfähige Rechtsgrundlage zur Verarbeitung personenbezogener Daten der Antragstellerinnen und Antragsteller (hier zur Erhebung der Antragsdaten). Darüber hinaus verlangen die sozialrechtlichen Vorschriften, dass Sozialdaten durch Leistungsträgerinnen bzw. Leistungsträger (hier die Wohngeldstellen) nicht unbefugt verarbeitet und auch innerhalb der Organisationseinheit nur Befugten zugänglich gemacht werden dürfen. Der Themenfeldführer ist jedoch wegen der fehlenden Aufgabenzuweisung schon kein Leis-

Sozialdaten – wer hat den Hut auf?

tungsträger im Sinne des Sozialrechts – eine konsequente Wahrung des Sozialgeheimnisses scheint fraglich.

Auch wenn mit der geplanten Novellierung des Onlinezugangsgesetzes¹² neue Vorschriften zur Zuweisung der datenschutzrechtlichen Verantwortung sowie zur Zulässigkeit der Verarbeitung personenbezogener Daten für Betreiberinnen und Betreiber von OZG-Online Diensten geschaffen werden sollen, bleiben Fragen nach dem Verhältnis dieser Regelungen zu jenen des Sozialrechts ungeklärt. Wir werden uns hierzu auch mit den Kolleginnen und Kollegen der anderen Datenschutzaufsichtsbehörden austauschen.

2.4 Novellierung des Onlinezugangsgesetzes

Das Onlinezugangsgesetz (OZG) wurde bereits 2017 vom Bundestag mit Zustimmung des Bundesrates beschlossen; es trat in demselben Jahr in Kraft. Unter Berücksichtigung der Erfahrungen bei der Umsetzung dieses Gesetzes und der Schwierigkeiten bei der flächendeckenden Bereitstellung von Onlinediensten der öffentlichen Verwaltung erarbeitete das Bundesministerium des Innern und für Heimat eine Novelle – das sogenannte OZG 2.0. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) richtete ihrerseits eine Kontaktgruppe „OZG 2.0“ unter Vorsitz der Berliner Beauftragten für Datenschutz und Informationsfreiheit ein, die den Prozess aus datenschutzrechtlicher Sicht begleiten und in Gesprächen mit dem Bundesministerium die datenschutzrechtlichen Anforderungen in das Gesetzgebungsverfahren einbringen sollte.

Nach verschiedenen Abstimmungsrunden, Gesprächen auf Arbeitsebene und schriftlichen Stellungnahmen der Kontaktgruppe der Datenschutzkonferenz lag im Berichtszeitraum zunächst ein Referentenentwurf zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften vor. Das Ministerium des Innern und für Kommunales des Landes Brandenburg war im Rahmen der Länderbeteiligung mit dem Entwurf befasst und räumte uns die Gelegenheit ein, zu diesem Stellung zu nehmen. Die Möglichkeit zur Kommentierung

12 Siehe A I 2.4.

nahmen wir wahr und bauten dabei auf den Ergebnissen der Kontaktgruppe der Datenschutzkonferenz auf.

In unserer Stellungnahme stellten wir fest, dass viele Anmerkungen und Hinweise der Datenschutzaufsichtsbehörden bereits Eingang in den Entwurf gefunden hatten. Positiv hoben wir u. a. hervor, dass die gesetzliche Definition des Begriffs „Antragsassistent“ im Vergleich zu früheren Versionen präziser war.¹³ Auch die neu geschaffene Regelung zur ausdrücklichen Zuweisung der datenschutzrechtlichen Verantwortlichkeit an die Betreiberin bzw. den Betreiber eines Antragsassistenten war grundsätzlich zu begrüßen, da dadurch diesbezügliche Schwierigkeiten, die in vielen OZG-Umsetzungsprojekten auftraten, vermieden werden konnten. Gleiches galt für die explizite Schaffung einer Rechtsgrundlage zur Verarbeitung personenbezogener Daten für den Betrieb eines Antragsassistenten. In der Gesamtschau blieb allerdings fraglich, welche Auswirkungen sich aus diesen Neuregelungen für andere Nachnutzungsmodelle von Onlinediensten im Sinne des OZG ergeben. Auch die bereits an anderer Stelle¹⁴ angesprochene Kollision mit spezialgesetzlichen Aufgabenzuweisungen verursachte einen erheblichen Klärungsbedarf.

Weiter thematisierten wir in der Stellungnahme u. a. die vorgesehene zentrale Bereitstellung des einheitlichen Bürgerkontos durch den Bund, die Migration existierender Bürgerkonten zum Angebot des Bundes, die Verschlüsselung von personenbezogenen Antragsdaten bei einer ggf. längerfristigen Speicherung, das Sicherheitsniveau bei der Identifizierung und Authentisierung für den Identitätsnachweis der antragstellenden Person oder die Verknüpfung von Behördenerklärungen mit einer qualifizierten elektronischen Signatur.

Der von uns kommentierte Referentenentwurf ist mittlerweile nicht mehr aktuell. Seit Mitte des Berichtsjahres liegt ein Gesetzentwurf der Bundesregierung zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung vor. Er befindet sich zum Redaktionsschluss dieses Berichts noch immer

13 Der Begriff „Antragsassistent“ wird im endgültigen Gesetzentwurf der Bundesregierung nicht mehr verwendet. Er wurde dort durch den ähnlich definierten Begriff „Onlinedienst“ ersetzt.

14 Siehe A I 2.3.4.



im parlamentarischen Verfahren. Es bleibt abzuwarten, welche konkreten Regelungen in der finalen Fassung enthalten sein werden und welche Auswirkungen sich daraus für aktuelle und geplante OZG-Umsetzungsprojekte ergeben.

3 Betrieb von Facebook-Fanpages durch öffentliche Stellen

In unserem letzten Tätigkeitsbericht¹⁵ haben wir ausführlich über unsere Prüfung des Betriebs von Facebook-Fanpages durch die Landesregierung Brandenburg berichtet. Das aufsichtsrechtliche Verfahren wird in Absprache mit der Landesregierung zunächst als Musterverfahren gegen die Facebook-Präsenz der Staatskanzlei „Unser Brandenburg“ geführt. Ein ggf. gerichtlich bestätigtes Ergebnis des Verfahrens soll dann auf die übrigen Landesbehörden übertragen werden, die ebenfalls Facebook-Fanpages betreiben. Das Interesse an der Klärung der Zulässigkeit von Facebook-Fanpages öffentlicher Stellen besteht nach unserem Eindruck auf beiden Seiten.

Die Staatskanzlei hatte bestritten, für die im Rahmen des Betriebs der Facebook-Fanpage anfallende Datenverarbeitung mitverantwortlich zu sein. Dies stützte sie insbesondere darauf, dass Meta, der Mutterkonzern von Facebook, die sogenannte Insights-Funktion für die Fanpage der Staatskanzlei abgeschaltet hatte. Diese Funktion ermöglicht es, verschiedene Statistiken und Analysen zu den Besuchen der Fanpage zu erhalten, beispielsweise um das Angebot zu optimieren. Im Ergebnis kommt es auf den Betrieb der Insights-Funktion bei der gemeinsamen Verantwortlichkeit jedoch nicht an, sodass diese auch ohne die Funktion fortbesteht. Die rechtmäßige Übernahme der Verantwortlichkeit konnte die Staatskanzlei bisher nicht nachweisen.

Die Landesbeauftragte hatte sich deshalb entschlossen zu prüfen, ob eine Untersagungsverfügung nach Artikel 58 Absatz 2 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) zu erlassen ist. Dabei stimmte sie sich mit anderen deutschen Datenschutzaufsichtsbehörden eng ab. Inzwischen haben zwei von ihnen – der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Sächsische Datenschutz- und Transparenzbeauftragte – jeweils einer öffentlichen Stelle den Betrieb der Fanpage untersagt. In beiden

15 Tätigkeitsbericht Datenschutz 2022, A I 1.

Fällen haben die Verantwortlichen das zuständige Verwaltungsgericht angerufen.

Unsere Anhörung der Staatskanzlei zum beabsichtigten Erlass einer Untersagungsverfügung basierte auf Erkenntnissen, die eine Taskforce der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) zuvor unter Berücksichtigung der einschlägigen Rechtsprechung erstellt und im weiteren Verlauf fortgeschrieben hatte. Unter anderem enthält das Gutachten die begründete Feststellung, dass eine Abschaltung der Insights-Funktion an der Mitverantwortung der Betreiberin oder des Betreibers der Facebook-Fanpage nichts ändert.

Zusätzlich verstärkt werden die Argumente der Datenschutzaufsicht durch ein Urteil des Europäischen Gerichtshofs vom 4. Juli 2023 (Rechtssache C-252/21). Danach können die Datenverarbeitungen von Facebook nicht ohne Weiteres auf Artikel 6 Absatz 1 Buchstabe b bis f DS-GVO gestützt werden. Das Urteil erschwert im Ergebnis auch die bisher von Meta versuchte Umgehung von Datenschutzrechten betroffener Personen, insbesondere durch individuelle Verträge.

Zwischenzeitlich hat Meta auf das Urteil des Europäischen Gerichtshofs reagiert und bietet neben dem werbefinanzierten Angebot noch ein kostenpflichtiges, werbefreies Abonnement an. Verschiedene Arbeitsgremien deutscher und europäischer Datenschutzaufsichtsbehörden prüfen die Zulässigkeit derartiger Abo-Modelle. Ein Ergebnis der Prüfung lag zum Zeitpunkt des Redaktionsschlusses dieses Berichts noch nicht vor.

Es ist derzeit eher unwahrscheinlich, dass hieraus eine grundlegend andere Beurteilung des Fanpage-Betriebs folgen wird. Bereits aus

Facebook-Fanpages weiter auf dem Prüfstand

der Erläuterung der Bedingungen des Abonnements geht lediglich hervor, dass der Nutzerin bzw. dem Nutzer nach Vertragsabschluss keine Werbung mehr eingeblendet wird. Die Freiheit von Werbung, so lästig sie für manche auch sein mag, ist aber kein Ziel des Datenschutzes. Der Datenschutz zielt in diesem Zusammenhang vielmehr auf eine rechtskonforme Verarbeitung personenbezogener Daten bei der

Ausspielung von Werbung. Die Frage, inwieweit die hierfür unternehmen, intransparenten und umfassenden Datenverarbeitun-

gen weiter stattfinden, wird in der Kommunikation durch Meta ausgespart. Wie bereits im Falle der Abschaltung der Insights-Funktion dürfte unseres Erachtens jedenfalls mit dem Verzicht auf Werbeeinblendungen gegen Geld kein Verzicht auf die Verfolgung des Nutzerverhaltens mit dem Ziel der Gewinnung wirtschaftlich nutzbarer Erkenntnisse einhergehen.

Zum 12. Dezember 2023 änderte Meta überraschend seine Cookie-Richtlinie u. a. dahingehend, dass zum ersten Mal konkret benannte Cookies konkreten Zwecken zugeordnet wurden. Da sich unsere Anhörung maßgeblich auf die den Nutzerinnen und Nutzern bisher erteilten Informationen zu den Cookies gestützt hatte, entschied die Landesbeauftragte, das Verfahren bis zur Analyse der neuen Richtlinie auszusetzen.



II **Datenschutzverstöße: Maßnahmen und Sanktionen**

1 **Geplante Videoüberwachung eines Stadtfestes**

Im Sommer 2023 fand in der Landeshauptstadt Potsdam ein Stadtfest statt. Kurz zuvor wandte sich die private Veranstalterin, eine Gesellschaft, an uns und erkundigte sich nach der Zulässigkeit einer Videoüberwachung. Damit sollte der Besucherstrom zu dem frei zugänglichen Festgelände kontrolliert und gelenkt werden. Geplant war eine Livebild-Beobachtung mit insgesamt 12 Kameras an 4 Kameratürmen aus einer Höhe von ca. 6 m. Die gewählte Auflösung verhindere das Identifizieren von Personen, so die Veranstalterin. Der Einsatz von Personal als Streckenposten vor Ort und Zählmethoden ohne Datenerfassung seien geprüft, aber als nicht ausreichend effektiv, fehleranfällig und wegen hoher Personalkosten verworfen worden.

Das geplante Vorhaben stellte sich nach Prüfung der eingereichten Unterlagen als datenschutzrechtlich unzulässig dar. Im näheren Umfeld der Kameratürme war mit einer Bildqualität zu rechnen, welche die Identifizierung der Besucherinnen und Besucher sowie der Beschäftigten auf dem Festgelände jedenfalls unter Berücksichtigung weiterer Umstände, z. B. des Gangbilds, der Uhrzeiten oder des Mitführens von Kinderwagen, ermöglicht hätte.

Die Datenschutz-Grundverordnung (DS-GVO) sieht für die Verarbeitung personenbezogener Daten mittels Videoüberwachung grundsätzlich ein Verbot mit Erlaubnisvorbehalt vor. Das bedeutet, dass eine Videoüberwachung grundsätzlich unzulässig ist, es sei denn, die Betroffenen haben eingewilligt oder eine andere Rechtsgrundlage erlaubt ausnahmsweise die Datenverarbeitung. Allein das Betreten des Festgeländes in Kenntnis der Videoüberwachung durch eine Hinweisbeschilderung erfüllt die Anforderungen an eine Einwilligung nicht. Die Videoüberwachung konnte auch nicht auf Artikel 6 Absatz 1 Buchstabe f DS-GVO gestützt werden. 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.

Die Gewährleistung der Sicherheit durch eine Besucherstromsteuerung und die Minimierung potenzieller Sicherheitsrisiken stellten dem Grunde nach zwar berechnete Interessen der Veranstalterin dar. Allerdings war die geplante Videoüberwachung zur Erreichung der angegebenen Zwecke nicht erforderlich, da mildere Maßnahmen zur Verfügung standen, mit denen weniger intensiv in die Rechte der Gäste und des Standpersonals eingegriffen worden wäre. Beispielsweise kam der Einsatz von zusätzlichen Sicherheitskräften an neuralgischen Punkten und von mobilen Absperrgittern oder sogenannten Wellenbrechern in Betracht, um bei drohender Überfüllung sofort einschreiten zu können. Darüber hinaus hätten – selbst bei gegebener Erforderlichkeit – im Rahmen der vorzunehmenden Interessenabwägung die grundrechtlich geschützten Interessen der Besucherinnen und Besucher, die flächendeckend und anlasslos im Rahmen ihrer Freizeitgestaltung videoüberwacht worden wären, gegenüber den Interessen des Veranstalters überwogen. Dies galt in besonderem Maß für Kinder. Zu berücksichtigen waren zudem die Interessen der auf dem Festgelände tätigen Beschäftigten, die sich der Videoüberwachung und dem damit einhergehenden Überwachungsdruck nicht hätten entziehen können.

Feiern unter Beobachtung

Zwar sagte die Veranstalterin nach der Mitteilung des Prüfergebnisses zu, von dem Einsatz der Videokameras Abstand zu nehmen und Alternativen zu planen. Gleichwohl sprachen wir ihr gegenüber eine Warnung nach Artikel 58 Absatz 2 Buchstabe a DS-GVO aus, da die ursprünglich beabsichtigte Videoüberwachung datenschutzrechtlich unzulässig gewesen wäre. Letztlich verzichtete die Veranstalterin – wie zugesichert – auf die Videoüberwachung, wovon wir uns vor Ort überzeugten.

2 Videokameras in Ferienwohnanlagen

Im Berichtszeitraum erreichten uns mehrere Beschwerden von Bürgerinnen und Bürgern, die als Gäste von Ferienwohnanlagen festgestellt hatten, dass diese mittels Videokameras überwacht wurden. Hierbei wurden zwar keine Innenräume der einzelnen Wohnungen erfasst, sehr wohl aber gemeinschaftlich genutzte Eingangsbereiche, Flure und Gänge, Gärten, Wege, Parkplätze, Außenschwimmb Becken sowie privat von den Gästen genutzte Außenterrassen. Dabei lagen in einem Fall auch benachbarte Grundstücke und Wohnhäuser teilweise im Erfassungsbereich. Gäste, deren Familienangehörige, Freundinnen und Freunde und Bekannte sowie die unmittelbaren Nachbarinnen und Nachbarn auf ihren Wohngrundstücken und Dritte, die sich dort aufhielten, wurden von den Videokameras gefilmt.

In einem Fall teilte uns der Verantwortliche mit, dass die Videokameras lediglich zu den vereinbarten An- und Abreisezeiten der Gäste, während der nächtlichen Ruhezeiten sowie außerhalb der Vermietungszeiten in Betrieb seien. Darüber hinaus werde eine Bildübertragung in Echtzeit auf das Mobiltelefon des Verantwortlichen durch Bewegung ausgelöst. Im zweiten gemeldeten Fall wurden Videosequenzen sogar aufgenommen und für bis zu sieben Tage gespeichert.

In beiden Fällen gaben die Verantwortlichen an, dass auf den Umstand der Videoüberwachung hingewiesen oder vorab eine ausdrückliche Einwilligungserklärung eingeholt würde. Zudem gingen beide Verantwortliche davon aus, dass im Betreten des Erfassungsbereichs in Kenntnis der Videoüberwachung eine Zustimmung zu sehen sei.

Die Verantwortlichen gaben diverse Zwecke der Videoüberwachung an: die Wahrnehmung des Hausrechts, die Zutrittskontrolle und Verhinderung unangekündigter Mehrbelegungen, den Eigentumsschutz, die Geltendmachung von Ansprüchen, die Verhinderung und Verfolgung von Straftaten, die Gewährleistung des ordnungsgemäßen Verschließens der Türen, die Sicherheit des Verantwortlichen und der anderen Gäste beim Aufenthalt auf dem Gelände sowie die Vorbeugung gegen Beschwerden wegen Lärmbelästigung. Überdies sollte durch die Videoüberwachung die kontaktlose An- und Abmeldung der Gäste ermöglicht werden.



Nur in einem Fall wurden konkrete Vorkommnisse aus der Vergangenheit, die Anlass zur Videoüberwachung gaben, durch den Verantwortlichen genannt. Die behaupteten regelmäßigen Diebstähle des Inventars durch Gäste, die geschilderten buchungswidrigen Überbelegungen oder die Fälle von Beschwerden wegen Ruhestörungen wurden jedoch nicht durch entsprechende Nachweise belegt.

Wir bewerteten die Videoüberwachung in rechtlicher Hinsicht wie folgt:

In keinem der beiden Fälle ließ sie sich nach Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) rechtfertigen. Grundsätzlich gilt, dass eine Videoüberwachung durch nicht öffentliche Stellen, von der andere Personen betroffen sind, nach Artikel 6 Absatz 1 DS-GVO nur zulässig ist, wenn alle Betroffenen eingewilligt haben oder die Überwachung auf eine gesetzliche Erlaubnisnorm gestützt werden kann.

Nachweise über eine schriftlich dokumentierte Einwilligung aller Betroffenen gemäß Artikel 6 Absatz 1 Buchstabe a, Artikel 7 i. V. m. Artikel 4 Nummer 11 DS-GVO wurden uns nicht vorgelegt. Auch das Betreten der Erfassungsbereiche in Kenntnis der Videoüberwachung nach Lesen der Hausordnung oder Kenntnisnahme der Hinweisbeschilderung war nicht als Einwilligungserklärung zu werten, da Stillschweigen oder Untätigkeit gemäß Satz 3 des Erwägungsgrundes 32 der Datenschutz-Grundverordnung gerade keine Einwilligung darstellen.

In keinem Fall konnte die Videoüberwachung nach Artikel 6 Absatz 1 Buchstabe b DS-GVO gerechtfertigt werden, da die Datenverarbeitung für die Erfüllung der Mietverträge über die Ferienwohnungen nicht erforderlich war.

Die Zulässigkeit der Videoüberwachung hätte sich allenfalls aus Artikel 6 Absatz 1 Buchstabe f DS-GVO ergeben können. Nach dieser Vorschrift ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und sofern nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dabei sind die Interessen betroffener Kinder besonders zu gewichten.

Berechtigte Interessen des Artikels 6 Absatz 1 Buchstabe f DS-GVO können rechtlicher, wirtschaftlicher oder ideeller Art sein. Die seitens der Verantwortlichen genannten Zwecke waren berechtigt. Allerdings konnten die jeweiligen Videoüberwachungen Diebstähle oder anderes regelwidriges Verhalten, wie eine buchungswidrige Überbelegung, nicht unterbinden. Dies musste insbesondere für die Videoüberwachung mit Bildspeicherung gelten. Nur bei einer dauerhaften Echtzeitbildbeobachtung rund um die Uhr wäre es möglich, im „Ernstfall“ zu reagieren. Zudem schied eine Erforderlichkeit der Videoüberwachung aus, da jeweils mildere Alternativmaßnahmen zur Verfügung standen, um die angestrebten Zwecke zu erreichen. Als mildere Mittel wären eine Alarmanlage oder zusätzliche Zutritts- oder Zugriffsbeschränkungen, wie einbruchsichere bzw. automatisch zuschnappende Türen, vermehrte personelle Präsenz beim An- und Abmelden, eine Inventarisierung der Einrichtungsgegenstände sowie die Installation einer durch Bewegungsmelder gesteuerten Beleuchtungsanlage in Betracht gekommen. Darüber hinaus wäre in einem der Fälle die zeitliche Beschränkung der Aktivierungszeiten der Videokameras auf Zeiten außerhalb der Vermietung oder hinsichtlich der Ruhestörungen eine entsprechende Hinweisbeschilderung und persönliche Anmahnung denkbar gewesen. Höhere Kosten und ein größerer Aufwand – etwa durch den Einsatz von zusätzlichem Personal oder vermehrte persönliche Präsenz – führen nicht dazu, die Alternativmaßnahmen von vornherein außer Betracht zu lassen. Hinsichtlich erfasster Personen auf benachbarten Grundstücken war ein berechtigtes Interesse der Verantwortlichen an der Videoüberwachung bereits von Anfang an nicht anzunehmen.

Auch bei unterstellter Erforderlichkeit hätten die Videoüberwachungen nicht auf die Rechtsgrundlage des Artikels 6 Absatz 1 Buchstabe f DS-GVO gestützt werden können, da die Interessenabwägung zugunsten der betroffenen Personen ausfiel. Die Videoüberwachung erfasste neben gemeinschaftlich genutzten Innen- und Außenbereichen u. a. Terrassen, auf denen Gäste verweilten, und in einem Fall sogar einen Pool, in bzw. an dem sie sich leicht bekleidet aufhielten. Solche Bereiche sind dazu bestimmt, dass sich Menschen dort in privatem Rahmen mit anderen oder alleine entspannen. Wegen der damit einhergehenden Interaktionen und Verhaltensweisen kann eine Videoüberwachung in diesen Bereichen in erheblicher Weise Aufschluss über den persönlichen Lebensbereich und die nach dem Grundgesetz besonders geschützte Privatsphäre geben. Eine Videoüberwachung in solchen schutzwürdigen Bereichen stellt



einen erheblichen Eingriff dar. Dies gilt nicht nur für Personen, die solche Wohnungen zu Urlaubszwecken anmieten, sondern auch im Falle von Handwerkerinnen und Handwerkern, die dort auf Montage übernachten. Es bestand überdies keine Möglichkeit für die Betroffenen, sich dem Erfassungsbereich zu entziehen. Somit war das Erstellen von Bewegungsprofilen möglich, womit ein hohes Risiko für die Rechte der Betroffenen verbunden sein kann. Zudem müssen

Ferien unter Beobachtung

Gäste einer Ferienwohnanlage nicht typischerweise mit einer Videoüberwachung rechnen. Auch Hinweisschilder vermögen nichts an diesem objektiven Erwartungshorizont zu ändern. Zudem war zu berücksichtigen, dass sich die meisten Gäste rechtstreu verhielten und erfasst wurden, ohne einen Anlass gegeben zu haben. Überdies war aufseiten der Betroffenen zu beachten, dass deren Bilddaten durch die Speicherung für eine weitere Aufbereitung, Auswertung und Verknüpfung mit anderen Informationen zur Verfügung standen und so einem Missbrauchsrisiko ausgesetzt waren.

Ebenso wenig wurde jeweils ein Nachweis erbracht, dass auf den Grundstücken eine erhöhte konkrete Gefahr sich wiederholender oder besonders schwerwiegender Vorfälle, wie etwa Einbrüche, besteht. Zudem handelte es sich bei den Erfassungsbereichen in und um die Ferienwohnanlage nicht um einen abstrakt gefährdeten Ort, an dem nach der allgemeinen Lebenserfahrung eine erhöhte Wahrscheinlichkeit für den Eintritt der erwarteten Störung besteht und eine Verarbeitung personenbezogener Daten durch Videoüberwachung gerechtfertigt wäre, wie es etwa bei Banken und Juweliergeschäften der Fall ist.

Selbst wenn in den beschriebenen Sachverhalten eine Erforderlichkeit der Videoüberwachung zu bejahen gewesen wäre, hätte die Interessenabwägung diese nicht zugelassen. In beiden Fällen musste dem Recht der Betroffenen auf Schutz der personenbezogenen Daten aus Artikel 8 der Charta der Grundrechte der Europäischen Union, auf Unverletzlichkeit der Wohnung gemäß Artikel 13 Grundgesetz (GG) sowie auf Schutz des allgemeinen Persönlichkeitsrechts aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG der Vorrang eingeräumt werden. Die Berufsfreiheit der Verantwortlichen gemäß Artikel 12 GG, deren Eigentumsrecht gemäß Artikel 14 GG und deren allgemeine Handlungsfreiheit nach Artikel 2 Absatz 1 GG mussten demgegenüber zurücktreten.

Die Datenverarbeitung war damit sowohl während der Vermietung als auch außerhalb dieser (soweit sie sich auf Nachbargrundstücke erstreckte) als rechtswidrig zu werten. Es gab mildere und geeignetere Mittel zur Förderung des legitimen Zwecks und die Rechte der Betroffenen überwogen.

Auf unsere Ausführungen hin sicherte der Verantwortliche in einem der beiden Fälle zu, eine der Videokameras dauerhaft zu entfernen und die übrigen nur außerhalb der Vermietung begrenzt auf das Grundstück der Ferienwohnanlage wieder in Betrieb zu nehmen. Aufgrund dieser Bereitschaft des Verantwortlichen, einen datenschutzkonformen Zustand herzustellen, beließen wir es bei einer Verwarnung nach Artikel 58 Absatz 2 Buchstabe b DS-GVO, womit das Verfahren sodann abgeschlossen wurde.

Im zweiten Fall untersagte die Landesbeauftragte gemäß Artikel 58 Absatz 2 Buchstabe f DS-GVO den Betrieb aller Videokameras zu Zeiten, in denen eine der Ferienwohnungen an Gäste vermietet ist. Derzeit wird geprüft, ob auch in diesem Fall eine Verwarnung ausgesprochen wird.

3 Umfangreiche Videoüberwachung in einem Produktionsbetrieb

Wir erhielten im Rahmen einer Beschwerde Hinweise darauf, dass ein produzierendes Unternehmen im Land Brandenburg eine umfangreiche Videoüberwachung vor allem der Beschäftigten in einem Betriebsgebäude und auf dem Außengelände betreibe. Das Unternehmen hörten wir im Rahmen der Sachverhaltsaufklärung an. Es teilte mit, dass insgesamt eine mittlere zweistellige Zahl an Kameras an mehreren Standorten betrieben werde. Die Videoüberwachung erfolge 24 Stunden am Tag durchgängig. Zweck sei u. a. die Prävention von Eigentumsdelikten sowie die Gewährleistung des Arbeitsschutzes. Die Videoüberwachung solle auch zur Aufklärung begangener Straftaten beitragen. Es wurden einige wenige Vorfälle aus den Vorjahren benannt, bei denen es zu Straftaten und Fehlverhalten des Personals gekommen sei.

Im Rahmen der datenschutzrechtlichen Überprüfung stellte sich die Videoüberwachung während der Geschäftszeiten als unzulässig dar. Einwilligungserklärungen der Mitarbeiterinnen und Mitarbeiter, auf die die Datenverarbeitung mittels Videoüberwachung ausnahmsweise hätte gestützt werden können, sind im Arbeitsverhältnis grundsätzlich kritisch zu sehen und wurden im Übrigen auch nicht vorgelegt. Anhaltspunkte dafür, dass Straftaten von Beschäftigten die durchgängige Videoüberwachung hätten rechtfertigen können, legte der Verantwortliche ebenfalls nicht dar. Auch die Voraussetzungen von Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) lagen nicht vor. Danach kann die Verarbeitung personenbezogener Daten durch eine Videoüberwachung zulässig sein, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Die Verhinderung von Diebstählen und Sachbeschädigungen hätte durch alternative, weniger eingriffsintensive Maßnahmen gleichfalls erreicht werden können. Dazu zählen u. a. eine Verbesserung der Sicherung von Büromaterialien oder die Protokollierung und Sicherung des Zugangs zu einzelnen Räumen. Auch wäre unseres Erachtens eine Videoüberwachung außerhalb der Geschäftszeiten zur Prävention von Eigentumsdelikten ausreichend gewesen, zumal konkrete Fälle für ein-

schlägige Straftaten an den einzelnen Kamerastandorten während der Geschäftszeiten nicht dargelegt wurden.

Selbst wenn die Erforderlichkeit der Datenverarbeitung mittels Videoüberwachung vorgelegen hätte, wäre die geplante Maßnahme an der datenschutzrechtlich gebotenen Interessenabwägung gescheitert. Beispielsweise wurden einzelne Arbeitsplätze, der Pausenraum und der Zugang zu Toiletten dauerhaft erfasst. Das hätte nahezu eine Vollkontrolle des Verhaltens der Beschäftigten ermöglicht. Die nur unzureichende Verpixelung hatte daran nichts geändert, da die Aufenthaltsorte und Bewegungen des Personals nachvollziehbar blieben. Als Maßnahme der nur abstrakten Gefahrenabwehr – eine konkrete Gefährdungslage während der Geschäftszeiten wurde nicht dargetan – waren die Interessen des Unternehmens schwächer als jene der Beschäftigten zu gewichten.

Auch eine Videoüberwachung der Produktionsanlagen zur Überwachung der Arbeitsabläufe und zur Einhaltung von Arbeitsschutzvorschriften war nicht datenschutzkonform, da mildere alternative Mittel zur Verfügung standen. Dazu gehören beispielsweise eine Kontrolle durch Personal vor Ort oder die Installation von Lichtschranken, um die Zufahrt oder den Zugang zu bestimmten Bereichen kontrollieren zu können. Zudem besteht die Möglichkeit, einen durch Sensoren gesteuerten Alarm auszulösen, wenn beispielsweise Türen zu Kühlräumen nicht vollständig geschlossen wurden. Im Rahmen der Interessenabwägung überwiegen auch insoweit die Interessen der betroffenen Mitarbeiterinnen und Mitarbeiter, die aufgrund der nahezu flächendeckenden Videoüberwachung einem ständigen Überwachungsdruck ausgesetzt waren.

Arbeiten unter Beobachtung

Nach Abschluss der datenschutzrechtlichen Bewertung wurde dem Unternehmen u. a. die Verarbeitung personenbezogener Daten mittels aller Videokameras während der Geschäftszeiten an sämtlichen Standorten gemäß Artikel 58 Absatz 2 Buchstabe f DS-GVO untersagt. Es hat gegen den Bescheid Klage erhoben, die vor dem Verwaltungsgericht anhängig ist.

4 Offenlegung hunderter E-Mail-Adressen bei der Versendung von Werbung

Eine beschwerdeführende Person brachte vor, dass ihre E-Mail-Adresse durch die Versendung von Werbung einer Vielzahl von Adressatinnen und Adressaten gegenüber offengelegt wurde. Die Versendung der E-Mail erfolgte durch ein Unternehmen, das auf das neue Konzept einer Langzeitvermietung seiner Pensionen aufmerksam machen wollte und um das Verbreiten dieser Information sowie einen Besuch der neuen Webseiten bat. Bei der Versendung der E-Mail verwendete es einen offenen Verteiler, der ca. 300 E-Mail-Adressen umfasste. Weiter teilte die Person mit, dass sie im Jahr 2011 bei dem Unternehmen ein Boot für einen Tagesausflug gemietet und zu diesem Zweck ihre E-Mail-Adresse angegeben hatte. Über deren Verarbeitung zu Zwecken der Werbung ist sie nicht informiert worden. Zudem erfolgte seitdem keine Kontaktaufnahme mehr durch das Unternehmen.

Im Rahmen der Anhörung führte der Verantwortliche aus, dass es sich bei der fraglichen E-Mail um eine „reine Informations-E-Mail“ gehandelt habe und das Unternehmen grundsätzlich keine Werbe-E-Mails versenden würde. Für die Verarbeitung der E-Mail-Adresse zum Zweck der Zusendung dieser E-Mail liege jedoch keine Einwilligung der beschwerdeführenden Person vor. Das Unternehmen räumte weiter ein, dass bei der Versendung versehentlich ein offener Verteiler verwendet wurde.

Da die E-Mail-Adressen Rückschlüsse auf Vor- und Nachnamen konkreter natürlicher Personen zuließen, stellten diese personenbezogene Daten im Sinne der Datenschutz-Grundverordnung (DS-GVO) dar. Für deren Verarbeitung bedarf es stets einer Rechtsgrundlage.

Entgegen der Ansicht des Unternehmens handelte es sich bei der versendeten E-Mail um Werbung. Dieser Begriff ist weit auszulegen. Werbung sind u. a. die von Unternehmen zum Aufbau und zur Förderung des Geschäftsbetriebs verbreiteten Informationen. Auch Zufriedenheitsbefragungen von Kundinnen und Kunden nach einem Geschäftsabschluss können Werbung darstellen. In dem zugrundeliegenden Fall machte das Unternehmen in der E-Mail darauf aufmerksam, dass seine Pensionen zukünftig langfristig vermietet

werden. Es wurde u. a. deren außergewöhnliche Ausstattung hervorgehoben sowie darum gebeten, das neue, im Internet vorgestellte Konzept zu kommentieren und diese Neuigkeiten weiterzuverbreiten. Da die Versendung der E-Mail der Förderung des Geschäftsbetriebs diene, handelte es sich dabei um Werbung.

Für die Verarbeitung personenbezogener Daten im Zuge der Versendung von Werbung bedarf es als Rechtsgrundlage grundsätzlich der Einwilligung der betroffenen Person gemäß Artikel 6 Absatz 1 Buchstabe a DS-GVO. Eine solche lag den Ausführungen des Unternehmens zufolge nicht vor. Rechtsgrundlage kann unter Umständen auch Artikel 6 Absatz 1 Buchstabe f DS-GVO sein, wenn die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder Dritter erforderlich ist. Dies macht jedoch eine Abwägung mit den schützenswerten Interessen der betroffenen Person erforderlich. Maßgeblich für die anzustellende Interessenabwägung sind die vernünftigen Erwartungen der betroffenen Person.

Die beschwerdeführende Person gab dem Unternehmen ihre E-Mail-Adresse im Jahr 2011 bei einem Vertragsabschluss. Seitdem war keine Kontaktaufnahme mehr durch das Unternehmen erfolgt. Rund 11 Jahre später musste sie nicht mehr mit der Verarbeitung ihrer E-Mail-Adresse zu Werbezwecken rechnen. Damit überwiegen die schützenswerten Interessen der betroffenen Person. In der Versendung der Werbe-E-Mail ohne Rechtsgrundlage war somit ein datenschutzrechtlicher Verstoß zu sehen.

Auch die Verwendung eines offenen E-Mail-Verteilers stellt eine Verarbeitung personenbezogener Daten dar, für die es einer Rechtsgrundlage bedarf. Hierdurch wurden im konkreten Fall ca. 300 E-Mail-Adressen, die Vor- und Nachnamen natürlicher Personen erkennen ließen, für alle Empfängerinnen und Empfänger offengelegt. Für diese Form der Datenverarbeitung gab es ebenfalls keine Rechtsgrundlage; sie war unzulässig.

Aufgrund der o. g. Verstöße sprachen wir eine Verwarnung im Sinne des Artikels 58 Absatz 2 Buchstabe b DS-GVO aus. Da der Inhaber des Unternehmens das Versehen jedoch einräumte und keine Anhaltspunkte dafür bestanden, dass zuvor Werbe-E-Mails verschickt wurden oder zukünftig verschickt werden sollen, sahen wir von weiteren Maßnahmen ab.

5 Unzulässige Datenverarbeitung einer Fahrerlaubnisbehörde nach Beantragung einer Parkerleichterung durch Schwerbehinderte und bei Umtausch des Führerscheins

Durch mehrere Presseberichte sowie Beschwerden betroffener Personen wurden wir darauf aufmerksam, dass die Fahrerlaubnisbehörde der Landeshauptstadt Potsdam die Anträge auf Parkerleichterung für Personen mit einer Schwerbehinderung zum Anlass nahm, die Fahreignung der Personen zu überprüfen, und zu diesem Zweck umfassende Gesundheitsgutachten anforderte. Ähnliches passierte bei Anträgen auf Umtausch des Führerscheins in einen EU-Kartenführerschein. Unsere Vor-Ort-Kontrolle ergab, dass die Fahrerlaubnisbehörde bereits in über 100 Verfahren so gehandelt hatte.

Zur Überprüfung dieser Vorgehensweise wählten wir stichprobenartig 25 Verfahren aus. Mit dem Antrag auf Parkerleichterung erhielt die Fahrerlaubnisbehörde in der Regel den Schwerbehindertenausweis der antragstellenden Person mit dem Merkzeichen im Sinne der Schwerbehindertenausweisverordnung sowie dem Grad der Behinderung. Nach jeder beantragten Parkerleichterung forderte die Fahrerlaubnisbehörde darüber hinaus Befundberichte behandelnder Ärztinnen und Ärzte oder den Feststellungsbescheid des Landesamtes für Soziales und Versorgung an. Diese Dokumente ließen Rückschlüsse auf bei den Personen vorliegende Erkrankungen oder Einschränkungen zu.

Zunächst ergab unsere Kontrolle, dass bereits die Prüfung der Anträge auf Parkerleichterung durch die Fahrerlaubnisbehörde einen datenschutzrechtlichen Verstoß darstellte. Die einschlägigen Vorschriften sehen vor, dass die untere Straßenverkehrsbehörde für die Prüfung der Anträge auf Parkerleichterung sachlich zuständig ist. Eine Prüfung durch die Fahrerlaubnisbehörde ist gesetzlich nicht vorgesehen, erfolgte in der Landeshauptstadt seit dem Jahr 2012 aber dennoch aufgrund eines internen Organisationsbeschlusses.

Da die Fahrerlaubnisbehörde sachlich für die Prüfung der Anträge auf Parkerleichterung nicht zuständig ist, fehlte es an einer Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten, insbesondere der Gesundheitsdaten. Die Verarbeitung dieser Daten

ohne Rechtsgrundlage stellt einen datenschutzrechtlichen Verstoß gegen Artikel 6 Absatz 1 und Artikel 9 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) dar.

Darüber hinaus stellten wir fest, dass die Fahrerlaubnisbehörde zu einer Überprüfung der Fahreignung allein aufgrund eines Antrags auf Parkerleichterung nicht berechtigt war.

§ 46 i. V. m. § 11 Fahrerlaubnis-Verordnung sieht zwar vor, dass die Fahrerlaubnisbehörde die Fahreignung von Fahrerlaubnisinhaberinnen und -inhabern überprüfen darf. Allerdings müssen dafür konkrete Tatsachen vorliegen, die Zweifel an ihrer körperlichen oder geistigen Eignung begründen und in dem individuellen Fall eine Verkehrsgefährdung beim Führen eines Kraftfahrzeugs erwarten lassen. Vor der Anordnung eines ärztlichen Gutachtens sind die gegenseitigen Interessen durch die Fahrerlaubnisbehörde im Einzelfall abzuwägen.

Allein das Bestehen einer Schwerbehinderung, das lediglich durch ein Merkzeichen und den Grad der Behinderung ausgewiesen wird, stellt jedoch keine konkrete Tatsache dar, die Zweifel an der Fahreignung einer betroffenen Person hervorrufen kann. Anhaltspunkte, die auf eine Verkehrsgefährdung beim Führen eines Kraftfahrzeugs hindeuten, lassen sich der Beantragung einer Parkerleichterung nicht entnehmen. Dennoch wurde hier den antragstellenden Personen eine mangelnde Fahreignung aufgrund der gesundheitlichen Einschränkungen pauschal unterstellt und es wurden in diesem Rahmen umfassende gesundheitliche Gutachten angefordert. Nach Angaben der Stadtverwaltung erfolgte eine Überprüfung der Fahreignung seit August 2022 „automatisch“ nach jedem Antrag auf Parkerleichterung.

**Behörde
überschreitet
Kompetenz**

Da die Vorschriften der Fahrerlaubnis-Verordnung bei der Prüfung der Fahreignung nicht berücksichtigt wurden, hatte die Fahrerlaubnisbehörde keine Rechtsgrundlage für die Verarbeitung der Gesundheitsdaten. Die Datenverarbeitung verstieß damit gegen Artikel 9 Absatz 1 DS-GVO.

Zudem kontrollierten wir einige Verfahren, die einen Antrag auf Umtausch des Führerscheins in einen EU-Kartenführerschein zum



Gegenstand hatten. Auch hier fiel auf, dass die Fahrerlaubnisbehörde die Tatsachen, die ihr im Rahmen der Beantragung eines Führerscheinumtauschs übermittelt wurden, nutzte, um die Fahreignung einzelner Personen zu überprüfen und zu diesem Zweck Befundberichte behandelnder Ärztinnen und Ärzte anzufordern. Dies stellte ebenfalls einen Verstoß gegen Artikel 9 Absatz 1 DS-GVO dar.

In Umsetzung einer EU-Richtlinie ist jede Person, deren Führerschein vor dem Jahr 2013 ausgestellt wurde, gesetzlich verpflichtet, bis zum Jahr 2033 ihren alten Führerschein in einen EU-Führerschein umzutauschen. Ein entsprechender Antrag ist bei der Fahrerlaubnisbehörde zu stellen. Die Fahrerlaubnisbehörde hat dabei die Auflagen und Beschränkungen des alten Führerscheins in aktuell geltende Schlüsselzeichen zu übertragen. Dem gesetzgeberischen Willen nach handelt es sich bei dem Führerscheinumtausch um einen rein formalen Vorgang, der für sich genommen nicht zum Anlass genommen werden darf, Gesundheitsdaten anzufordern, um die Fahreignung zu überprüfen.

Die Landeshauptstadt Potsdam stoppte die Bearbeitung der Anträge auf Parkerleichterung durch die Fahrerlaubnisbehörde. Sie stimmte unserer rechtlichen Bewertung zu und versicherte, die gegenständlichen Verfahren aus datenschutzrechtlicher und fahrerlaubnisrechtlicher Sicht neu zu bewerten. Dafür werde eine eigene Arbeitsgruppe eingerichtet. Die Behörde stellte in Aussicht, die ohne Rechtsgrundlage erhobenen Gesundheitsdaten zu löschen. Bei den betroffenen Personen wollte sich die Verwaltung entschuldigen.

Da die datenschutzrechtlichen Verstöße vor dem Hintergrund des besonderen Schutzbedarfs der Gesundheitsdaten schwerwiegend waren und das Vorgehen in mehreren Verfahren zu einem freiwilligen Verzicht auf die Fahrerlaubnis oder zu ihrer Entziehung geführt hatte, verwarten wir die Stadtverwaltung gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO.

6 Bericht der Bußgeldstelle

6.1 Aushang der Krankentage von Beschäftigten eines Lebensmittelgeschäfts

Infolge einer Beschwerde erlangten wir davon Kenntnis, dass der Geschäftsführer eines inhabergeführten Lebensmittelgeschäfts im Pausenraum eine Tabelle mit den krankheitsbedingten Abwesenheitstagen von insgesamt 50 namentlich aufgelisteten Beschäftigten für das Jahr 2022 aufgehängt hatte. Die Tabelle enthielt Angaben darüber, an welchen Tagen sie aufgrund eigener Krankheit oder aufgrund einer Erkrankung des Kindes nicht zur Arbeit erschienen waren. Bei einigen Mitarbeiterinnen und Mitarbeitern war zudem vermerkt, dass sie sich im sogenannten Hamburger Modell befanden. Von den Angaben der Abwesenheitsgründe waren 40 Beschäftigte betroffen. Die Tabelle hing vier Wochen im Pausenraum aus. Neben den Beschäftigten hatten auch Dritte, z. B. Lieferantinnen und Lieferanten, Zugang zu den Daten.

**Krankentage
für alle?**

Die Inhaberin des Lebensmittelgeschäfts teilte im Rahmen unserer Anhörung im Bußgeldverfahren mit, dass sich das Unternehmen im Jahr 2022 in einer schlechten wirtschaftlichen Lage befand. Der Aushang der Tabelle mit den Abwesenheitstagen sollte verdeutlichen, dass ein hoher Krankenstand für das Unternehmen „kaum noch zu tragen“ sei. Eine Schwärzung der Namen der Beschäftigten sei zwar vor dem Aufhängen der Tabelle geplant gewesen. Dies habe der Geschäftsführer wohl vergessen.

Die Übermittlung der krankheitsbedingten Fehlzeiten der Beschäftigten verstieß gegen Artikel 6 Absatz 1 i. V. m. Artikel 9 Absatz 1 Datenschutz-Grundverordnung (DS-GVO). Bei den Abwesenheitsgründen handelte es sich um Gesundheitsdaten im Sinne des Artikels 9 Absatz 1 DS-GVO i. V. m. Artikel 4 Nummer 15 DS-GVO. Demnach sind Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Diese können nach Artikel 9 Absatz 2 Buchstabe h DS-GVO verarbeitet werden, wenn sie für Zwecke der

Gesundheitsvorsorge oder Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit der oder des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich sind. Das war hier nicht der Fall. Vielmehr sollte die Offenlegung der Gesundheitsdaten gegenüber den Mitarbeiterinnen und Mitarbeitern die schlechte wirtschaftliche Lage des Unternehmens aufzeigen und verdeutlichen, dass ein hoher Krankenstand dem Unternehmen schade.

Auch die – angeblich geplante – Unkenntlichmachung der Namen der Beschäftigten hätte einen Datenschutzverstoß bedeutet. Ein Aushang mit geschwärzten Namen hätte lediglich eine Übermittlung pseudonymer Daten im Sinne des Artikels 4 Nummer 5 DS-GVO dargestellt; sie wären weiterhin personenbeziehbar gewesen. Unter Zugrundelegung der allgemeinen Lebenserfahrung ist davon auszugehen, dass die Belegschaft aufgrund einer bestimmten Reihenfolge und Dauer von Krankheitstagen Rückschlüsse auf die jeweiligen betroffenen Kolleginnen und Kollegen hätte ziehen können. Denn die Beschäftigten des Lebensmittelgeschäfts verfügten aufgrund der überschaubaren Mitarbeiterzahl über zusätzliche Informationen, die ihnen eine Identifizierung der betroffenen Personen ermöglicht hätte.

Wegen dieses Datenschutzverstoßes setzten wir ein Bußgeld in fünfstelliger Höhe fest. Das Unternehmen akzeptierte dies.

6.2 Unbefugte Datenabfragen in Krankenhäusern

Eine Mitarbeiterin eines Krankenhauses beschwerte sich bei uns, dass Kolleginnen und Kollegen über einen längeren Zeitraum mehrfach auf ihre in einem elektronischen Krankenhausinformationssystem gespeicherte Patientenakte zugegriffen hatten, ohne mit ihrer Behandlung betraut gewesen zu sein. Sie riefen die Akte nur aus Neugier auf, um sich über den Krankheitsverlauf während ihres stationären Aufenthalts zu informieren. Während unserer Ermittlungen stellte sich heraus, dass insgesamt fünf Beschäftigte ohne einen dienstlichen Grund auf die Patientenakte der betroffenen Mitarbeiterin zugegriffen hatten.

Aus einem anderen Krankenhaus erreichte uns eine ähnliche Beschwerde. Auch hier rief eine Kollegin aus Neugier hinsichtlich des

Verlaufs einer Operation der betroffenen Mitarbeiterin – und damit ohne einen dienstlichen Grund – deren in einem elektronischen Krankenhausinformationssystem gespeicherte Patientenakte ab.

Durch die Abrufe der Patientenakten erlangten die Kolleginnen und Kollegen in beiden Fällen Einblicke in die besonders durch Artikel 9 Datenschutz-Grundverordnung (DS-GVO) geschützten Gesundheitsdaten der betroffenen Mitarbeiterinnen, wie Arztbriefe, Laborergebnisse sowie Berichte über Behandlungen und Operationen. Diese Abrufe waren hier nicht nach Artikel 9 Absatz 2 Buchstabe h und Absatz 3 DS-GVO i. V. m. § 28 Absatz 1 Brandenburgisches Krankenhausentwicklungsgesetz (BbgKHEG) gerechtfertigt. Nach § 28 Absatz 1 Nummer 1 BbgKHEG dürfen Patientendaten mit Ausnahme der Offenlegung verarbeitet werden, soweit dies zur Behandlung der Patientin oder des Patienten einschließlich der notwendigen Dokumentation erforderlich ist. Da die Kolleginnen und Kollegen beim Abruf der Patientenakte der jeweiligen Mitarbeiterin weder mit ihrer Behandlung noch mit deren Abrechnung betraut waren und nur aus einem privaten Interesse heraus gehandelt hatten, verstießen sie gegen Datenschutzrecht.

Im Rahmen unserer Ermittlungen gaben die beiden Krankenhäuser an, dass sie die Mitarbeiterinnen und Mitarbeiter im Datenschutzrecht geschult hatten und entsprechende Dienstanweisungen zum Datenschutz hinsichtlich der Zugriffe auf Hard- und Software zur elektronischen Datenverarbeitung vorlagen. Eines der Krankenhäuser teilte uns mit, dass die Patientenakten bei Beschäftigten auf eigenen Wunsch unter einem fiktiven Namen geführt werden können, um künftige Missbrauchsfälle zu vermeiden.

Generell ist festzuhalten, dass im Berichtszeitraum auffällig viele Fälle von sogenannten Mitarbeiterexzessen in Krankenhäusern gemeldet und von uns bearbeitet wurden. Beschäftigte handeln dann im sogenannten Mitarbeiterexzess, wenn sie dienstliche Auskunftssysteme aus privaten Gründen und ohne dienstlichen Anlass nutzen, um damit beispielsweise Informationen über eine Person zu erlangen. Sie werden dadurch selbst zu Verantwortlichen nach Artikel 4 Nummer 7 DS-GVO. Verstöße wie diese sind in hohem Maß geeignet, das Vertrauen in die Rechtmäßigkeit des Umgangs mit Gesundheitsdaten in Krankenhäusern zu beeinträchtigen.

Wir möchten darauf hinweisen, dass Krankenhäuser verpflichtet sind, solche Exzesse gemäß Artikel 33 DS-GVO der Landesbeauftragten zu melden. Ansonsten droht den Unternehmen ein Bußgeldverfahren nach Artikel 83 Absatz 4 Buchstabe a DS-GVO.

Weil die Rechtsverstöße in den beiden konkreten Fällen nicht den Krankenhäusern als datenschutzrechtlich Verantwortlichen, sondern den einzelnen Beschäftigten zuzurechnen waren, setzten wir gegen diese Bußgelder in jeweils dreistelliger Höhe fest. Die jeweiligen Bußgelder wurden akzeptiert.

6.3 Polizist nutzt Telefonnummer einer Anzeigerstatterin zur privaten Kontaktaufnahme

Bei der Aufnahme einer Anzeige teilte der zuständige Polizist der Anzeigerstatterin seine private Mobilfunknummer mit. Hierüber sollte die Geschädigte ihm weiteres Beweismaterial zukommen lassen, welches er dann an die entsprechenden Stellen weiterleiten würde.

Zu diesem Zweck schrieb sie ihm sodann über einen Messenger-Dienst. Der Polizeibedienstete machte jedoch sehr schnell deutlich, lieber privat kommunizieren zu wollen. Hierfür meldete er sich mit seinem Vornamen, sprach die Anzeigerstatterin mit „du“ an und drängte, dass sie ihn ebenfalls duzen solle. Darüber hinaus forderte er sie auf, sie solle sich an seinem freien Tag bei ihm melden, was er mit vier Rosen-Emojis dekorierte.

Der Polizeibedienstete verwendete die ihm zu dienstlichen Zwecken bekannt gewordene Telefonnummer der Anzeigerstatterin für eine private Kontaktaufnahme, obwohl ein Zugriff auf polizeiliche Datenbestände nur gestattet ist, wenn dies zur Erfüllung der polizeilichen Aufgaben erforderlich ist.

Rosen-Emojis für Anzeigerstatterin

Gemäß § 32 Absatz 1 Nummer 1 Brandenburgisches Datenschutzgesetz handelt ordnungswidrig, wer entgegen einer Datenschutzvorschrift personenbezogene Daten, die nicht offenkundig sind, verwendet. Nach § 39 Absatz 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 da-

nach grundsätzlich ein dienstlicher Anlass vorliegen. Die Nutzung zu privaten Zwecken gehört nicht zur Aufgabenerfüllung der Polizei.

Wir setzten gegen den Polizeibediensteten eine Geldbuße im oberen dreistelligen Bereich fest. Das Bußgeld wurde akzeptiert.

6.4 Mitgliederdaten eines Anglervereins im Internet abrufbar

Im Rahmen seines Internetangebots ermöglichte ein Anglerverein interessierten Nutzerinnen und Nutzern nicht nur Einblicke in die Vereinstätigkeiten, sondern darüber hinaus auch in zahlreiche persönliche Daten der Vereinsmitglieder. Über die Homepage des Vereins waren Listen u. a. mit Vor- und Nachnamen der Mitglieder, vollständigen Anschriften mit Telefonnummern, Geburtsdaten sowie Kontoverbindungsdaten abrufbar. Jedermann konnte die Daten mithilfe der Suchfunktion der Webpräsenz oder über eine allgemeine Internetsuche auffinden.

Bei den im Internet frei abrufbaren Daten handelte es sich um Informationen, die sich jeweils auf eine identifizierte oder identifizierbare natürliche Person bezogen und damit um personenbezogene Daten im Sinne des Artikels 4 Nummer 1 Datenschutz-Grundverordnung (DS-GVO). Sie wurden durch das Bereitstellen im Internet und die freie Abrufbarkeit offengelegt, also gemäß Artikel 4 Nummer 2 DS-GVO verarbeitet. Dass ein Dritter tatsächlich Kenntnis von den Daten erlangte, war für die Erfüllung des bußgeldrelevanten Tatbestandes im Übrigen nicht erforderlich – die Möglichkeit der Kenntnisnahme genügt.

Ein ehemaliges Vorstandsmitglied des Anglervereins hatte die Dokumente im jeweiligen Beitragsjahr auf der Webseite zum Abruf hinterlegt. Da keine Erlaubnisnorm die Offenlegung der persönlichen Angaben der Mitglieder über das Internet legitimierte, stellte dies einen Verstoß gegen Artikel 6 DS-GVO dar. Bei Anwendung der im Verkehr erforderlichen Sorgfalt hätte das Vorstandsmitglied prüfen und erkennen müssen, dass die Dokumente nicht frei zugänglich über das Internet bereitgestellt werden durften. Alle Dateien auf einem Webserver müssen so geschützt werden, dass sie nicht unbefugt gelesen oder geändert werden können. Auch muss der Webserver die Ereignisse, wie z. B. erfolgreiche Zugriffe und fehlgeschlagene Zugriffe auf Ressourcen aufgrund von mangelnder Berechtigung, protokollieren. Anhand solcher Protokolle hätte erkannt werden können, dass auf



besagte Listen im vorliegenden Fall erfolgreich zugegriffen wurde, weil es keine Zugriffsbeschränkung gab.

Wir setzten wegen dieses Verstoßes gegen den Anglerverein gemäß Artikel 83 Absatz 5 Buchstabe a DS-GVO eine Geldbuße im mittleren dreistelligen Bereich fest. Hierbei berücksichtigten wir insbesondere den Umfang der offengelegten Daten und die Zahl der betroffenen Personen sowie die Tatsache, dass für einen Missbrauch geeignete Kontoverbindungsdaten offengelegt wurden. Eine unbefugte Verarbeitung personenbezogener Daten kann zu einem physischen, materiellen oder immateriellen Schaden führen. So birgt die Veröffentlichung im Internet insbesondere die Gefahr eines Verlustes der Kontrolle über die personenbezogenen Daten, einer Diskriminierung, eines Identitätsdiebstahls oder -betrugs sowie finanzieller Verluste. Auf der anderen Seite war zu berücksichtigen, dass der Anglerverein umfänglich an der Aufklärung des Sachverhalts mitgewirkt hatte. Auch hatte er die Webseiten nach Bekanntwerden der Offenlegung unverzüglich vom Netz genommen. Zudem war der geringe Jahresumsatz des Vereins bei der Höhe der Geldbuße zu berücksichtigen.

III Anlasslose Prüfungen

1 Einhaltung der Betroffenenrechte beim Versand von Newslettern

Im Rahmen unserer Aufsichts- und Kontrolltätigkeit stellen wir immer wieder Defizite im Umgang mit Kundendaten fest. Dies fiel uns auch auf, als wir im Berichtszeitraum ein Unternehmen im Hinblick auf den Versand von Werbung prüften.

Gewinnspiele, Rabatt-Aktionen, personalisierte Werbung und der regelmäßige Versand eines Newsletters werden von Unternehmen häufig genutzt, um Kundinnen und Kunden zu gewinnen oder zu binden. Betroffene Personen empfinden dies zum Teil als Belästigung und wollen der Nutzung ihrer Daten zu Werbezwecken widersprechen oder fordern das Unternehmen auf, detailliert Auskunft über die Verarbeitung der Daten zu erteilen bzw. sie zu löschen. Mängel in der Organisation des Umgangs mit Kundendaten stehen dem nicht selten entgegen. Dies vermuteten wir auch bei dem geprüften Unternehmen, nachdem wir zahlreiche Beschwerden von betroffenen Personen aus ganz Deutschland erhielten.

Unsere Vor-Ort-Prüfung begann mit einem Gespräch mit den verantwortlichen Personen über relevante Unternehmensprozesse sowie Abläufe der Verarbeitung von Kundendaten im Allgemeinen. Hierbei ging es uns vor allem darum, einen Überblick über die Gesamtstruktur des Unternehmens und relevante Geschäftsprozesse zu erhalten. Abgefragt wurden auch konkrete Maßnahmen zur Umsetzung der Anforderungen der Datenschutz-Grundverordnung (DS-GVO) und Dokumentationen, wie beispielsweise das Verzeichnis der Verarbeitungstätigkeiten, das Lösch- oder das Zugriffskonzept. Die Unterlagen waren zwar vorhanden, wiesen jedoch Defizite auf. So enthielt das Verarbeitungsverzeichnis nicht alle gesetzlich geforderten Angaben, war zu allgemein gehalten und umfasste nicht alle Datenverarbeitungsprozesse des Unternehmens.

Stichprobenartig nahmen wir Einsicht in die IT-Systeme und die Unterlagen zur Umsetzung technischer und organisatorischer Maß-



nahmen im Sinne des Artikels 32 DS-GVO. Wir stellten fest, dass zwar ein Großteil der Maßnahmen von dem Unternehmen bereits umgesetzt wird, die zugehörige Dokumentation jedoch unvollständig bzw. teilweise nicht vorhanden war. Dies verletzt sowohl die Nachweis- und Rechenschaftspflicht, kann darüber hinaus aber auch zu vielfältigen Problemen führen. Die Unterlagen werden im Unternehmen z. B. für die Aufrechterhaltung und Weiterentwicklung des Niveaus des Datenschutzes und der Informationssicherheit, zur Planung entsprechender Ressourcen und Einweisung von Beschäftigten hinsichtlich technischer und organisatorischer Abläufe benötigt.

Im Rahmen unserer Kontrolle der Organisation des Newsletter-Versands an Kundinnen und Kunden des Unternehmens ließen wir uns den konkreten Anmeldeprozess in unterschiedlichen Fallgestaltungen erläutern. Den Schwerpunkt legten wir auf die Bedingungen der Anmeldung bzw. die Ausgestaltung der Möglichkeiten für die Abmeldung. Außerdem ließen wir uns stichprobenartig die Dokumentation der Einwilligung der betroffenen Personen zum Erhalt des Newsletters vorweisen.

Wie für alle Verarbeitungen personenbezogener Daten gilt, dass E-Mail-Adressen verarbeitet werden dürfen, wenn eine Rechtsgrundlage vorliegt. Das geprüfte Unternehmen stützt die Verarbeitung zu Werbezwecken auf eine Einwilligung der betroffenen Personen. Dies setzt voraus, dass dieser Zweck der E-Mail-Werbung entsprechend Artikel 13 Absatz 1 Buchstabe c DS-GVO

Der Werbung ausgeliefert?

den betroffenen Personen bei der Datenerhebung transparent dargelegt worden ist. Darüber hinaus müssen die Einwilligungen gemäß Artikel 7 Absatz 1 DS-GVO nachgewiesen werden können. Im konkreten Fall war vorgesehen, dass Dokumentation und

Nachweis der Einwilligung mit dem für die Verwaltung der Kundendaten genutzten System erfolgt. Hierzu ergab unsere Prüfung, dass die Einwilligung nicht in allen Fällen informiert erteilt wurde. Wir wiesen die Verantwortlichen darauf hin, dass insoweit dringender Nachbesserungsbedarf bestand.

Außerdem ließen wir uns die genauen Abläufe der Bearbeitung von Anfragen betroffener Kundinnen und Kunden z. B. auf Auskunft oder Löschung darstellen. Im Rahmen der Begehung einzelner Büroräume befragten wir Mitarbeiterinnen und Mitarbeiter zu ihrer Arbeit mit personenbezogenen Daten. In den Gesprächen fiel auf, dass kaum

Kenntnisse der datenschutzrechtlichen Regelungen oder Grundsätze vorhanden waren. So war vielen Beschäftigten unklar, wie sie mit Löschanträgen oder Bewerbewidersprüchen umzugehen hatten. Derartige Anfragen wurden oftmals nicht rechtzeitig weitergeleitet und fristgerecht innerhalb eines Monats beantwortet. Dies hatte zu zahlreichen Beschwerden bei unserer Behörde geführt und bestätigte unsere Erfahrung aus anderen Fällen, nach der viele Verstöße im Umgang mit personenbezogenen Daten darauf zurückzuführen sind, dass Beschäftigte nicht ausreichend geschult werden. Allen Verantwortlichen ist dringend angeraten, diejenigen Beschäftigten, die regelmäßig mit personenbezogenen Daten umgehen, für datenschutzrechtliche Fragen zu sensibilisieren und entsprechend fortzubilden.

Eine abschließende Bewertung ist uns noch nicht möglich, weil die Prüfung zum Ende des Berichtszeitraums weiter andauerte.

2 Prüfung von Webseiten auf Cookies, Tracking und eingebundene Drittdienste

Bereits im letzten Tätigkeitsbericht informierten wir über Änderungen bei den rechtlichen Regelungen zum Einsatz von sogenannten Cookies durch Anbieterinnen und Anbieter von Webseiten. Darüber hinaus erläuterten wir die Anforderungen, die aus Sicht der Datenschutzaufsichtsbehörden für die rechtskonforme Verwendung von Cookies zu beachten sind.¹⁶ Insbesondere verwiesen wir darauf, dass das Speichern und Auslesen von Cookies einer Einwilligung der jeweiligen Nutzerinnen und Nutzer bedarf, wenn dies für den Betrieb der Webseiten nicht zwingend erforderlich ist. Gleiches gilt in der Regel für die Weiterverarbeitung von aus Cookies gewonnenen Informationen, z. B. zur Verfolgung von Nutzeraktivitäten oder dem Ausspielen von Werbung. Alle damit verbundenen Verarbeitungsprozesse sind durch die Anbieterinnen bzw. Anbieter von Webseiten transparent zu beschreiben. Analoge Vorgaben gelten für die Einbeziehung von Diensten Dritter, etwa wenn es um die Einbettung von Videos, Landkarten, speziellen Schriftarten, Programmskripten u. Ä. geht.

Wie schon im Vorjahr erhielten wir auch im Berichtsjahr eine Vielzahl von Beschwerden, mit denen Nutzerinnen und Nutzer uns über die aus ihrer Sicht unrechtmäßige Einbindung von Cookies und Diensten Dritter in Webseiten, die vermutete Weiterverarbeitung von Daten zu Werbezwecken oder die mangelnde Aufklärung darüber (z. B. in der Datenschutzerklärung) informierten. Wir gingen sowohl diesen Beschwerden in jedem Einzelfall nach, führten allerdings auch anlassunabhängig entsprechende Prüfungen durch.

Für diese anlassunabhängigen Prüfungen wählten wir ca. 50 Webpräsenzen aus, die in der Regel auf touristische Angebote, Sehenswürdigkeiten Brandenburgs, Freizeitaktivitäten u. Ä. aufmerksam machen sollten. Zu jeder Webpräsenz ermittelten wir, ob und, wenn ja, welche Cookies bzw. Drittdienste eingebunden waren, ob Nutze-

¹⁶ Tätigkeitsbericht Datenschutz 2022, A I 2.1.

rinnen und Nutzer über die Einbindung informiert wurden und ob sie die Möglichkeit hatten, eine rechtskonforme Einwilligung zu erteilen.

Positiv festzuhalten ist, dass bei knapp der Hälfte der geprüften Webseiten keine Mängel festgestellt wurden. Rund ein Drittel nutzte bei der Gestaltung der Seiten Schriftarten, die von einem Server des Unternehmens Google nachgeladen wurden. Hiermit ist stets eine Übermittlung der IP-Adresse der Nutzerin bzw. des Nutzers an den genannten Konzern verbunden. Diese Übermittlung wäre allerdings vermeidbar, wenn die verwendeten Schriftarten lokal auf dem Webserver der Anbieterin bzw. des Anbieters der Webpräsenz gespeichert würden.

Ungefähr ein Viertel der Webseiten sammelte Informationen über die Besucherinnen und Besucher mit dem Werkzeug Google Analytics. Zwar ist bei dessen Einbindung auch eine datenschutzkonforme Lösung umsetzbar, diese erfordert jedoch zusätzlichen Aufwand für die Webseitenanbieterin bzw. den -anbieter. Insbesondere sind entsprechende Verträge mit Google abzuschließen und eine Anonymisierungsfunktion für die IP-Adressen zu nutzen. Der Aufwand ließe sich vermeiden, wenn von Anfang an eine datenschutzgerechte und bestenfalls in eigener Regie betriebene Analyseplattform genutzt würde.

Im Hinblick auf die Einbindung anderer Drittdienste oder die Nutzung von Cookies bekannter Werbetracker stellten wir fest, dass nur ein geringer Teil der geprüften Webpräsenzen hiervon Gebrauch machte. Es handelte sich in jedem Fall lediglich um eine niedrige einstellige Anzahl. Dies erstaunte uns – auch vor dem Hintergrund, dass bei der Mehrzahl der Beschwerden, die uns zu dem Thema erreichen, oftmals gleich eine ganze Reihe von unterschiedlichen Cookies und Trackingdiensten in die gerügten Webseiten integriert wird.

Zu den Einwilligungsmöglichkeiten und der transparenten Aufklärung der Nutzerinnen und Nutzer über die Verwendung von Cookies und Trackingdiensten ergab unsere Prüfung, dass viele Webauftritte offensichtlich aus einfach bedienbaren, baukastenartig aufgebauten Werkzeugsammlungen zusammengestellt wurden. Das Funktionieren eines bestimmten Elements der Webpräsenz wird dann von der jeweiligen Anbieterin bzw. dem Anbieter als wichtiger eingeschätzt als die Beachtung datenschutzrechtlicher Anforderungen. So ist beispielsweise ein Baustein für ein Cookie-Banner, mit dessen Hilfe



eine Einwilligung der Nutzerin bzw. des Nutzers eingeholt werden soll, schnell eingefügt. Über die rechtskonforme Gestaltung des Banners sagt das jedoch noch nichts aus.

Immer wieder mussten wir bei unserer Prüfung auch feststellen, dass die Datenschutzerklärungen für die Webpräsenzen mittels frei im Internet verfügbarer Generatoren erstellt wurden. In manchen Fällen beschrieb die Webseitenanbieterin bzw. der -anbieter einfach alle

Transparenz großschreiben

möglichen Datenverarbeitungen – auch solche, die auf den Seiten gar nicht stattfanden. In der Regel traf jedoch der umgedrehte Fall zu: Der Nutzerin bzw. dem Nutzer wurde die Verwendung von Cookies oder die Einbindung von Drittdiensten verschwiegen bzw. selbige nicht hinreichend erläutert. Das

Verschweigen stellt einen Rechtsverstoß dar; bei einer mangelhaften Erläuterung wäre die Wirksamkeit einer möglicherweise erteilten Einwilligung zu bezweifeln, womit darauf basierende Datenverarbeitungen unrechtmäßig wären.

Wir haben in denjenigen Fällen, in denen wir Mängel bei den Webpräsenzen feststellten, die jeweilige Anbieterin bzw. den Anbieter über unsere Erkenntnisse und die wesentlichen rechtlichen Anforderungen informiert. Gleichzeitig forderten wir sie bzw. ihn auf, die Mängel zu beseitigen. In anschließenden Gesprächen stellten wir oftmals fehlende Fachkenntnisse oder Sensibilität für Datenschutzfragen fest. Manche Verantwortliche waren für die Hinweise dankbar und stellten ihre Webpräsenz entsprechend um. Bei anderen bedurfte es mehrerer Interventionen und hartnäckiger Überzeugungsarbeit durch uns. Im Rahmen von Nachprüfungen werden wir die Einhaltung der Rechtsvorschriften kontrollieren. Wer Webseiten anbietet, darf die datenschutzrechtlichen Anforderungen nicht hintanstellen.

3 Technisch-organisatorische Prüfung nach einem Angriff auf die IT-Infrastruktur der Landeshauptstadt Potsdam

Wie bereits im Januar 2020¹⁷ ereignete sich auch im Dezember 2022 ein Angriff auf die IT-Infrastruktur der Landeshauptstadt Potsdam. Gemäß der ersten Meldung der Stadt an uns waren Ausgangspunkt diesmal so genannte Brute-Force-Angriffe auf die Webseiten der Volkshochschule, die jedoch erfolglos blieben. Die Stadtverwaltung entschied noch am gleichen Tag, alle Netzverbindungen zu trennen – insbesondere diejenigen zum Internet. Hiervon ausgenommen waren lediglich Verbindungen über ein Virtual Private Network, die über eine Multifaktorauthentisierung verfügten. Der neuerliche Vorfall und die Trennung der Systeme vom Internet zogen einen wochenlangen Ausfall der Bürgerdienste und Einschränkungen in der Arbeitsfähigkeit der Verwaltung nach sich.

Eine Vervollständigung der Erstmeldung ging bei der Landesbeauftragten nicht ein, weshalb wir die Verantwortlichen der Landeshauptstadt schriftlich daran erinnerten. Weiterhin forderten wir im Januar 2023 die Übersendung des Verzeichnisses der Verarbeitungstätigkeiten gemäß Artikel 30 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) sowie die Dokumentation des Datenschutzvorfalls gemäß Artikel 33 Absatz 5 DS-GVO an. Darüber hinaus wollten wir über den Stand der polizeilichen Ermittlungen (soweit der Landeshauptstadt bekannt) informiert werden.

Daraufhin erhielten wir vom damaligen Datenschutzbeauftragten der Stadtverwaltung sowie vom Informationssicherheitsbeauftragten eine E-Mail, wonach Zugriffsversuche von bekannten „Command and Conquer“-Servern zu verzeichnen seien, welche aufgrund der deaktivierten Internetverbindung jedoch erfolglos blieben. Weiterhin wurde uns mitgeteilt, dass diese Kommunikationsversuche möglicherweise schon längere Zeit andauerten und erst jetzt durch die Verschärfung der Überwachungssensorik aufgefallen seien. Abschließend übersandte der Informationssicherheitsbeauftragte die

17 Tätigkeitsbericht Datenschutz 2020, A IV 8.



Rückmeldung, dass keine Kompromittierung der IT-Systeme und kein Abfluss personenbezogener Daten festgestellt werden konnten, womit auch keine Datenschutzverletzung im Sinne der Datenschutz-Grundverordnung vorläge.

Da wir bereits bei dem vorangegangenen Vorfall Lücken in der Dokumentation der IT-Infrastruktur der Landeshauptstadt und der Informationssicherheitsmaßnahmen sowie Mängel bei der Informationssicherheitsorganisation festgestellt hatten, entschieden wir uns, diese Punkte erneut zu prüfen. Insbesondere wollten wir wissen, ob die Dokumentation nunmehr auf einem aktuellen Stand ist und ein geeignetes Notfallkonzept z. B. für Angriffsszenarien vorliegt. Letzteres hätte eventuell ein Abschalten der gesamten IT-Infrastruktur verhindert oder die Dauer der eingeschränkten Verfügbarkeit reduziert. Um den aktuellen Sachstand zu ermitteln, forderten wir im Rahmen einer Prüfungsankündigung vorab nochmals das Verzeichnis der Verarbeitungstätigkeiten, den Netzplan, das Notfallkonzept, das Informationssicherheitskonzept sowie die bereits im Januar 2023 erbetene vollständige Dokumentation zum aktuellen Cyberangriff an.

Die Ergebnisse waren ernüchternd: Ein Verzeichnis der Verarbeitungstätigkeiten und ein gültiges Informationssicherheitskonzept haben wir nicht erhalten. Im Gespräch mit Vertreterinnen und Vertretern der Landeshauptstadt während unserer Prüfung vor Ort im April des Berichtszeitraums stellte sich heraus, dass sowohl der Informationssicherheitsbeauftragte als auch die Datenschutzbeauftragte erst seit kurzer Zeit in ihren jeweiligen Positionen bei der Stadt angestellt waren und ihnen auch keine vollständigen, aktuellen Unterlagen, wie von uns angefordert, vorlagen.

Hinsichtlich der Umsetzung unserer Empfehlungen aus dem Sicherheitsvorfall im Jahr 2020 war festzustellen, dass aktuelle Meldungen und Warnungen vor potenziellen IT-Sicherheitslücken – z. B. des Computer Emergency Response Teams der Landesverwaltung, von Herstellerinnen und Herstellern sowie sonstigen Medien – nun regelmäßig ausgewertet werden. Dieses Versäumnis führte 2020 dazu, dass eine IT-Sicherheitslücke zu spät geschlossen wurde. Weiter informierte man uns, dass ein Security Operations Center mit der Rund-um-die-Uhr-Überwachung der IT-Systeme beauftragt und das Notfallmanagement angegangen wurde. Auch wurden Incident Response-Pläne implementiert. Nicht umgesetzt hat die Landeshauptstadt dagegen z. B. unseren Vorschlag, ein Informati-

Informationssicherheitsmanagementteam zu etablieren, das vom Informationssicherheitsbeauftragten koordiniert wird und die Arbeiten zur Informationssicherheit in der Stadtverwaltung bündelt.

Als Ergebnis der Vor-Ort-Prüfung vereinbarten wir mit der Landeshauptstadt kurze Fristen, zu denen uns ein Zeitplan für die Erarbeitung des Verzeichnisses der Verarbeitungstätigkeiten sowie des Informationssicherheitskonzeptes vorzulegen waren. Weiter wurde vereinbart, dass die Stadt im Austausch mit der Landesbeauftragten bleibt und diese regelmäßig über die Fortschritte zur Finalisierung der Dokumente unterrichtet.

In der Folgezeit verletzte die Landeshauptstadt jedoch regelmäßig und zunächst unbegründet gesetzte Fristen. Rückmeldungen zu den durch sie selbst in den eigenen Zeitplänen festgelegten Terminen erfolgten nicht. Es bedurfte erneuter Anfragen unserer Behörde, worauf mitgeteilt wurde, dass die Fristversäumnisse durch eine fehlende finale Klärung der Verantwortlichkeiten innerhalb der Stadtverwaltung verursacht und vereinzelte Fragmente des Verzeichnisses der Verarbeitungstätigkeiten doch nicht wie erhofft nutzbar wären. Wir gaben daraufhin Hinweise zur Priorisierung der Arbeiten und erläuterten nochmals unsere Erwartungen an die Inhalte der fehlenden Dokumente.

Gemäß Artikel 30 Absatz 1 DS-GVO führt der datenschutzrechtlich Verantwortliche ein Verzeichnis der Verarbeitungstätigkeiten. Ist ein solches nicht vorhanden, stellt dies einen klaren Verstoß gegen die Datenschutz-Grundverordnung dar. Darüber hinaus implementiert der Verantwortliche gemäß Artikel 24 Absatz 1, Artikel 25 Absatz 1 und Artikel 32 DS-GVO geeignete und angemessene technische und organisatorische Maßnahmen, um die durch die Verarbeitung personenbezogener Daten entstehenden Risiken für die Rechte und Freiheiten der betroffenen Personen hinreichend zu mindern. Dies ist durch den Verantwortlichen auch nachzuweisen – in der Regel durch ein geeignetes Datenschutz- und Informationssicherheitskonzept. Ein solches legte die Landeshauptstadt bis zum heutigen Tag nicht vor. Auch hier ist insofern eine Verletzung der Rechtsvorschriften festzustellen. Aufgrund dieser Versäumnisse prüft die Landesbeauftragte derzeit, von einer Abhilfebefugnis gemäß Artikel 58 Absatz 2 DS-GVO Gebrauch zu

**Datenschutz
ernst nehmen**



machen. Wir werden gleichwohl im Austausch mit der Landeshauptstadt bleiben, bis die erforderlichen Nachweise vollständig vorliegen.

IV Ausgewählte Fälle

1 Datenleck bei einem Fahrzeughersteller – unsere Rolle im europäischen Aufsichtsverfahren

Im Frühjahr des Berichtsjahres kontaktierte uns ein ehemaliger Beschäftigter eines weltweit agierenden, auch in Brandenburg ansässigen Fahrzeugherstellers. Er informierte uns darüber, dass in dem Unternehmen über ein internes Informationssystem große Datenbestände für nicht zuständige Beschäftigte abrufbar seien. Konkret benannte er Daten über Mitarbeiterinnen und Mitarbeiter mit teils sensiblen Inhalten. Von dem Datenleck umfasst seien darüber hinaus Daten von Kundinnen und Kunden sowie Daten z. B. zu Fahrzeugmodellen und zur Produktion.

Kurze Zeit später stellte uns der ehemalige Beschäftigte über eine sichere, anonym nutzbare Download-Plattform und in verschlüsselter Form ca. 270 Megabyte Daten bereit, die offensichtlich aus dem internen Informationssystem des Unternehmens stammten. Im Wesentlichen handelte es sich dabei um Tabellen. Aus dem Kontext war zu schließen, dass diese Tabellen zu Aufträgen an die Softwareentwicklungsabteilung gehörten und auf Fehler im internen Personalverwaltungssystem des Unternehmens hinweisen sollten (z. B. Dubletten oder fehlerhafte Verweise). Bereits bei einer ersten Sichtung offenbarte sich die Brisanz der Daten: Eine Tabelle enthielt beispielsweise knapp 200.000 Datensätze zu ehemaligen Beschäftigten des Konzerns weltweit mit Angaben zum Einstellungs- und Kündigungsdatum, davon über 9.000 Beschäftigte in der EU und über 2.000 in Deutschland. Eine andere Datei umfasste ca. 80.000 Datensätze zu Kündigungen in den Jahren 2020 und 2021. Zu jeder bzw. jedem ehemaligen Beschäftigten waren die konkrete Position in der Hierarchie des Unternehmens und die Funktion bzw. das Jobprofil vermerkt; bei der überwiegenden Zahl auch die Kündigungsgründe wie z. B. schlechte Arbeitsleistung, Verletzung interner Anweisungen, unentschuldigte Abwesenheiten, Wechsel zu einem Konkurrenzunternehmen, Pflegefall in der Familie, Überlastung oder Langzeiterkrankung. In dieser Datei waren Daten zu ca. 3.000 Be-

schäftigten in der EU und ca. 1.000 aus Deutschland vermerkt. Eine dritte Tabelle gab Auskunft über mehr als 68.000 Beschäftigte des Konzerns – davon über 5.000 in der EU und über 1.800 in Deutschland – in den meisten Fällen jeweils mit privater Anschrift, Telefonnummer und E-Mail-Adresse sowie der Sozialversicherungsnummer und der Nummer des Reisepasses (bzw. des nationalen Identitätsdokuments). Zu den betroffenen Personen gehörte auch der Vorstandsvorsitzende des Konzerns. Kunden-, Fahrzeug- oder Produktionsdaten waren nicht Bestandteil des Datenpaketes, das uns der Hinweisgeber übersandte. Der ehemalige Beschäftigte wies allerdings ausdrücklich darauf hin, dass er in seiner Position eigentlich keinen Zugriff auf eine derart umfangreiche Datensammlung über Beschäftigte des Konzerns hätte haben dürfen, da er in keiner Weise mit Aufgaben aus dem Bereich der Personalverwaltung betraut war.

Nachdem wir uns einen ersten Überblick über die zugesandten Daten verschafft hatten, prüften wir unsere datenschutzrechtliche Zuständigkeit für weitere Ermittlungen. Wenn die Angaben des Hinweisgebers zutreffen sollten, handelte es sich unzweifelhaft um eine grenzüberschreitende Datenverarbeitung personenbezogener Daten. Für diesen Fall sieht Artikel 56 Datenschutz-Grundverordnung (DS-GVO) vor, dass die Aufsichtsbehörde am europäischen Hauptsitz des Unternehmens die Federführung bei der Bearbeitung innehat. Andere Datenschutzaufsichtsbehörden in der EU können sich als sogenannte betroffene Aufsichtsbehörden z. B. dann melden, wenn die Datenverarbeitung erhebliche Auswirkungen auf Personen in ihrem örtlichen Zuständigkeitsbereich hat. Federführende und betroffene Aufsichtsbehörden arbeiten gemäß Artikel 60 DS-GVO zusammen, insbesondere um eine einheitliche datenschutzrechtliche Bewertung vorzunehmen.

In diesem Sinne informierten wir im Rahmen einer Videokonferenz die niederländische Aufsichtsbehörde über die uns vorliegenden Erkenntnisse, da sie wegen des europäischen Hauptsitzes des Unternehmens in diesem Fall federführend ist. Unsere Kolleginnen und Kollegen in Den Haag übernahmen die weiteren Ermittlungen. Wir stellten ihnen über eine sichere Datenaustauschmöglichkeit auch die vom Hinweisgeber übersandten Daten zur Verfügung. Darüber hinaus meldeten wir uns im gemeinsamen Informationssystem der europäischen Datenschutzaufsichtsbehörden (dem Binnen-

markt-Informationssystem IMI¹⁸ der Europäischen Kommission) als betroffene Aufsichtsbehörde für den Fall.

Auch Journalisten einer großen deutschen Wirtschafts- und Finanzzeitung, denen ebenfalls entsprechende Hinweise und Daten vorlagen, recherchierten in der Angelegenheit. Sie nahmen Kontakt mit einzelnen vom Datenleck betroffenen Personen auf und ließen durch externe Fachleute die Authentizität der Daten überprüfen. Im Ergebnis sahen sie keine Anhaltspunkte, dass es sich nicht um unternehmensinterne Daten handelte. Dementsprechend konfrontierten sie das Unternehmen mit einer Reihe von Fragen, bevor entsprechende Artikel veröffentlicht wurden.

Kurze Zeit später erhielten die niederländische Aufsichtsbehörde und auch wir eine formale Meldung gemäß Artikel 33 DS-GVO zu einer Datenschutzverletzung in dem in Rede stehenden Konzern. Nach entsprechenden internen Ermittlungen informierte das Unternehmen im weiteren Verlauf darüber hinaus die betroffenen Beschäftigten nach Artikel 34 DS-GVO und offerierte seine Unterstützung, um einen möglichen Identitätsmissbrauch zu verhindern.

Die Untersuchungen unserer niederländischen Kolleginnen und Kollegen dauerten zum Ende des Berichtsjahres weiter an. Insbesondere wurde das Unternehmen zur Stellungnahme und zur Beantwortung einer Reihe von Fragen aufgefordert. Die Auswertung der Antworten ist noch nicht abgeschlossen. Wir werden uns als betroffene Aufsichtsbehörde bei der datenschutzrechtlichen Bewertung und ggf. der Einleitung von Aufsichtsmaßnahmen einbringen.

18 Siehe A VI 6.

2 Herausgabe von Protokolldaten einer Bank

Der Missbrauch fremder Kreditkarten birgt ein hohes Schädigungspotenzial. Glück im Unglück kann für Geschädigte solcher Taten sein, dass die im Hintergrund ablaufenden Arbeitsschritte von Finanztransaktionen umfassend protokolliert und gespeichert werden. Aus diesen Daten lassen sich möglicherweise Hinweise auf die Täterin oder den Täter ableiten. Das nahm ein Geschädigter zum Anlass, diese Protokolle bei seiner Bank unter Berufung auf einen Auskunftsanspruch aus Artikel 15 Datenschutz-Grundverordnung (DS-GVO) anzufordern. Dieser Schritt blieb jedoch zunächst erfolglos, da die Bank den Antrag mit der Begründung ablehnte, die Voraussetzungen des Auskunftsanspruchs lägen nicht vor. Die hierauf fußende Beschwerde nahmen wir zum Anlass, das zu überprüfen.

Artikel 15 DS-GVO setzt voraus, dass personenbezogene Daten verarbeitet werden. Das sind gemäß Artikel 4 Nummer 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Zur Vermeidung von Anwendungslücken ist der Begriff sehr weit zu verstehen. Die Protokolle, so die Argumentation der Bank, hätten jedoch keinerlei Personenbezug. Denn es handele sich um numerische Transaktionsdaten sowie Aufzeichnungen der Authentifizierungen. Bezüge zu Person und Konto seien den Protokollen hingegen nicht zu entnehmen.

Uns wurde ein solches Protokoll zur Ansicht und Prüfung vorgelegt. Wir sind sodann zu einer anderen Auffassung gelangt. Zwar ist den Protokollen weder ein Name noch eine Kontonummer zu entnehmen. Dennoch müssen die Protokolle einer Transaktion und damit einem Konto zugeordnet werden können. Wäre dem nicht so, entfele eine mögliche Beweisfunktion sowie die Notwendigkeit der Anfertigung und Speicherung. Denn bei einer vollständigen Anonymisierung könnte bei der Fülle der Kreditkarteneinsätze nie zugeordnet werden, welcher Protokolleintrag welche Transaktion betrifft. Es besteht damit ein hohes praktisches Bedürfnis einer Zuordnung zu Transaktion, Konto und kontoführender Person. Mit dieser Zuordnung besteht zumindest eine mittelbare Personenbeziehbarkeit. Aufgrund der weiten Begriffsbestimmung des Artikels 4 Nummer 1 DS-GVO folgt daraus, dass die Protokolle

**Wo ist mein
Geld geblieben?**

durchaus Personenbezug haben, von dem Auskunftsanspruch aus Artikel 15 DS-GVO umfasst sind und herausgegeben werden müssen.

Nachdem wir der Bank unsere Rechtsauffassung dargelegt hatten, schloss sie sich den Ausführungen an und stellte die vom Beschwerdeführer geforderten Unterlagen zur Verfügung.

3 Ein Mailserver, zwei Sicherheitslücken und kein Backup

Im April 2023 erreichte uns eine Meldung einer Verletzung des Schutzes personenbezogener Daten eines brandenburgischen Unternehmens. Der Verantwortliche berichtete uns zunächst, dass alle erreichbaren IT-Systeme durch Schadsoftware verschlüsselt, das letzte Backup der Daten vollständig gelöscht und Datenabflüsse von rund 1,5 Terabyte über einen Zeitraum von ca. sechs Stunden festgestellt wurden. Eine im System hinterlegte Erpresserbotschaft bestätigte den Befall der Systeme mit einer sogenannten Ransomware. Bemerkte wurde dies durch den Wachschutz des Unternehmens. Ihm fiel auf, dass die IT-basierten Alarmanlagen nicht mehr funktionierten. Vom Vorfall betroffen waren die personenbezogenen Daten der Beschäftigten (inklusive des ehemaligen Personals), der Kundinnen und Kunden sowie der Aktionärinnen und Aktionäre des Unternehmens. Betroffene Datenkategorien waren gemäß der Meldung – neben Name, Adresse, Telefonnummer und E-Mail-Adresse – insbesondere auch Personal-, Bank- und Ausweisdaten. Eine genaue Anzahl der betroffenen Personen konnte der Verantwortliche bis zum Abschluss des Vorgangs nicht ermitteln; auch eine grobe Schätzung war ihm nicht möglich. Der relativ große Umfang an abgeflossenen Daten erklärt sich insbesondere dadurch, dass das Unternehmen datenintensive Aufträge von Kundinnen und Kunden bearbeitete.

Backups an anderem Ort lagern

Im Zuge der Meldung leitete die Landesbeauftragte ein Verwaltungsverfahren ein und hörte den Verantwortlichen an. Er erläuterte uns, dass der Zugriff zunächst auf einen extern erreichbaren E-Mail-Server und von dort via RDP-Protokoll auf die internen Server erfolgte. Über diesen Weg gelang den Angreifenden die Infiltration der Systeme mit Ransomware. Da der Backup-Server in derselben Domäne wie die anderen Server integriert war, konnte die Schadsoftware auch die Datensicherung befallen.

Laut Darstellung des Verantwortlichen wurden die IT-Systeme „auf unerklärliche Art und Weise“ mit erweiterten Administrationsrechten erreicht und verändert. Unbekannte Dritte löschten alle virtualisierten Server, sodass eine Analyse des Vorfalls nur anhand der

physischen Server möglich gewesen sei. Der Verantwortliche gab an, dass die Ursache des Vorfalls auf zwei Sicherheitslücken der genutzten Software zurückzuführen sei. Ein eigenes Verschulden konnte er nicht feststellen. Zum Zeitpunkt des Vorfalls waren laut Unternehmen alle relevanten und aktuellen Sicherheitsupdates aufgespielt.

In einer zweiten Anhörung teilte uns der Verantwortliche mit, man habe nun festgestellt, dass nur personenbezogene Daten im Dateiserver vom Vorfall betroffen waren. Systeme zur Finanz- und Lohnbuchhaltung sowie das Dokumentenmanagementsystem für Rechnungen und digitale Personalakten sollen aufgrund der zusätzlichen Zugangssperren sowie der weiteren ergriffenen technischen und organisatorischen Maßnahmen von der Verletzung des Schutzes personenbezogener Daten nicht betroffen gewesen sein. Diese neuen Informationen reduzierten die datenschutzrechtliche Schwere des Vorfalls, wenngleich sie teilweise widersprüchlich zu den Inhalten der Erstmeldung waren. Die Landesbeauftragte stellte das Verfahren mit einigen Hinweisen zu technischen und organisatorischen Maßnahmen ein, erwägt allerdings eine Prüfung der IT-Systeme vor Ort.

4 Verlust von Gesundheitsdaten bei Transport und Aufbewahrung

Im Berichtsjahr wurden der Landesbeauftragten erneut verschiedene Fälle von Verletzungen des Datenschutzes gemeldet, bei denen es zu einem Verlust von personenbezogenen Gesundheitsdaten kam. Diese werden den besonderen Kategorien personenbezogener Daten nach Artikel 9 Datenschutz-Grundverordnung (DS-GVO) zugerechnet. Ihre Verarbeitung unterliegt spezifischen Bedingungen. Auch die Anforderungen an die technischen und organisatorischen Maßnahmen zur Wahrung des Datenschutzes sind naturgemäß höher, da z. B. der Verlust, die unbefugte Änderung oder die Kenntnisnahme dieser Daten durch hierzu nicht Berechtigte mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden sein können. Nicht alle Verantwortliche sind sich dessen immer bewusst, wie drei ausgewählte Beispiele zeigen:

Im ersten Fall vergaß eine Mitarbeiterin eines ambulanten Pflegedienstes ihren Rucksack mit Leistungsnachweisen zur Pflegefähigkeit. Als sie eine Straßenbahn bestieg, verblieb der Rucksack an der Haltestelle. In den Nachweisen hatte sie dokumentiert, welche konkreten Arbeiten bei welchen zu pflegenden Personen ausgeführt wurden. Die Unterlagen enthielten neben deren Namen und Anschrift auch Gesundheitsdaten. Obwohl die Mitarbeiterin sofort zur Haltestelle zurückfuhr, nachdem sie den Verlust bemerkte, konnte der Rucksack mit den Dokumenten nicht wieder aufgefunden werden.

Die Leitung des Pflegedienstes meldete den Verlust der Leistungsnachweise als Verletzung des Datenschutzes gemäß Artikel 33 DS-GVO unverzüglich an unsere Dienststelle. Auch die betroffenen Personen bzw. ihre mit einer Vorsorgevollmacht ausgestatteten Angehörigen wurden darüber informiert. Aufgrund der besonderen Risiken halten wir eine solche Information nach Artikel 34 DS-GVO beim Verlust von Gesundheitsdaten in der Regel für erforderlich. Im Rahmen der Untersuchung des Vorfalls wollten wir vom Verantwortlichen wissen, welche Maßnahmen er ergriffen hatte, um eine Wiederholung zu vermeiden. In seiner Antwort erläuterte der Pflegedienstleiter die umfangreichen Sensibilisierungen der Beschäftigten für einen sorgsamen Umgang mit Dokumenten zu Pflegeleistungen.

Wir empfehlen darüber hinaus zu prüfen, ob eine pseudonymisierte Führung der Pflegedokumentation vor Ort zur Minderung der Risiken für betroffene Personen beitragen könnte. Zumindest wären bei Verwendung von Pseudonymen keine Klardaten wie Name und Anschrift aus den verlorenen Unterlagen ersichtlich.

In einem zweiten, ähnlich gelagerten Fall verlor die Inhaberin einer psychotherapeutischen Praxis eine Patientenakte während der Fahrt in einem Nahverkehrsbus. Sie hatte die Akte in einer separaten Tasche verstaut, diese Extratasche jedoch beim Aussteigen vermutlich vergessen. Sofort nach Ankunft in der Praxis telefonierte sie mit der Busgesellschaft, dem Ordnungsamt der entsprechenden Gemeinde und dem Fundbüro. Aber auch nach mehreren Tagen fand sich die Tasche mit der Patientenakte nicht wieder an. Wie im ersten Fall enthielt die Akte sensible Daten aus dem besonderen Verhältnis zwischen der Psychotherapeutin und dem Patienten.

Patientendaten erfordern Obacht

Nachdem die Psychotherapeutin uns gemäß Artikel 33 DS-GVO von dem Datenverlust unterrichtet hatte, suchte sie das persönliche Gespräch mit dem Patienten. Auch er wurde insofern entsprechend der rechtlichen Vorschriften über den Vorfall informiert. Im Ergebnis – so teilte uns die Verantwortliche mit – entschied er sich, die Behandlung fortzusetzen.

Der dritte Fall betraf keine Papierunterlagen, sondern elektronisch gespeicherte Daten. Ein Verein, der u. a. Wohngruppen für Menschen mit Behinderung betreut, teilte uns mit, dass ein USB-Stick mit mehreren Datensätzen zu Mitgliedern einer Wohngruppe und mit Beschreibungen ihrer Entwicklung nicht mehr auffindbar war. Die Daten waren zuvor für das zuständige Sozialamt zusammengestellt und aufbereitet worden.

Die Leitung des Vereins fragten wir, welche grundsätzlichen Regelungen zum Umgang mit externen Datenspeichern bestanden und welche konkreten technischen Maßnahmen getroffen wurden, um Daten auf solchen Datenspeichern vor unbefugter Kenntnisnahme (etwa bei einem Verlust) zu schützen. Es stellte sich heraus, dass die Vereinsleitung die Nutzung von USB-Sticks zwar untersagt, diese Festlegung aber bislang nicht konsequent kontrolliert hatte. Sie führte unverzüglich entsprechende Belehrungen der Beschäftigten durch und sagte zu, die Mängel bei den Kontrollen abzustellen. Wir



empfehlen darüber hinaus dringend, auch die auf den Festplatten der genutzten PCs gespeicherten Gesundheitsdaten standardmäßig zu verschlüsseln, um mögliche Risiken unbefugter Kenntnisnahme (z. B. bei einem Einbruch in die Geschäftsräume und Diebstahl der Geräte) zu mindern.

Die drei beschriebenen Fälle zeigen, dass der sorgsame Umgang mit sensiblen Daten – hier mit Gesundheitsdaten – von grundlegender Bedeutung für die Einhaltung der datenschutzrechtlichen Bestimmungen ist. Hierzu gehört insbesondere, dass Verantwortliche ihre Beschäftigten umfassend sensibilisieren, dass sie technische und organisatorische Maßnahmen umsetzen, um entsprechenden Risiken zu begegnen, und dass sie die Einhaltung der Vorgaben auch kontrollieren. Sollte es gleichwohl zu einer Verletzung des Datenschutzes kommen, ist der Vorfall unserer Behörde unverzüglich und möglichst binnen 72 Stunden anzuzeigen. Darüber hinaus sind im Regelfall auch die betroffenen Personen hierüber zu informieren.

5 Mitteilung der Arbeitsunfähigkeit per E-Mail

Zu Beginn des Berichtszeitraums erreichte uns die Beschwerde eines Beschäftigten, der mit einer geänderten Verfahrensweise für die Mitteilung der Arbeitsunfähigkeit, die seine Arbeitgeberin im neuen Jahr eingeführt hatte, nicht einverstanden war. Wie bisher sollten Beschäftigte für den Fall einer krankheitsbedingten Abwesenheit zunächst unverzüglich ihre direkt vorgesetzte Person informieren. Diese war somit in der Lage, organisatorische Maßnahmen für die Aufrechterhaltung der Geschäftsabläufe zu ergreifen. Zusätzlich wurden die Beschäftigten angewiesen, im Krankheitsfall „eine formlose E-Mail an das Personalmanagement“ zu senden. Sie mussten dabei Beginn und (voraussichtliches) Ende der Arbeitsunfähigkeit angeben.

Die Beschwerde richtete sich nur gegen den zweiten Teil der Anweisung: Der Beschwerdeführer monierte, dass er nicht wisse, wer sich hinter dem „Personalmanagement“ verbirgt. Jedenfalls gehörte die E-Mail-Adresse, an welche die Informationen zu senden waren, nicht zu seiner Arbeitgeberin. Außerdem schien ihm der Versand von Gesundheitsdaten per einfacher E-Mail als zu unsicher – zu technischen und organisatorischen Maßnahmen, durch die Risiken für die Vertraulichkeit und Integrität der Daten bei ihrer Übersendung und Weiterverarbeitung beherrscht werden können, gab es in der neuen Dienstanweisung keine Angaben.

Wir baten das Unternehmen, bei dem der Beschwerdeführer beschäftigt war, um eine Stellungnahme. Insbesondere wollten wir wissen, welche Stelle das Personalmanagement war, welche Aufgaben diese Stelle hatte und – wenn es, wie vermutet, eine externe Stelle war – wie die datenschutzrechtliche Einbindung erfolgte (z. B. die Form der Beauftragung). Weiter fragten wir, ob Beschäftigte auch alternative Wege zur Information des Personalmanagements hatten, falls sie Daten zu ihrer Arbeitsunfähigkeit nicht per E-Mail mitteilen wollten oder konnten. Und letztlich interessierten wir uns für die umgesetzten technischen und organisatorischen Maßnahmen, wie z. B. die verschlüsselte Übertragung der E-Mails, die Beschränkung der Zugriffe oder die Löschrufen der eingegangenen Meldungen.

In seiner Antwort informierte uns das Unternehmen, dass sich bereits mehrere Beschäftigte hinsichtlich der neuen Geschäftsanwei-



sung beschwert hatten und deshalb ohnehin schon eine Korrektur der Vorgaben erfolgt war. Neben der Übersendung einer E-Mail mit Angaben zur voraussichtlichen Krankheitsdauer wurde nun auch der postalische Weg zugelassen (wie früher). Die ursprüngliche Intention der Neuregelung war, den Beschäftigten einen einfachen und schnellen Weg zur Information der Arbeitgeberin anzubieten. Allerdings wollte man den Informationsweg nicht auf die elektronische Form reduzieren; vielmehr sollte sie zusätzlich zugelassen werden. Dies hat die Geschäftsführung in der Anweisung unverzüglich klar gestellt.

Weiter wurde ein neues E-Mail-Postfach in der Domäne des Unternehmens eingerichtet, an das die elektronischen Krankmeldungen zu richten waren. Somit war für Beschäftigte erkennbar, dass ihre Arbeitgeberin die Adressatin der Nachrichten war. Gleichwohl erfolgte die Bearbeitung der Meldungen durch das erwähnte Personalmanagement. Dabei handelte es sich tatsächlich um eine externe Stelle, konkret um eine separate Servicegesellschaft in der Unternehmensgruppe. Dort sollten u. a. personalwirtschaftliche Aufgaben zusammengefasst werden. Hierzu gehörten auch die Erfassung der Abwesenheiten der Beschäftigten sowie der Abruf der Bescheinigungen zur Arbeitsunfähigkeit vom zu Jahresbeginn eingeführten Portal der Krankenkassen. Aus datenschutzrechtlicher Sicht erfolgte die Einbindung der Servicegesellschaft über einen Vertrag zur Auftragsverarbeitung. Dieser wurde uns vorgelegt. Wir haben das Unternehmen nochmals auf die strikte Weisungsgebundenheit des Dienstleisters in diesem Vertragsverhältnis hingewiesen.

Darüber hinaus erinnerten wir das Unternehmen an seine Informationspflichten. Die Tatsache, dass eine externe Servicegesellschaft die Bearbeitung der Krankmeldungen übernahm sowie auch eventuelle Nachfragen der Beschäftigten beantworten sollte und dabei im Auftrag der Arbeitgeberin agierte, war den Beschäftigten transparent (z. B. im Rahmen der Datenschutzinformation) bekannt zu geben.

Im Hinblick auf die umgesetzten technischen und organisatorischen Maßnahmen verwies das Unternehmen zunächst auf die Verschlüsselung der E-Mails bei ihrem Transport über das Internet. Es räumte ein, dass Nachrichten an Knotenpunkten (z. B. beim Provider) auch unverschlüsselt vorliegen und dort ggf. zur Kenntnis genommen werden konnten. Das Unternehmen bot seinen Beschäftigten keine Möglichkeit an, für die Übersendung der Arbeitsunfähigkeits-

daten per E-Mail eine Ende-zu-Ende-Verschlüsselung zu nutzen und so eine unbefugte Kenntnisnahme zu verhindern. Lediglich die postalische Alternative wurde benannt. Dies bemängelten wir und erläuterten, dass datenschutzrechtlich Verantwortliche, die sensible personenbezogene Daten (hier: Gesundheitsdaten) gezielt entgegennehmen, auch technische Voraussetzungen schaffen müssen, durch die Absenderinnen und Absender von E-Mails die Möglichkeit erhalten, eine Ende-zu-Ende-Verschlüsselung zu nutzen.¹⁹ Weiterhin bemerkten wir, dass durch den E-Mail-Server des Unternehmens neben aktuellen auch veraltete kryptografische Verfahren unterstützt wurden, deren Abschaltung wir dringend empfahlen. Und letztlich gaben wir Hinweise zu dem technischen Zertifikat, mit dem sich der E-Mail-Server beim Aufbau der Kommunikation im Internet ausweist.

Richtig krankmelden

Unsere Fragen zur Verhinderung unberechtigter Zugriffe auf die bei der Servicegesellschaft verarbeiteten Meldungen zur Arbeitsunfähigkeit beantwortete das Unternehmen unter Verweis auf das strenge Rollen- und Rechtekonzept. Danach wurden nur für die Arbeitstätigkeit unbedingt erforderliche Zugriffsrechte an die beim Dienstleister tätigen Mitarbeiterinnen und Mitarbeiter vergeben. Dies bezog sich insbesondere auf Zugriffe auf das Postfach, in dem die E-Mails eingingen und gespeichert waren. Eine Weiterleitung der dort enthaltenen E-Mails an andere Adressen war untersagt. Die Löschung der E-Mails erfolgte unverzüglich, nachdem die entsprechenden Bescheinigungen zur Arbeitsunfähigkeit vom Portal der Krankenkassen abgerufen wurden.

¹⁹ Siehe A V 1.

6 Veröffentlichung von Alarmmeldungen der Feuerwehr im Internet

In den vergangenen Jahren erhielt unsere Dienststelle wiederholt Hinweise von Bürgerinnen und Bürgern sowie Informationen von verantwortlichen Rettungsleitstellen, dass Alarmmeldungen der Feuerwehr live im Internet veröffentlicht wurden. Zum Teil hatten Unberechtigte die Meldungen abgefangen und publiziert. Zum Teil hatten auch Einsatzkräfte der (Freiwilligen) Feuerwehr selbst ein Empfangsgerät für Alarmmeldungen mit einem Computer verbunden und diesen so eingerichtet, dass die auf dem Empfänger eingehenden Meldungen automatisch an einen entsprechend konfigurierten Webserver weitergereicht wurden. Die über den Webserver bereitgestellten Alarmierungen konnten so z. B. auf einem Smartphone von Feuerwehreinsatzkräften empfangen werden. Sie wollten damit der Pflicht entgegen, einen gesonderten und verschlüsselten Alarmmeldeempfänger mitzuführen.

Bei dieser Vorgehensweise wurde nicht nur die Verschlüsselung der Alarmnachrichten umgangen; vielmehr waren die Meldungen frei im Internet verfügbar, wenn auf dem Webserver keine entsprechenden Sicherheitsmaßnahmen (wie z. B. eine Passwortsicherung oder die Einschränkung von Zugriffsrechten nach einem geeigneten Rollen-Rechte-Konzept) umgesetzt wurden. Sie konnten dann auch von unberechtigten Personen abgerufen und eingesehen werden.

Problematisch ist die Tatsache, dass in Alarmmeldungen regelmäßig auch besondere Kategorien personenbezogener Daten gemäß Artikel 9 Datenschutz-Grundverordnung (DS-GVO) – wie z. B. Gesundheitsdaten – verarbeitet werden. Diese Daten bedürfen danach eines höheren Schutzes. An ihre Verarbeitung sind spezifische Anforderungen zu stellen, da ein Missbrauch für betroffene Personen mit besonderen Risiken verbunden sein kann. Selbst aus gekürzten Alarmmeldungen lassen sich noch oft

Schneller als die Feuerwehr

Adressen und Gesundheitsdaten extrahieren oder ableiten, sodass die Kenntnis dieser Informationen auf die an der Rettung beteiligten Stellen beschränkt bleiben muss.

Spätestens nach unserem Einschreiten konnten die in Rede stehenden, mangelhaft gesicherten Webserver bisher immer zeitnah abgeschaltet werden. Falls die Verursacherinnen oder Verursacher bzw. die Verantwortlichen identifizierbar waren, wurden sie dahingehend belehrt, dass das unbefugte Abfangen bzw. Veröffentlichen von Funknachrichten eine Straftat gemäß § 5 Telekommunikation-Telemedien-Datenschutz-Gesetz darstellt, welche nach § 27 der Vorschrift mit bis zu zwei Jahren Haft oder Geldstrafe geahndet werden kann. Da Strafermittlungsverfahren bei der Polizei eingeleitet wurden, haben wir Maßnahmen gemäß Artikel 58 DS-GVO zunächst zurückgestellt.

Der Umstand, dass die unberechtigten Veröffentlichungen von Alarmmeldungen im Internet zuvor vermutlich bereits über Monate oder gar Jahre erfolgten, besorgte uns allerdings sehr. Wir wandten uns daher mit der Bitte an den Landesbranddirektor, die Regionalleitstellen bzw. die Feuerwehren im Land Brandenburg entsprechend zu sensibilisieren und z. B. über ein Rundschreiben zu informieren, dass ein derartiger Umgang mit Alarmmeldungen sowohl datenschutzrechtlich unzulässig ist als auch eine Straftat darstellt. Gerade angesichts der ansteigenden Zahlen dieser Vorkommnisse mit jeweils zahlreichen betroffenen Personen sahen wir die Notwendigkeit für eine Belehrung der Einsatzkräfte vor Ort.

Im Rahmen eines Gesprächs mit Vertreterinnen und Vertretern des Ministeriums des Innern und für Kommunales erörterten wir das weitere Vorgehen. Während des Termins stellte sich heraus, dass auch Einsatzkräfte von Rettungsdiensten zum Teil in ähnlicher Weise mit Alarmmeldungen umgingen. Deshalb wurde auch das zuständige Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz bei der Erarbeitung des Informationsschreibens einbezogen.



V Ausgewählte Beratungen

1 Schutz personenbezogener Daten bei der E-Mail-Kommunikation

E-Mails werden seit vielen Jahren routinemäßig für die Kommunikation in bzw. mit Unternehmen, Vereinen, Behörden und anderen datenschutzrechtlich Verantwortlichen eingesetzt. In der Regel umfassen die Inhalte von E-Mails sowie die näheren Umstände der Kommunikation (d. h. wer hat wann mit wem E-Mails ausgetauscht) auch personenbezogene Daten. Verantwortliche und ihre Auftragsverarbeiter müssen die Risiken, die sich bei dem Transport und der Weiterverarbeitung von E-Mails ergeben, durch geeignete und angemessene technische und organisatorische Maßnahmen hinreichend mindern. Sie haben dabei gemäß Artikel 25 und 32 Datenschutz-Grundverordnung Art, Umfang, Umstände und Zwecke der Datenverarbeitung, die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie den Stand der Technik und die Implementierungskosten zu berücksichtigen.

Bereits 2020 in einer ersten und 2021 in einer leicht überarbeiteten Fassung verabschiedete die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) eine Orientierungshilfe zu Maßnahmen für den Schutz personenbezogener Daten bei der Übermittlung per E-Mail. Diese richtet sich an Verantwortliche und Auftragsverarbeiter und enthält Anforderungen, die beim Transport von E-Mails umzusetzen sind. Ausdrücklich nicht betrachtet werden die Speicherung und Aufbewahrung von E-Mails sowie die Weiterverarbeitung innerhalb der öffentlichen bzw. nicht öffentlichen Stelle oder durch Dritte.

In der Orientierungshilfe werden Maßnahmen für typische Verarbeitungssituationen dargestellt. Ausgangspunkt bilden dabei mögliche Risiken für betroffene Personen im Hinblick auf die Gewährleistung der Vertraulichkeit und Integrität der Kommunikation, die Rolle der kommunizierenden Parteien (d. h. Empfang bzw. Versand) sowie der Stand der Technik. Unter Beachtung der konkreten Umstände der

Datenverarbeitung, ihres Umfangs und der verfolgten Zwecke sind im Einzelfall auch abweichende Maßnahmen denkbar. Besondere Schwierigkeiten können sich dadurch ergeben, dass bei der datenschutzkonformen E-Mail-Kommunikation die sendende und die empfangende Seite zusammenarbeiten müssen. Zwar trifft für eine einzelne, konkrete Übermittlung die sendende Seite die Hauptverantwortung, allerdings müssen auf der empfangenden Seite entsprechende Vorkehrungen getroffen worden sein, um Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Werden Auftragsverarbeiter in Anspruch genommen, müssen Verantwortliche durch Weisungen sicherstellen, dass die Anforderungen durch diese umgesetzt werden.

Die in der Orientierungshilfe der Datenschutzkonferenz beschriebenen Maßnahmen lassen sich kurz wie folgt zusammenfassen:

- Nehmen Verantwortliche gezielt personenbezogene Daten per E-Mail entgegen, müssen sie zur Wahrung der Vertraulichkeit bereits bei normalen Risiken für die Rechte und Freiheiten der betroffenen Personen die Kommunikation über einen verschlüsselten Kanal ermöglichen. Der empfangende E-Mail-Server muss den Aufbau einer verschlüsselten Verbindung erlauben²⁰ und darf dabei nur solche kryptografischen Algorithmen zulassen, die dem aktuellen Stand der Technik entsprechen.²¹ Der sendende E-Mail-Server muss so konfiguriert sein, dass er von der Möglichkeit der verschlüsselten Kommunikation auch Gebrauch macht und nur sichere kryptografische Algorithmen verwendet. Sind diese Voraussetzungen erfüllt, wird die Kommunikationsverbindung stets verschlüsselt (obligatorische Transportverschlüsselung). Damit lässt sich ein Basisschutz gegen passives Belauschen des Datenverkehrs durch Angreiferinnen oder Angreifer erreichen. Erfüllen empfangende oder sendende Partei die Anforderungen nicht oder nicht vollständig, sind geeignete Maßnahmen festzulegen, z. B. den Verbindungsaufbau abubrechen, die andere Seite auf die Verschlüsselungs-

20 In der Regel per TLS (Transport Layer Security), aktuell gelten die Versionen TLS 1.2 und 1.3 als sicher.

21 In der Regel entsprechend der Technischen Richtlinie TR 02102 des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

anforderungen hinzuweisen und alternative Kommunikationsmechanismen zu nutzen.

- Bestehen bei der E-Mail-Kommunikation hohe Risiken für die Rechte und Freiheiten der betroffenen Personen, falls die Vertraulichkeit gebrochen wird, müssen Verantwortliche sowohl eine Ende-zu-Ende-Verschlüsselung der Nachrichten ermöglichen (empfangende Seite) bzw. nutzen (sendende Seite) als auch besondere Vorkehrungen treffen, um zusätzlich die Authentizität der kommunizierenden Parteien zu überprüfen und sicherzustellen (qualifizierte Transportverschlüsselung). Die Ende-zu-Ende-Verschlüsselung²² schützt die Inhalte einer E-Mail beim Transport so, dass nur die empfangende Seite sie zur Kenntnis nehmen kann. Die qualifizierte Transportverschlüsselung sichert darüber hinaus, dass es sich dabei tatsächlich um die richtige, zum Empfang befugte Kommunikationspartei handelt. Sie wirkt auch gegen aktive Angriffe auf den Datenverkehr bzw. die beteiligten E-Mail-Server. Zur Gewährleistung der Authentizität der Kommunikationsparteien existieren technische Standards, bei denen die Information über die zugelassenen, berechtigten E-Mail-Server digital signiert und verschlüsselt ausgetauscht werden.²³ Diese Informationen sind auf der jeweils anderen Seite der Kommunikation zu validieren.
- Werden E-Mails empfangen, bei denen die Verletzung der Integrität Risiken für die Rechte und Freiheiten der betroffenen Personen verursacht, sollten Verantwortliche ihre E-Mail-Server so konfigurieren, dass sie automatisch entsprechende digitale Signaturen an die Nachrichten anfügen (sendende Seite) bzw. die Signaturen überprüfen (empfangende Seite). Im Fall hoher Risiken, die durch die Verletzung der Integrität entstehen, sind für die Signatur von E-Mails beim Versand speziell gesicherte kryptografische Schlüssel zu verwenden bzw. beim Empfang die Nachrichtensignaturen so zu prüfen, dass auch die Authentizität der sendenden Partei zuverlässig gewährleistet ist. Im Regelfall

22 Z. B. per PGP (Pretty Good Privacy) oder S/MIME (Secure/Multipurpose Internet Mail Extensions).

23 Z. B. DNSSEC (Domain Name System Security Extensions) und DANE (DNS-based Authentication of Named Entities).

wird hierfür zuvor die Zugehörigkeit eines kryptografischen Schlüssels zu einer Kommunikationspartei durch vertrauenswürdige Dritte bestätigt.

Aus unserer Beratungs- und Aufsichtstätigkeit wissen wir, dass viele Verantwortliche Schwierigkeiten haben, die genannten Maßnahmen in vollem Umfang umzusetzen. Vielfach wird zwar eine einfache Transportverschlüsselung implementiert, allerdings nur dann, wenn beide kommunizierende E-Mail-Server die Funktion unterstützen. Falls dies nur auf eine Seite zutrifft oder kryptografische Verfahren genutzt werden, die nicht dem Stand der Technik entsprechen, findet die Kommunikation oft trotzdem statt – sie ist dann allerdings unsicher. Auch eine Prüfung der Authentizität der kommunizierenden E-Mail-Server im Rahmen der qualifizierten Transportverschlüsselung findet nur bei einem geringen Anteil der Gesamtkommunikation statt, da oftmals die entsprechenden Vorkehrungen zur

Verschlüsselung – fremde Augen sehen nichts

Umsetzung der o. g. technischen Standards nicht getroffen werden. Hinsichtlich der Ende-zu-Ende-Verschlüsselung können wir in den letzten Jahren zwar eine Zunahme der Nutzung verzeichnen (auch bei unserer Kommunikation mit Unternehmen oder beschwerdeführenden Personen), die jedoch bezogen auf den Gesamtumfang der E-Mail-Kommunikation nur gering ist.

Gerade in Fällen, bei denen der Verlust von Vertraulichkeit oder Integrität der E-Mail-Inhalte oder der Umstände der Kommunikation zu hohen Risiken für Betroffene führt, halten wir die aktuelle Situation für verbesserungswürdig. Bereits in der Vergangenheit haben wir die Verantwortlichen entsprechend sensibilisiert und auf die in der Orientierungshilfe der Datenschutzkonferenz beschriebenen Maßnahmen hingewiesen. Beispielhaft sei hier auf Fälle verwiesen, bei denen Landesbehörden die Inhalte disziplinarischer Ermittlungen per einfacher E-Mail versandten, Lehrkräfte sensible Daten von Schülerinnen und Schülern nicht hinreichend verschlüsselten²⁴ oder Jugendämter den freien Trägern der Jugendhilfe keine Möglichkei-

24 Tätigkeitsbericht Datenschutz 2020, A V 1.4.

ten zur Ende-zu-Ende-verschlüsselten Übermittlung von Gutachten oder Hilfeplänen für Jugendliche bereitstellten.²⁵

Im Berichtszeitraum wurden wir durch einen interessierten Journalisten auf die unzureichende Umsetzung der Maßnahmen zum Schutz personenbezogener Daten bei der E-Mail-Kommunikation hingewiesen. Er hatte automatisiert für eine Vielzahl öffentlicher Stellen die „zuständigen“ E-Mail-Server hinsichtlich der von außen erkennbaren Funktionsmerkmale getestet. Auch wenn das Bild nicht vollständig ist, da beispielsweise die Möglichkeit einer Ende-zu-Ende-Verschlüsselung nicht in die Auswertung einfluss, bestätigten sich unsere oben dargestellten Beobachtungen. Wir werden dies zum Anlass nehmen, verstärkt die Umsetzung der Maßnahmen zum Schutz der E-Mail-Kommunikation bei Verantwortlichen und Auftragsverarbeitern in unserem Zuständigkeitsbereich einzufordern. Bei begründetem Anlass werden wir auch von unseren Abhilfemaßnahmen nach der Datenschutz-Grundverordnung Gebrauch machen.

2 Das Standard-Datenschutzmodell – ein Werkzeug zur Erfüllung datenschutzrechtlicher Anforderungen

Spätestens seit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) sollte – nach dem Willen des europäischen Gesetzgebers – für jeden Verantwortlichen die systematische Umsetzung der datenschutzrechtlichen Anforderungen selbstverständlich sein. Gleichwohl erfahren wir immer wieder, dass öffentliche wie nicht öffentliche Stellen – von der Gemeindeverwaltung bis zum Ministerium, vom Kleinstunternehmen bis zum Großkonzern – große Schwierigkeiten mit den abstrakt gehaltenen rechtlichen Anforderungen haben und selbst mit einiger Fachkenntnis regelmäßig Probleme bei der konkreten Implementierung vor Ort auftreten.

Um diesem Problem zu begegnen, hat eine Arbeitsgruppe des Arbeitskreises Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) unter Leitung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein in den vergangenen Jahren das Standard-Datenschutzmodell (SDM) entwickelt. Es beansprucht für sich, Verantwortliche dabei zu unterstützen, die normativen Anforderungen der Datenschutz-Grundverordnung in funktionale Anforderungen zu transformieren. Das Modell ermöglicht, die rechtlichen Soll-Vorgaben systematisch und nachvollziehbar mit dem Ist-Zustand der Verarbeitung personenbezogener Daten zu vergleichen sowie technische und organisatorische Maßnahmen abzuleiten, um die Risiken der Datenverarbeitung für betroffene Personen hinreichend zu mindern. Die Anwendung des SDM kann so einen wesentlichen Beitrag zur effektiven Umsetzung der Datenschutz-Grundverordnung leisten.

Version 3.0 des Standard-Datenschutzmodells wurde von der Datenschutzkonferenz im November 2022 per Beschluss verabschiedet. Vor diesem Hintergrund wurden im Berichtsjahr die Mitarbeiterinnen und Mitarbeiter unserer Behörde zu den Inhalten und der Anwendung des SDM geschult. Das Modell fand auch Eingang in das IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik: Dessen Baustein CON.2 verlangt, dass datenschutzrechtliche Bestimmungen eingehalten werden müssen. Wird

das SDM durch Verantwortliche nicht angewandt und werden entsprechende Maßnahmen nicht mit den im Modell vorgeschlagenen Maßnahmen abgeglichen, sollte dies begründet und dokumentiert werden.

Das Standard-Datenschutzmodell greift zunächst die 14 elementaren Verarbeitungstätigkeiten aus Artikel 4 Nummer 2 DS-GVO auf, gruppiert diese in 9 Verarbeitungsvorgänge und überführt sie letztlich in 4 Phasen der Datenverarbeitung. So wird z. B. aus dem „Erheben“ und „Erfassen“ personenbezogener Daten zunächst die Gruppe „Sammeln“ und schließlich die Verarbeitungsphase „Kollektion“. Nach diesem Vorgehen entstehen neben der „Kollektions-“ die „Bereithaltungs-“, „Nutzungs-“ und „Beseitigungsphase“, welche den vollständigen Lebenszyklus einer Verarbeitung personenbezogener Daten abdecken. Die Verarbeitungsaktivitäten werden anschließend hinsichtlich der drei Ebenen der Verarbeitung „Fachlichkeit/Geschäftsprozesse“, „Fachapplikationen“ und „technische Infrastruktur“ betrachtet. Hierbei enthält die erste Ebene alle rechtlichen und fachlichen Anforderungen im Sinne von Verfahren, Geschäftsprozessen und Akteuren. Die zweite Ebene umfasst die eigentliche praktische Umsetzung der Verarbeitung (z. B. mit Softwareanwendungen, Fachapplikationen usw.) und erbt die Anforderungen der ersten Ebene. In der dritten Ebene wird die technische Infrastruktur erfasst, in der die Verarbeitung stattfindet (z. B. technische Dienste, Netze, Server, Datenbanken usw.). Im Ergebnis ermöglicht diese Aufbereitung der Verarbeitungsvorgänge eine ganzheitliche Betrachtung der Verarbeitungen über den vollständigen Lebenszyklus personenbezogener Daten.

Datenschutz systematisch umsetzen

Weiterhin bricht das SDM die rechtlichen Anforderungen der Datenschutz-Grundverordnung auf 7 Gewährleistungsziele herunter. Da sich die Gewährleistungsziele teilweise gegenüberstehen, werden aus 6 elementaren Gewährleistungszielen 3 Dualachsen gebildet, die eine Abwägung zwischen den Zielen bei einer konkreten Verarbeitung unterstützen. Die entsprechenden Gewährleistungsziele nach der Ordnung der Dualachsen sind:

- Integrität und Intervenierbarkeit, also die Unversehrtheit und Originalität der Daten gegenüber der Möglichkeit zum Eingrei-

fen und Verändern (z. B. im Rahmen der Beachtung von Betroffenenrechten),

- Nichtverkettung und Transparenz, also die Umsetzung der Zweckbindung bei der Verarbeitung personenbezogener Daten gegenüber der Nachvollziehbarkeit, Kontrollierbarkeit und möglichen Einsichtnahme in Daten,
- Vertraulichkeit und Verfügbarkeit, also das Ausschließen der unbefugten Kenntnisnahme oder Nutzung personenbezogener Daten gegenüber der Anforderung, den Zugriff für Berechtigte zu gestatten und ihnen die Verarbeitung zu ermöglichen.

Da drei der Gewährleistungsziele (Vertraulichkeit, Integrität und Verfügbarkeit) auch klassische Schutzziele der Informationssicherheit sind, ermöglicht die beschriebene Systematisierung, Maßnahmen zur Gewährleistung des Datenschutzes gegenüber solchen für die Informationssicherheit abzuwägen. Dabei ist die jeweilige Perspektive zu beachten: Aus Sicht des Datenschutzes sind insbesondere solche Maßnahmen relevant, die die Einhaltung der Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen garantieren. Das siebte Schutzziel, die Datenminimierung, begrenzt die Verarbeitung personenbezogener Daten auf den für den jeweiligen Zweck notwendigen Umfang.

Verantwortliche können für konkrete Verarbeitungen personenbezogener Daten die jeweiligen Verarbeitungsvorgänge bzw. -phasen, die Ebenen der Verarbeitung und die Gewährleistungsziele in das „Herzstück“ des SDM – den sogenannten SDM-Würfel – einordnen. Die drei übergreifenden Aspekte werden hierbei unabhängig voneinander betrachtet, wodurch ein dreidimensionaler Würfel mit bis zu 189 Teilwürfeln entsteht. Eine konkrete Verarbeitungstätigkeit wird sich immer nur in einem Ausschnitt des SDM-Würfels bewegen. Die Vorgehensweise ermöglicht es jedoch, Verarbeitungsprozesse vollumfänglich und ganzheitlich zu modellieren, um im Anschluss die entstehenden Risiken für betroffene Personen zu identifizieren sowie kompensierende technische und organisatorische Maßnahmen abzuleiten und lückenlos anzuwenden.

Risiken der Verarbeitung können sich aus der Nichteinhaltung der genannten Gewährleistungsziele ergeben. Das SDM beschreibt 4 Risikotypen sowie eine Methode zur Ermittlung von Risiken und zur

Bestimmung der jeweiligen Risikohöhe. Weiterhin bietet das SDM eine Übersicht mit generischen Maßnahmen, um die Gewährleistungsziele einzuhalten. Sie sind in der Praxis erprobt und zur Anwendung empfohlen. Die Übersicht mit den generischen Maßnahmen wird ergänzt durch einen Katalog an konkreten Referenzmaßnahmen, die in Bausteinen zusammengefasst sind und sich an Verarbeitungstätigkeiten oder Aktivitäten bei der Umsetzung der datenschutzrechtlichen Anforderungen orientieren. Die dort enthaltenen Maßnahmeempfehlungen werden auf die Ebenen Daten, Systeme und Prozesse heruntergebrochen und den Phasen eines Zyklus zur kontinuierlichen Prozessoptimierung zugeordnet. Dies erleichtert die Integration in ein bestehendes Managementsystem wie den BSI-Grundschutz.

Im Ergebnis bietet das Standard-Datenschutzmodell nach unserer Auffassung eine funktionierende Methode, um die Umsetzung des Datenschutzes in einer Organisation zu etablieren und zu kontrollieren. Weiterhin besteht die Möglichkeit, einzelne Aspekte des SDM wie z. B. die Einhaltung der Gewährleistungsziele mit den entsprechenden Maßnahmen auch losgelöst in das unternehmens- oder behördeneigene Datenschutzmanagementsystem zu integrieren. Vor diesem Hintergrund empfehlen wir allen Verantwortlichen die Lektüre. Die entsprechenden Dokumente sind auf unserer Webseite zu finden.

3 Meldedatenerhebung zur Beteiligung von Kindern und Jugendlichen in Gemeindeangelegenheiten

Im Januar 2023 erreichte uns die Anfrage einer amtsfreien Stadt über die Reichweite des § 18a Brandenburgische Kommunalverfassung (BbgKVerf). Die Norm sichert Kindern und Jugendlichen Beteiligungs- und Mitwirkungsrechte in allen sie berührenden Gemeindeangelegenheiten zu und verpflichtet die Kommunen, die Berücksichtigung der Interessen von Kindern und Jugendlichen bei Planungsvorhaben zu dokumentieren. Die Stadt wollte in Umsetzung des Bundesprogramms „Zukunftspaket für Bewegung, Kultur und Gesundheit“ zufällig ausgewählte Jugendliche in einen sogenannten Zukunftsausschuss berufen und die zu diesem Zweck erforderlichen Meldedaten verarbeiten.

Die Frage betraf die Tauglichkeit von § 18a BbgKVerf als alleinige Rechtsgrundlage für die Datenverarbeitung im Sinne von Artikel 6 Absatz 1 Buchstabe e und Absatz 3 Datenschutz-Grundverordnung (DS-GVO), speziell zur Einbindung von Kindern und Jugendlichen in kommunalpolitischen Angelegenheiten.

Für die Weitergabe von Meldedaten ist es erforderlich, dass sich sowohl die Meldebehörde als auch die empfangende Organisationseinheit auf eine Rechtsgrundlage stützen können. Da die Stadt über eine eigene Meldebehörde verfügt, war für diese als Rechtsgrundlage § 37 Absatz 1 i. V. m. § 34 Bundesmeldegesetz über die Weitergabe von Meldedaten innerhalb derselben Verwaltungseinheit heranzuziehen. Danach ist die Weitergabe zulässig, soweit dies zur Erfüllung einer öffentlichen Aufgabe erforderlich ist, die in der Zuständigkeit der empfangenden Organisationseinheit liegt.

Der Bereich stellte zunächst auf § 18a BbgKVerf i. V. m. Artikel 6 Absatz 1 Buchstabe e und Absatz 3 DS-GVO ab. Allerdings ist dieser allein nicht als Rechtsgrundlage tauglich. Grundsätzlich müssen nach Artikel 6 Absatz 3 Satz 2 DS-GVO die Zwecke in der Rechtsgrundlage so bestimmt sein, dass festgestellt werden kann, welche Datenverarbeitungen für die Zweckerreichung erforderlich sind. § 18a BbgKVerf, der zunächst nur von der Sicherung der Beteiligungsrechte spricht, ist für sich genommen ungeeignet: Die Norm erlegt den

Gemeinden nämlich die Pflicht auf, die konkreten Formen der Beteiligung von Kindern und Jugendlichen in der Hauptsatzung zu regeln.

Im Ergebnis stellen die Kommunen durch die Regelung in der Hauptsatzung selbst die Bestimmtheit her, die in § 18a BbgKVerf noch fehlt, um eine taugliche Rechtsgrundlage zu sein. Erst die Satzung bietet auch die Grundlage für die Bestimmung des erforderlichen Umfangs der Verarbeitung personenbezogener Daten. Soll etwa ein Zukunftsausschuss gegründet werden, so ist in einer Satzung dessen Zusammensetzung zu regeln, woraus dann geschlossen werden kann, wie viele Kinder und Jugendliche nach welchem Verfahren zur Beteiligung aufgefordert werden sollen. Eine ordnungsgemäß bestimmte Satzung erlaubt der Gemeinde mithin, von der Meldebehörde diejenigen Datensätze abzurufen, die erforderlich sind, um die dort ebenfalls geregelten Beteiligungsformen zu ermöglichen.

Im vorliegenden Fall war geplant, eine bestimmte Anzahl zufällig ausgewählter Jugendlicher anzuschreiben – eine gängige Vorgehensweise, gegen die datenschutzrechtlich im Falle einer entsprechenden Satzungsbestimmung nichts einzuwenden ist. Die vorab festgelegte Anzahl der abzurufenden Datensätze überstieg die Zahl der tatsächlich verfügbaren Plätze des Ausschusses, da die Stadtverwaltung mit Nichterreichbarkeit oder Ablehnung durch einzelne Jugendliche rechnete. Auch dies konnten wir gut nachvollziehen. Zweifel an der Erforderlichkeit der genannten Daten bestanden nach alledem keine.

Allerdings stellte sich heraus, dass die erforderliche Satzungsregelung noch fehlte. Ein allgemeiner Verweis der Hauptsatzung auf die Beteiligungsformen in der Einwohnerbeteiligungssatzung erwies sich als nicht ausreichend, da dort der geplante Zukunftsausschuss noch keine Erwähnung fand. Wir wiesen darauf hin, dass es erst einer Ergänzung der Satzung bedurfte, um die Verarbeitung von Meldedaten zu erlauben. Darüber hinaus erläuterten wir, dass grundsätzlich mit dem Anschreiben an die Jugendlichen zugleich auch eine Betroffeneninformation nach Artikel 14 DS-GVO zu versenden ist.

Im Ergebnis ist festzustellen, dass Rechtsgrundlagen nur dann im Sinne von Artikel 6 Absatz 1 Buchstabe e und Absatz 3 DS-GVO tauglich sind, wenn deutlich wird, welche personenbezogenen Daten und Verarbeitungsschritte zur Erreichung der Zwecke erforderlich sind. Die Kommunen haben im Rahmen ihrer Selbstverwaltung häufig die



Aufgabe, diese Bestimmtheit selbst herbeizuführen. Sie müssen dies jedoch tun, bevor mit der Datenverarbeitung begonnen wird.

4 Gesetz zur Modernisierung des Kommunalrechts

Im März 2023 begann das Ministerium des Innern und für Kommunales mit der Anhörung zum Entwurf eines Gesetzes zur Modernisierung des Kommunalrechts. Dessen Ziel war u. a. die vollständige Überarbeitung der Brandenburgischen Kommunalverfassung (BbgKVerf). Schon in den letzten Jahren gab es wichtige, eher punktuelle Änderungen.

Der Entwurf betrifft auch die für den Datenschutz bedeutende Vorschrift § 36 Absatz 4 BbgKVerf. In ihrer bei Redaktionsschluss noch gültigen Fassung lautete die Vorschrift: „Jeder hat das Recht, Beschlussvorlagen der in öffentlichen Sitzungen zu behandelnden Tagesordnungspunkte einzusehen. Das Nähere kann die Hauptsatzung regeln.“ Diese einfache Regelung war bisher mit großen praktischen und rechtlichen Umsetzungsschwierigkeiten verbunden, die sich aus dem Spannungsverhältnis zwischen Veröffentlichungsgebot und Datenschutzrecht ergeben:

Es ist seit geraumer Zeit gängige Praxis der Kommunen im Land, der Öffentlichkeit im Interesse der Transparenz möglichst viele Sitzungsunterlagen im Internet zur Verfügung zu stellen. Üblicherweise erfolgt dies in Ratsinformationssystemen. Hierbei ergibt sich das Problem, dass die Veröffentlichung als Übermittlung an eine unbestimmte Anzahl von Empfängerinnen und Empfängern auch datenschutzrechtlichen Einschränkungen unterliegt, wenn die Unterlagen personenbezogene Daten enthalten. Deren Veröffentlichung stellt einen Grundrechtseingriff dar, der nur zulässig ist, wenn sie verhältnismäßig und zum Zweck der Information der Öffentlichkeit nach § 13 Satz 1 BbgKVerf erforderlich ist. Im Zweifelsfall ist zu prüfen, ob ggf. eine Schwärzung von personenbezogenen Daten vorgenommen werden muss.

Die Veröffentlichung von Sitzungsunterlagen, die personenbezogene Daten enthalten, ist inzwischen der häufigste Gegenstand kommunalrechtlicher Beschwerden, die uns erreichen.

Wir beobachten in den letzten Jahren auch, dass die Kommunen das Thema ernster nehmen und zu Unrecht veröffentlichte Daten in der



Regel auf Hinweis betroffener Personen oder Dritter zeitnah löschen. Die Bereitschaft zur Löschung begrüßen wir ausdrücklich; sie ersetzt jedoch nicht die gezielte und rechtzeitige Prüfung der Unterlagen. Schließlich können auch bei kurzzeitigen Veröffentlichungen die unzulässig ins Netz gestellten Daten oft bereits vielfach heruntergeladen werden. Ihre Verbreitung – oft über soziale Medien – kann auch nach der Rücknahme der Veröffentlichung meist nicht mehr wirksam beeinflusst werden.

Eine in der Praxis sehr bedeutsame und besonders problematische Fallgruppe muss in diesem Zusammenhang gesondert erwähnt werden: Beschwerden über die gleichzeitige, ungeprüfte Bereitstellung identischer Sitzungsunterlagen an Gemeindevertretungen und Öffentlichkeit. Ursache hierfür ist, dass Anlagen zu Beschlussvorlagen der öffentlichen Sitzung ungeprüft in der Form, in der sie den Gemeindevertreterinnen und -vertretern zur Verfügung gestellt werden sollen, auch im öffentlichen Teil des Ratsinformationssystems hinterlegt werden und damit der Öffentlichkeit zugänglich sind.

Diese Vorgehensweise verkennt, dass die Übermittlung der Unterlagen an beide Zielgruppen unterschiedlichen Zwecken dient: Die der Verschwiegenheitspflicht gemäß § 21 BbgKVerf unterliegenden Gemeindevertreterinnen und -vertreter erhalten die Beschlussvorlagen zur Erfüllung ihrer Aufgaben und sind hierfür in aller Regel auf ungeschwärzte Unterlagen angewiesen. Der Allgemeinheit werden diese Daten dagegen nach § 13 Satz 1 BbgKVerf zur Information über Gemeindeangelegenheiten überlassen. Der Fokus liegt hier auf der Transparenz und der Nachvollziehbarkeit des gemeindlichen Handelns. Personenbezogene Daten dürfen solche Unterlagen nur enthalten, wenn sie zur Erreichung dieser Zwecke unbedingt erforderlich sind.

Hieran ändert auch der Umstand nichts, dass mit der Entscheidung, Tagesordnungspunkte überhaupt in öffentlicher Sitzung zu behandeln, bereits eine gewisse Bewertung des Schutzbedarfs der verarbeiteten Daten getroffen wurde. Es macht in diesem Zusammenhang einen Unterschied, ob beispielsweise die Anlagen zu Beschlussvorlagen eingesehen werden oder ob Zuschauerinnen und Zuschauer lediglich die Diskussion der öffentlichen Sitzung verfolgen. Schließlich kann das Lesen personenbezogener Unterlagen wesentlich eingriffintensiver als die bloße Beobachtung entsprechender Diskussionen sein. Gleichzeitig ist es nicht zuletzt wegen der damit verbundenen

Gefährdung der Wirksamkeit von Beschlüssen kein gangbarer Weg, Tagesordnungspunkte nur wegen der Pflicht zur Veröffentlichung von Sitzungsunterlagen in den nicht öffentlichen Sitzungsteil zu verlegen.

Nach alledem besteht eine Pflicht der Kommunen, zwischen der Bereitstellung von Sitzungsunterlagen für Mitglieder der Gemeindevertretung einerseits und für interessierte Bürgerinnen und Bürger andererseits zu differenzieren. Im letztgenannten Fall sind personenbezogene Daten zu schwärzen oder anderweitig zurückzuhalten, die nicht zwingend zum Verständnis eines Beschlusses erforderlich sind.

Ziel des uns übersandten Gesetzentwurfs war ursprünglich nur, für die Veröffentlichung von Sitzungsunterlagen die elektronische Form vorzuschreiben. Diese sollte auf der Website der jeweiligen Kommune erfolgen. Hiergegen hatten wir keinerlei Einwände. Nach der Gesetzesbegründung sollten personenbezogene Daten in Beschlussvorlagen grundsätzlich anonymisiert werden, außer „wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der betroffenen Person beeinträchtigt werden.“

Ratsinformationen datenschutzgerecht bereitstellen

In unserer Stellungnahme setzten wir uns dafür ein, die Passage der Begründung aufgrund ihrer oben skizzierten praktischen Bedeutung in den Normtext selbst zu verlegen. Dem konnte das Ministerium auch folgen. Sodann schlugen wir weitere Änderungen der Normstruktur mit dem Ziel vor, die Veröffentlichung personenbezogener Daten klarer zu regeln. Ausnahmen von der Anonymisierung sollen danach nur noch erfolgen, wenn ohne sie die Verständlichkeit der Beschlussvorlage nicht mehr gegeben ist. Auch diesem Vorschlag folgte das Ministerium. Der Gesetzentwurf in der zum Ende des Berichtszeitraums vorliegenden Fassung²⁶ sieht vor, dass Beschlussvorlagen grundsätzlich zu anonymisieren sind, es sei denn, dass die personenbezogenen Daten zu deren Verständnis erforderlich sind und durch die Veröffentlichung schutzwürdige Belange der betroffenen Personen nicht beeinträchtigt werden.

26 Entwurf der Landesregierung für ein Gesetz zur Modernisierung des Kommunalrechts, Landtags-Drucksache 7/7839 vom 7. Juni 2023.



Aus unserer Sicht besteht mit dem Gesetzentwurf die Chance, eine Veröffentlichungspraxis von Beschlussvorlagen nebst Anlagen in Ratsinformationssystemen einzuführen, durch die Bürgerinnen und Bürger gleichzeitig umfassend informiert und die Rechte aller betroffenen Personen gewahrt werden.

5 Kinder- und Jugendgesundheitsdienst-Verordnung

Im Mai 2023 erhielten wir Gelegenheit, gegenüber dem Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz eine Stellungnahme zur geplanten Änderung der Kinder- und Jugendgesundheitsdienst-Verordnung abzugeben. Die Verordnung trifft nähere Bestimmungen zu Untersuchungen für Kinder und Jugendliche, die das Brandenburgische Gesundheitsdienstgesetz den Kommunen aufgibt, z. B. liefert sie hierfür standardisierte Dokumentations- und Fragebögen. Wir stellten fest, dass Empfehlungen zu diesen Unterlagen, die wir bereits im Jahr 2014 abgegeben hatten, nunmehr weitgehend aufgegriffen wurden. Zu den aktuellen Änderungen hatten wir folgende Anmerkungen:

Die Schuleingangsuntersuchung ist eine staatliche Pflichtuntersuchung. Sie dient ausschließlich dazu, die gesundheitliche Schulfähigkeit des Kindes festzustellen. Weitergehende Zwecke, wie z. B. die kommunale Gesundheitsberichterstattung, sind von den schulrechtlichen Vorschriften nicht gedeckt. Das durch das Ministerium zur Verfügung gestellte Elternanschreiben zur Information über die Schuleingangsuntersuchung sah vor, dass entsprechende Fragen freiwillig beantwortet werden konnten. Wir wiesen auf die schulrechtlichen Regelungen hin, nach denen Fragen zur Persönlichkeitssphäre, auch der Eltern und sonstiger nahestehender Personen, die über den Zweck der Feststellung der Schulreife hinausgehen, bei der Schuleingangsuntersuchung nicht gestellt werden dürfen. Eine Einwilligungslösung ermöglicht das Gesetz hier gerade nicht.

Kindergesundheit auf dem Prüfstand

Zudem haben wir empfohlen, die Informationen für die Datenverarbeitung gemäß Artikel 13 und 14 Datenschutz-Grundverordnung, die dem Elternanschreiben beigefügt werden sollten, in einigen Punkten zu überarbeiten. Dies betraf z. B. Zwecke der Datenverarbeitung, Kategorien personenbezogener Daten und Quellen von Datenübermittlungen.

Der ärztliche Dokumentationsbogen für Kinder und Jugendliche (Anlage 1 der Verordnung) dient der Darstellung der Ergebnisse von

Untersuchungen u. a. in der Kita oder für die Schulaufnahme. Wir wiesen darauf hin, dass gemäß § 4 Absatz 5 Grundschulverordnung bereits aus einer Kita-Untersuchung vorliegende Testergebnisse bei einer Schuleingangsuntersuchung nur mit Zustimmung der Eltern verwendet werden dürfen. Der vorgegebene Bogen ließ nicht erkennen, dass diesem Erfordernis Rechnung getragen wurde.

Für Kita-Untersuchungen und Schuleingangsuntersuchungen ist ein sogenannter Elternfragebogen vorgesehen. Die im Verordnungsentwurf einheitlich vorgegebene Fassung (Anlage 2 der Verordnung) differenzierte nicht zwischen diesen Untersuchungen. Wir verdeutlichten, dass für die im Gegensatz zur Schuleingangsuntersuchung freiwillige Untersuchung in der Kita ein gesonderter Elternfragebogen zu verwenden ist. Diesem muss ein Hinweis auf die Freiwilligkeit der Angaben vorangestellt werden. Der bisher vorgesehene einheitliche Fragebogen für beide Zwecke ist deshalb ungeeignet.

Hinsichtlich der Einschätzung der gesundheitlichen Schulfähigkeit bezweifelten wir die Erforderlichkeit einzelner Fragen. Hierzu zählten:

- die spezifische Angabe eines Sozialpädiatrischen Zentrums als unterstützende Institution mit Name und Ort,
- Krankenhausbehandlungen, die sich nicht aktuell auf die Fähigkeit, am Schulunterricht teilzunehmen, auswirken,
- Verletzungen nach einem Unfall, die keine Beschwerden mehr nach sich ziehen,
- der Unfallort.

Wir haben vorgeschlagen, diese Fragen in den Teil des Elternfragebogens zur Gesundheitsberichterstattung im Rahmen der Kita-Untersuchung zu übernehmen. Auch hierzu hatten wir kritische Anmerkungen. Diese betrafen z. B. Fragen zu:

- dem Medienkonsum des Kindes,
- den Stillgepflogenheiten und der Stillfähigkeit der Mutter,
- der Dauer des Besuchs der Kindertagespflege bzw. Kindertagesstätte,
- dem Geburtsland, der Staatsangehörigkeit, den gesprochenen Sprachen, den Schulabschlüssen, der Berufsausbildung und der Erwerbstätigkeit der Eltern.

Durchgängig ist eine anonyme Übermittlung der Daten im Rahmen der Gesundheitsberichterstattung sicherzustellen. Schließlich handelt es sich hier um eine Aufgabe der Gesundheitsvorsorge, durch die gesundheitliche Risiken identifiziert und Schwerpunkte für gesundheitspolitische Entscheidungsprozesse abgeleitet werden sollen.

Letztlich kritisierten wir auch die Formulierung in der Einwilligungserklärung, einzelne Fragen auch während des Arztgespräches beantworten zu können, und forderten deren Streichung. Die zusätzlichen, allein für die Gesundheitsberichterstattung erhobenen Daten haben gerade nichts mit den für die Beurteilung der Gesundheit des Kindes notwendigen Fragen im Arztgespräch zu tun.

Ähnliche Anmerkungen hatten wir auch zu dem separaten Elternfragebogen für die Jahrgangsstufen 6 und 10 (Anlage 3 der Verordnung).

Ob unsere Kritik berücksichtigt wird, war zum Zeitpunkt des Redaktionsschlusses dieses Berichts noch offen.

6 18. Jahrestreffen mit den behördlichen Datenschutzbeauftragten

Nach der pandemiebedingten Pause konnten wir im Berichtszeitraum die behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Städte und Gemeinden wieder zu einer ganztägigen Beratung einladen. Angesichts der unzulänglichen Raumkapazitäten auf unserer Liegenschaft in Kleinmachnow stellte uns das Ministerium des Innern und für Kommunales freundlicherweise einen Sitzungsraum in Potsdam zur Verfügung.

Zweck des Jahrestreffens ist ein informeller und kritischer Wissens- und Erfahrungsaustausch. Die Themen werden grundsätzlich von den behördlichen Datenschutzbeauftragten eingebracht. Während der Veranstaltung referieren Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten unsere Auffassung zu rechtlichen und technisch-organisatorischen Aspekten. In der anschließenden Diskussion werden noch offene Fragen angesprochen und Lösungen aus dem Arbeitsalltag der beteiligten Behörden erörtert. Dies soll den Datenschutzbeauftragten beispielsweise ermöglichen, die Einführung datenschutzrelevanter Projekte in den Kommunen bereits frühzeitig und effektiv zu begleiten.

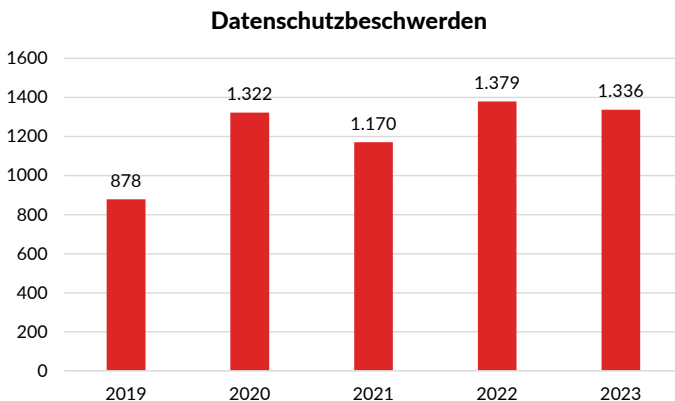
Inhaltliche Schwerpunkte der diesjährigen Beratung waren u. a. die datenschutzrechtlichen Anforderungen bei dem behördlichen Einsatz von IT-Systemen mit Künstlicher Intelligenz, der Schutz personenbezogener Daten bei der E-Mail-Kommunikation und die Umsetzung von Projekten auf der Grundlage des Onlinezugangsgesetzes. Auch standen die E-Akte bzw. die digitale Personalakte, die Datenübermittlung in Drittstaaten sowie die Nutzung sozialer Medien und ein Bericht zum Sachstand des elektronischen Wohngeldverfahrens „eWoG“ auf der Tagesordnung.

Die Wiederaufnahme des Jahrestreffens hat gezeigt, dass ein regelmäßiger Austausch zwischen den kommunalen Datenschutzbeauftragten und unserer Dienststelle von großem beiderseitigen Nutzen ist.

VI Zahlen und Fakten

1 Beschwerden

Im Berichtszeitraum gingen bei der Landesbeauftragten 1.336 schriftliche Beschwerden gemäß Artikel 77 Datenschutz-Grundverordnung ein. Damit hat sich die Anzahl gegenüber dem Vorjahr nur leicht verringert und bleibt weiterhin auf hohem Niveau. Die Beschwerden wurden von Personen eingereicht, die der Ansicht waren, dass die Verarbeitung ihrer personenbezogenen Daten sie in ihren Rechten verletzt und gegen das Datenschutzrecht verstößt.



2 Beratungen

Neben der Bearbeitung von Beschwerden berät die Landesbeauftragte auch zu Datenschutzfragen. Im Berichtsjahr unterstützte sie betroffene Personen, Verantwortliche im öffentlichen und nicht öffentlichen Bereich sowie die Landesregierung bei Rechtssetzungsverfahren in insgesamt 324 Fällen durch schriftliche Stellungnahmen, Hinweise und Anmerkungen. Hinzu kommt eine Vielzahl telefonischer Beratungen, die nicht statistisch erfasst werden.

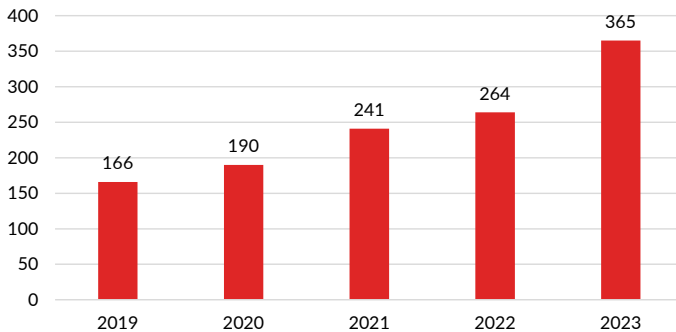
3 Videoüberwachung: Beschwerden und Beratungen

Im Berichtszeitraum wandten sich erneut zahlreiche Bürgerinnen und Bürger an die Landesbeauftragte, um Videoüberwachungen aus datenschutzrechtlicher Sicht überprüfen zu lassen. Meist schilderten die beschwerdeführenden Personen, dass sie sich auf dem eigenen Grundstück bzw. im öffentlichen Straßenland durch Videokameras der Nachbarschaft beobachtet fühlten. Darüber hinaus sahen sich Mieterinnen und Mieter erheblich in ihrem Persönlichkeitsrecht verletzt, wenn Feriengrundstücke, Ferienhäuser und Mehrfamilienhäuser mit einer Vielzahl von Kameras ausgestattet waren. Auch beschwerten sich Beschäftigte bei uns darüber, dass die Arbeitgeberin oder der Arbeitgeber sie während der Arbeit und sogar in der Pause filmte. Weitere Schwerpunkte waren die datenschutzrechtliche Überprüfung von Videokameras in Fitnessstudios, Unternehmen, Restaurants sowie in Pflegeeinrichtungen und Arztpraxen. Insgesamt konnten wir eine deutliche Zunahme an Beschwerden über Videoüberwachungen, ob im Privaten, in der Freizeit, am Arbeitsplatz oder in Kundenbereichen, verzeichnen.

In aller Regel eröffnen wir nach Eingang der Beschwerde ein Verwaltungsverfahren, in dem wir der verantwortlichen Kamerabetreiberin bzw. dem verantwortlichen Kamerabetreiber den Gegenstand der Beschwerde mitteilen und Gelegenheit geben, zum geschilderten Sachverhalt Stellung zu nehmen. Dies kann beschwerdeführenden Personen zwar langwierig erscheinen, allerdings müssen in einem Verwaltungsverfahren auch die Argumente der Gegenseite gehört und Fristen eingehalten werden. Wirken die Verantwortlichen nicht mit, können sie verpflichtet werden, uns die notwendigen Auskünfte zu erteilen. Stellen wir im Verlauf des Verfahrens fest, dass die Videoüberwachung gegen Datenschutzvorschriften verstößt, kann als Abhilfemaßnahme z. B. die Datenverarbeitung untersagt oder ihre Einschränkung angeordnet werden. Zur Durchsetzung kommt auch die Anwendung von Verwaltungszwang in Betracht. Bisher haben wir aber die Erfahrung gemacht, dass der überwiegende Teil der Verantwortlichen daran interessiert ist, die Videoüberwachungsanlage datenschutzgerecht zu betreiben.

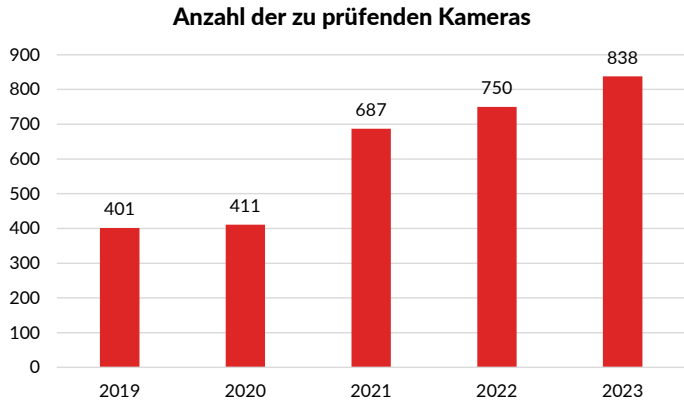
Zudem wandten sich zahlreiche öffentliche und nicht öffentliche Stellen mit der Frage an uns, ob die von ihnen vorgesehene Videoüberwachung zulässig wäre. So befassten wir uns beispielsweise mit geplanten Kameras an Schulen, in Freizeiteinrichtungen und Wäldern sowie für Fahrradabstellanlagen vor Bahnhöfen.

Beschwerden und Beratungen zur Videoüberwachung



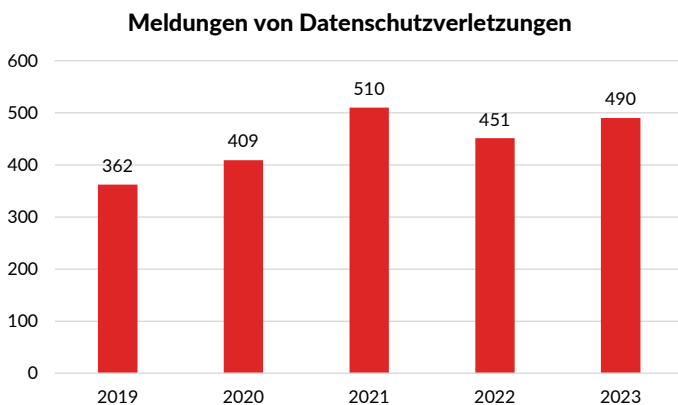
Im Berichtsjahr erfassten wir 322 Beschwerden, im Jahr zuvor waren es 247. Damit hat sich die Gesamtanzahl seit der Einführung der Datenschutz-Grundverordnung kontinuierlich erhöht. Auch der Beratungsbedarf ist signifikant gestiegen – nach 17 Fällen im Vorjahr haben wir im Jahr 2023 zum Thema Videoüberwachung insgesamt 43 Beratungen durchgeführt. Die zahlreichen telefonischen Auskünfte haben wir nicht statistisch erfasst.

Da die datenschutzrechtliche Bewertung einer Videoüberwachung stets eine Einzelfallprüfung erforderlich macht, ist jede Kamera gesondert auf ihre rechtliche Zulässigkeit sowie ggf. auf die Umsetzung technisch-organisatorischer Maßnahmen zu kontrollieren. Im Berichtsjahr überprüften wir 838 Kameras, im Jahr zuvor waren es 750. Auch in dieser Hinsicht ist ein deutlicher Zuwachs unserer Aktivitäten zu erkennen.

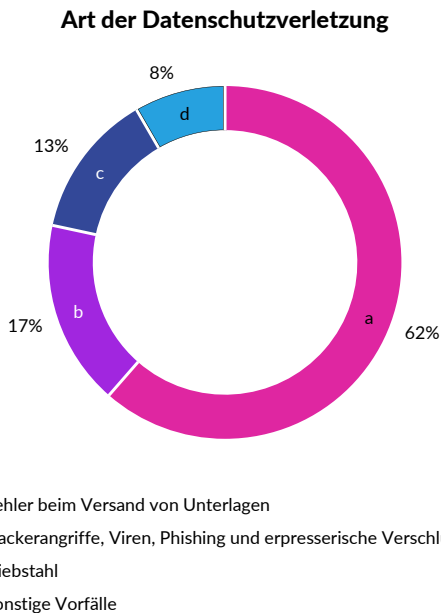


4 Meldungen von Datenschutzverletzungen

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 490 Meldungen von Datenschutzverletzungen. Das bedeutet eine Steigerung gegenüber dem Vorjahr, in welchem 451 Meldungen eingingen. Die Datenschutzverletzungen passierten sowohl im öffentlichen (231 Meldungen) als auch im nicht öffentlichen Bereich (259 Meldungen). Beachtlich ist, dass sich die Zahl der Meldungen durch öffentliche Stellen überproportional – um ca. 30 % – erhöhte.



Deutlich mehr als die Hälfte aller Meldungen betraf den Fehlversand von Unterlagen (insgesamt 301 Fälle). Hiervon umfasst sind Fehlkuvertierungen von Briefpost, versehentlicher E-Mail-Versand an einen offenen Verteilerkreis, Namensverwechslungen oder die Beifügung von Unterlagen unbeteiligter Dritter.

Einen im Vergleich zum Vorjahr geringeren Anteil der Meldungen (83) machten Datenschutzverletzungen aus, die auf technischen Mängeln beruhten und insofern Virenbefall, Phishing, Hackerangriffe, unberechtigte Zugriffe Dritter und erpresserische Verschlüsselungen von Datensätzen ermöglichten.

Ein Abhandenkommen physischer Datenträger, etwa durch Diebstähle aus Räumen des Verantwortlichen oder durch Verlust auf dem Postweg, wurde der Landesbeauftragten in 65 Fällen gemeldet. Dies bedeutet einen besorgniserregenden Anstieg um über 100 %.

Eine bunte Mischung aus 41 Datenschutzverletzungen fällt in die Kategorie „Sonstiges“. Hier finden sich so unterschiedliche Fälle wie

die Übersendung von Kontoauszügen via WhatsApp durch einen Verein, die Veröffentlichung des Videomitschnitts aus Sitzungen von Stadtverordnetenversammlungen ohne Einwilligung oder die Videoaufzeichnung einer universitären Lehrveranstaltung ohne Rechtsgrundlage.

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 fehlerhafter Briefpost zu erklären. Hohe Betroffenenzahlen ergaben sich dagegen etwa bei erfolgreichen Hackerangriffen, in deren Verlauf Datenbestände verschlüsselt und so dem Zugriff der eigentlich Befugten entzogen wurden, oder auch bei der unbeabsichtigten Verwendung eines umfangreichen offenen E-Mail-Verteilers.

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 zum 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, 11 Verwarnungen und 3 Anordnungen aus. Hinzu kommen die im folgenden Abschnitt behandelten Bußgeldverfahren.

5.2 Geldbußen

Im Berichtszeitraum wurden der Bußgeldstelle der Landesbeauftragten insgesamt 47 Sachverhalte wegen Verstößen gegen datenschutzrechtliche Vorgaben zur Kenntnis gegeben. Die Verfahren wurden zu einem großen Teil, nämlich in 41 Fällen, von den zuständigen Polizeibehörden oder Staatsanwaltschaften an die Bußgeldstelle weitergeleitet. Insgesamt 6 Sachverhalte haben aufsichtsbehördlich tätige Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten oder andere Aufsichtsbehörden mangels eigener Zuständigkeit an die Bußgeldstelle abgegeben.

57 Verfahren, die sich sowohl gegen nicht öffentliche Stellen als auch gegen Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen richteten, hat die Bußgeldstelle im Berichtszeitraum abgeschlossen. Etwas weniger als die Hälfte der abgeschlossenen Verfahren war im Vorjahr eröffnet worden.

In 10 Fällen verhängte die Landesbeauftragte wegen der festgestellten datenschutzrechtlichen Verstöße ein Bußgeld. Die Gesamtsumme der festgesetzten Bußgelder betrug knapp 13.900 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 in Fällen grenzüberschreitender Datenverarbeitung eine europaweite Zusammenarbeit der Datenschutzaufsichtsbehörden erfolgen muss. Eine solche grenzüberschreitende Verarbeitung liegt z. B. dann vor, wenn der Verantwortliche personenbezogene Daten von betroffenen Personen aus mehreren Mitgliedstaaten verarbeitet oder verarbeiten lässt. Um die Zusammenarbeit der EU-Behörden zu erleichtern, erfolgt der gegenseitige Austausch elektronisch über das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission.

Im Berichtszeitraum erhielt die Landesbeauftragte insgesamt 1.678 einzelne Benachrichtigungen aus dem Binnenmarkt-Informationssystem, für die sie das Ergreifen von Maßnahmen zu prüfen hatte.

Von allen eingegangenen Benachrichtigungen prüften wir gemäß Artikel 56 DS-GVO in 667 Fällen, die von anderen europäischen Aufsichtsbehörden gemeldet wurden, ob eine Zuständigkeit der Landesbeauftragten als federführende oder betroffene Aufsichtsbehörde in Betracht kommt und entsprechende Verfahrensschritte ergriffen werden müssen. In 12 Fällen initiierten wir aufgrund uns vorliegender Beschwerden selbst ein Verfahren gemäß Artikel 56 DS-GVO. Die Federführung orientiert sich dabei an der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen in der EU. Eine Betroffenheit ist demgegenüber dann gegeben, 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 3 Fällen festgestellt. Bei 51 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 967 Fällen beteiligten wir uns an Verfahren der Zusammenarbeit und Kohärenz, etwa im Rahmen gegenseitiger Amtshilfe, bei der Vorbereitung einer Stellungnahme des Europäischen Datenschutzausschusses oder durch Prüfung, ob die Landesbeauftragte einen Einspruch gegen die Entscheidung einer federführenden Aufsichtsbehörde einlegen möchte.

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

Im Berichtsjahr gingen 43 Beschwerden gegen PayPal bei der Landesbeauftragten ein; wir haben sie zum Teil selbst bearbeitet, zum Teil an die CNPD weitergeleitet. Im Vergleich zum Vorjahr war die Zahl solcher Beschwerden damit deutlich geringer. In 23 Verfahren haben wir gegenseitige Amtshilfe gemäß Artikel 61 DS-GVO geleistet – jedem Verfahren lagen bis zu 5 Beschwerden zugrunde.

7 Förmliche Begleitung von Rechtsetzungsvorhaben

Aus den zahlreichen Beratungen ist die Begleitung rechtsetzender Maßnahmen durch die Landesbeauftragte besonders hervorzuheben. Insgesamt nahmen wir im Berichtszeitraum 40 Mal zu Gesetzen, Verordnungen, Satzungen oder Verwaltungsvorschriften Stellung.

Die rechtliche Grundlage zur Beteiligung der Landesbeauftragten folgt aus § 18 Absatz 5 Satz 1 Brandenburgisches Datenschutzgesetz. Danach ist 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	Gesetz zur Verhinderung von Gewalt gegen Frauen und häuslicher Gewalt	121
2	Digitalisierungsprojekte bei der Polizei	127
3	Lernplattform zur Sensibilisierung für Datenschutz	129
4	Kontrolle personengebundener und ermittlungsunterstützender Hinweise in Kriminalakten	130
5	Geschwindigkeitsübertretung: Abruf personenbezogener Daten aus der Elektronischen Einwohnerakte	134
6	Zahlen und Fakten	136

1 Gesetz zur Verhinderung von Gewalt gegen Frauen und häuslicher Gewalt

Bereits im Jahr 2022 wurde die Landesbeauftragte durch das Ministerium des Innern und für Kommunales an der Abstimmung von Entwürfen zu einer umfangreichen Änderung des Brandenburgischen Polizeigesetzes beteiligt. Das Ministerium sah sich aufgrund verschiedener Umsetzungsgesetze des Bundes²⁷ zu europäischen Übereinkommen verpflichtet, ein Gesetz zur Verhinderung von Gewalt gegen Frauen und häuslicher Gewalt einzubringen, um bestehende Defizite zu beseitigen und Lösungen für einen verbesserten Schutz der Betroffenen zu schaffen. Die sogenannte Istanbul-Konvention²⁸ stellt fest, dass Gewalt gegen Frauen als geschlechtsspezifische Gewalt strukturellen Charakter hat und häusliche Gewalt Frauen unverhältnismäßig stark betrifft. Um eine ganzheitliche Antwort auf diese Gewalt zu geben, haben sich die Vertragsparteien neben einer Verständigung auf koordinierte politische Maßnahmen auch verpflichtet, durch gesetzgeberische und sonstige Maßnahmen ihrer Sorgfaltspflicht zur Verhütung, Untersuchung und Bestrafung dieser Gewalttaten besser nachzukommen. Der zur Erfüllung dieses Auftrags im Berichtszeitraum vorgelegte Gesetzentwurf der Landesregierung²⁹ enthält in Artikel 1 Änderungen des Brandenburgischen Polizeigesetzes (BbgPolG-E), die bestehende polizeiliche Befugnisse täterbezogen an die festgestellte Situation anpassen sollen und neue Maßnahmen vorsehen. Die Landesbeauftragte hat dazu erneut Stellung genommen und im Rahmen einer Anhörung des Ausschus-

Umsetzung der Istanbul-Konvention

-
- 27 Gesetz zum Übereinkommen des Europarats vom 11. Mai 2011 zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt vom 17. Juli 2017 (BGBl. 2017 II S. 1026).
- 28 Übereinkommen des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt vom 11. Mai 2011, Europarat, CETS No. 210, <https://rm.coe.int/16806b076a>.
- 29 Entwurf der Landesregierung für ein Gesetz zur Verhinderung von Gewalt gegen Frauen und häuslicher Gewalt, Landtags-Drucksache 7/7349 vom 8. März 2023.

ses für Inneres und Kommunales des Landtages Brandenburg ihre Position erläutert.

Aus datenschutzrechtlicher Sicht bedeutsam ist die mit dem Gesetzentwurf neu eingeführte, umfangreiche und sehr ausdifferenzierte Regelung der elektronischen Aufenthaltsüberwachung in § 15b BbgPolG-E. Danach soll eine Person von der Polizei verpflichtet werden können, ein technisches Sendegerät (Tracker – eine „elektronische Fußfessel“) am Körper zu tragen, mit dem ihr Aufenthaltsort permanent festgestellt und die Standortdaten an eine Überwachungsstelle übermittelt und gespeichert werden können. Die elektronische Aufenthaltsüberwachung soll für unterschiedliche präventive Zwecke durchgeführt werden. Zusammengefasst erlaubt die Ermächtigungsgrundlage die Datenverarbeitung gemäß § 15b Absatz 1 BbgPolG-E

- bei sogenannten „Hochrisikofällen“, wenn eine Person nach polizeilichen Erkenntnissen bereits schwere Gewalttaten oder Straftaten gegen die sexuelle Selbstbestimmung begangen hat und aufgrund des Tatverhaltens, der individuellen Verhaltensweise sowie der Lebensumstände die Prognose getroffen wird, dass eine wesentlich erhöhte Wahrscheinlichkeit besteht, dass die Person künftig wieder Gewalt- oder Sexualstraftaten begehen könnte (Gefährlichkeitsprognose im Einzelfall), und eine hinreichend konkretisierte Gefahrenlage vorliegt. Letzteres bedeutet, dass der Verdacht ausreicht, die Person werde innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat an einer ihr fremden Person begehen. Die Überwachung muss für diesen Zweck auch unerlässlich sein.
- wenn eine Person nach polizeilichen Erkenntnissen bereits einen besonders schweren Fall einer Nachstellung begangen hat, Tatsachen für die erneute Begehung einer solchen auch im Einzelfall schwerwiegenden Straftat sprechen, die in absehbarer Zeit von der betroffenen Person begangen werden könnte, und andere Maßnahmen nicht erfolgversprechend erscheinen oder
- zur Feststellung von Verstößen gegen ein Rückkehrverbot nach einer Wohnungsverweisung gemäß § 16a BbgPolG oder zur Kontrolle eines Kontakt- und Näherungsverbots gemäß § 16b BbgPolG-E zum Schutz einer gefährdeten Person.

Die elektronische Aufenthaltsüberwachung darf nur auf richterliche Anordnung erfolgen, kann bei Gefahr im Verzug jedoch zunächst auch von der Leiterin oder dem Leiter der jeweiligen Polizeibehörde für bis zu drei Tage angeordnet werden.

Zweck der Maßnahme ist eine bessere Kontrolle gewalttätiger Personen anstelle der für sie invasiveren und für die Polizei personalintensiven verdeckten Observation oder „offenen Begleitung“. Die übermittelten Standortdaten sollen es der Polizei ermöglichen, einen Interventionsbedarf zu erkennen und rechtzeitig erforderliche Maßnahmen zur Verhinderung einer Gewalttat zu veranlassen.

Die Landesbeauftragte hat hinsichtlich dieser Regelung erhebliche Bedenken geäußert:

Die elektronische Aufenthaltsüberwachung stellt einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung dar, da über den Tracker ständig automatisiert Daten zum Aufenthaltsort der betroffenen Person erhoben, übermittelt und gespeichert werden. Die lückenlose Nachverfolgung des Standorts ermöglicht das Erstellen eines vollständigen Bewegungsprofils. Nur wenn diese Maßnahme für den Zweck des präventiven Schutzes vor Taten gegen die sexuelle Selbstbestimmung und Gewalttaten geeignet, erforderlich und verhältnismäßig wäre, ließe sich dieser Eingriff in das Recht auf informationelle Selbstbestimmung rechtfertigen.

Aus unserer Sicht bestehen bereits deutliche Zweifel, ob die elektronische Aufenthaltsüberwachung in der Praxis einen Abschreckungseffekt bei als gefährlich eingestuften Personen hat und damit überhaupt ein taugliches Mittel für die präventive Nutzung ist, sich also eignet, Gewalt- und Sexualstraftaten zu verhindern. Für die Behauptung, dass dies so sei, liegen bisher kaum ausgewertete Erfahrungen vor. Die elektronische Aufenthaltsüberwachung wird zwar seit 2011 eingesetzt, aber ausschließlich als richterliche Weisung im Rahmen der Führungsaufsicht für bereits verurteilte Straftäter (gemäß § 68b Absatz 1 Nummer 12 Strafgesetzbuch). Dennoch sind Fälle bekannt geworden, in denen ein vorbestrafter Straftäter trotz „Fußfessel“ erneut ein einschlägiges Delikt begangen hat. Das Bundesverfassungsgericht hat im Jahr 2020 die Maßnahme zwar für verurteilte Straftäter zugelassen, jedoch eingeräumt, dass es bisher keine empirischen Nachweise dafür gibt, dass die elektronische Aufenthaltsüberwachung bei diesem Personenkreis das Risiko erneuter Straffälligkeit



wirksam mindert. Vor wenigen Jahren führten einige Länder diese Maßnahme auch in ihre Polizeigesetze ein.³⁰ Sofern es zu der präventiven Nutzung in diesen Ländern Evaluierungen zur Wirksamkeit gegeben hat, wurde in der Gesetzesbegründung der Landesregierung darauf jedenfalls nicht Bezug genommen.

Auch die Unsicherheit der zuständigen polizeilichen Stellen, eine zuverlässige Prognose abzugeben, spricht gegen diese eingriffsintensive Maßnahme. Zum einen, weil nicht in allen Varianten der geplanten Regelungen gerichtlich festgestellte Vortaten vorliegen müssen, sondern polizeiliche Erkenntnisse ausreichend sind. Zum anderen, weil in der Regel – anders als bei der repressiven Verhängung der elektronischen Aufenthaltsüberwachung im Rahmen der Führungsaufsicht – auch keine fachlichen Einschätzungen von Therapeutinnen bzw. Therapeuten oder anderen Sachverständigen zu den betroffenen Personen existieren. Ferner ist anzunehmen, dass die Prognose in deutlich kürzeren Zeiträumen als bei der repressiven Nutzung erstellt werden muss.

Ungeachtet dieser Zweifel an der Geeignetheit ist ein milderer Mittel für die jederzeitige Bestimmung des Aufenthaltsortes der betroffenen Person nicht ersichtlich. Insbesondere würde die permanente Observation durch Polizeivollzugsbeamtinnen und -beamte im Vergleich zur durchgängigen automatisierten Erhebung der Aufenthaltsdaten einen stärkeren Eingriff in das Persönlichkeitsrecht darstellen. Insoweit würden wir die Erforderlichkeit der Maßnahme bejahen.

Eine wesentliche Kritik der Landesbeauftragten richtete sich darauf, dass bei bestimmten Anwendungsvarianten als Voraussetzung des Einsatzes eine nur hinreichend „konkretisierte Gefahr“ vorliegen muss. Der im Polizeiabwehrrecht übliche Begriff einer „konkreten Gefahr“ wird dadurch herabgestuft und erlaubt einen vorverlagerten Eingriff bereits dann, wenn innerhalb eines „übersehbaren Zeitraums“ eine Tatbegehung „auf zumindest ihrer Art nach konkretisierte Weise“ angenommen wird. Diese, weit ins Vorfeld der eigentlichen Gefahr reichende, vom Bundesverfassungsgericht zum Schutz herausgehobener Rechtsgüter für Kriminalitätsphänomene des

30 Z. B. Artikel 34 Bayerisches Polizeiaufgabengesetz sowie § 34c Polizeigesetz Nordrhein-Westfalen, beide geändert im Jahr 2018.

Terrorismus entwickelte eingriffsbegründende Gefahrenlage sollte nach unserer Auffassung nicht für die präventive Anordnung einer elektronischen Aufenthaltsüberwachung herangezogen werden. Die Tatsache, dass das Bundesverfassungsgericht diese Gefahrenschwelle auch in einem Beschwerdefall für rechtmäßig hielt, in dem die elektronische Aufenthaltsüberwachung für einen wegen Mordes und schwerer Sexualstraftaten verurteilten Täter mit dokumentiertem schwierigen Vollzugsverhalten angewendet wurde, erlaubt keine andere Bewertung. Die Unterschiede zwischen den Zielgruppen der präventiven und repressiven elektronischen Aufenthaltsüberwachung sind erheblich – also bereits bestrafte Täter betreffend. Da die Maßnahme tief in das Persönlichkeitsrecht eingreift, ist sie unter der Voraussetzung einer zusätzlich abgesenkten Gefahrenschwelle in Kombination mit den oben erwähnten Schwierigkeiten, eine zutreffende Prognoseentscheidung für eine betroffene Person zu stellen, im Polizeirecht unverhältnismäßig.

Ferner wiesen wir darauf hin, dass die für eine elektronische Aufenthaltsüberwachung verwendeten sogenannten Home-Units standardmäßig sicherstellen sollten, dass über das Datum der bloßen Anwesenheit in einer Wohneinheit hinaus keine überschießenden Aufenthaltsdaten innerhalb der Wohnung erhoben werden. Sollte eine Überwachung ohne Home-Units mittels GPS-Daten erfolgen, bedürfte es klarer Festlegungen, welches GPS-Datum als Beweis für die Anwesenheit heranzuziehen ist.

Kritisch haben wir uns auch mit der neu eingefügten Regelung zur Übermittlung von Kontaktdaten gefährdeter Personen gemäß § 16a Absatz 4 Satz 3 und 4 BbgPolG-E auseinandergesetzt. In einer konkreten Gefahrensituation für häusliche Gewalt hat die Polizei nach bestehendem Recht die Verpflichtung, im Zuge einer Wohnungsverweisung zur Abwehr von Gefahren für eine andere Person diese auf die Möglichkeit des zivilrechtlichen Schutzes und der Unterstützung durch geeignete Beratungsstellen hinzuweisen. Nun soll die Unterstützung dahingehend erweitert werden, dass die zur Kontaktaufnahme erforderlichen Daten an eine geeignete Beratungsstelle übermittelt werden können, ohne dass die gefährdete Person einwilligen muss oder ein absolutes Widerspruchsrecht hat. Hierbei stützte sich der Entwurf auf eine Regelung des § 13 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz, wonach die Datenübermittlung zulässig ist, wenn die Polizei sie für erforderlich hält. Wir hatten dies zunächst zurückgewiesen, weil die letzte Ent-

scheidung über eine Datenübermittlung bei der gefährdeten Person liegen sollte.

Wir haben unsere Auffassung jedoch geändert. Bei der Anhörung zum Gesetzentwurf im September 2023 erläuterten Expertinnen aus der Praxis, die sich um den Schutz von Frauen in Situationen häuslicher Gewalt kümmern, dass diese vielfach eingeschüchtert und traumatisiert seien. Auch bei entsprechender Kenntnis würden sie Beratungsstellen nicht selbstständig kontaktieren, um Hilfe in Anspruch zu nehmen. Vielmehr sei seitens der Beratungsstellen eine Kontaktaufnahme und aufsuchende, zugewandte Beratung nötig, um Auswege aus der Gewaltsituation zu ermöglichen. Diese Aussagen überzeugten uns, dass die Übermittlung der Kontaktdaten einer gefährdeten Person als Nebenregelung zur polizeilichen Gefahrenabwehrmaßnahme der Wohnungsverweisung zu rechtfertigen ist. Sie lässt sich aus unserer Sicht auf die bestehende Rechtsgrundlage zur Datenübermittlung an private Stellen gemäß § 44 Absatz 1 BbgPolG stützen, wonach die Polizei von sich aus personenbezogene Daten übermitteln darf, soweit dies zur Erfüllung ihrer Aufgaben oder zur Abwehr erheblicher Nachteile für das Gemeinwohl bzw. einer schwerwiegenden Beeinträchtigung der Rechte einer Person erforderlich ist. Ein entgegenstehender Wille der gefährdeten Person ist in diesen Fällen unbeachtlich. Ihr steht es frei, nach einer Kontaktaufnahme jede weitere Beratung oder Begleitung durch die Beratungsstelle abzulehnen.

Gegen Ende des Berichtszeitraums fand die abschließende Beratung des Ausschusses für Inneres und Kommunales des Landtages Brandenburg statt.³¹

31 Das Gesetz zur Verhinderung von Gewalt gegen Frauen und häuslicher Gewalt wurde am 21. Februar 2024 verabschiedet.

2 Digitalisierungsprojekte bei der Polizei

Das Polizeipräsidium des Landes Brandenburg und die Landesbeauftragte stehen in regelmäßigem Kontakt hinsichtlich der verschiedenen Digitalisierungsprojekte der Polizei. Auch im Berichtsjahr fand ein Austausch zur Einführung und Änderung von entsprechenden IT-gestützten Diensten statt.

Die Polizei Brandenburg muss auf dem Weg zu einer digital gut aufgestellten Institution große Herausforderungen bewältigen. So besteht vielfach noch Nachholbedarf hinsichtlich des Einsatzes von Hard- und Software, die dem aktuellen Stand der Technik entspricht. Wenn alte polizeiliche Fachverfahren durch moderne Technologien abgelöst werden, ist es häufig notwendig, die dazugehörenden Geschäftsprozesse zu analysieren und anzupassen. Weiter ist es zwingend erforderlich, Datenschutz- und Informationssicherheitskonzepte so zu entwickeln und umzusetzen, dass sich die technischen Möglichkeiten auf das erforderliche Maß beschränken und die Sicherheit der Datenverarbeitung sowie die Rechte der betroffenen Personen gewährleistet sind. Die Projektarbeit umfasst eine Vielzahl an Aktivitäten, die sinnvoll koordiniert und gesteuert werden müssen. Dies wird durch einen von der Stabsstelle Digitalisierung des Polizeipräsidiiums eingeführten Prozess ermöglicht, der das Anforderungsmanagement von der ersten Bedarfsanmeldung bis zur Freigabe systematisiert und digital über ein Ticket- und Wissensmanagementsystem abbildet.

Wichtige aktuelle Projekte im Bereich Digitalisierung sind beispielsweise die umfassende Transformation der polizeilichen Datenverarbeitung im Rahmen des Programms P20 (ehemals Polizei 2020), die Ausstattung der Beamtinnen und Beamten mit dienstlichen Smartphones, der Einsatz aktueller Technologien wie Bodycams oder die Nutzung von Drohnen zur Abstandsmessung von Kraftfahrzeugen auf Autobahnen. So unterschiedlich diese Vorhaben sind, müssen doch bei jedem einzelnen Projekt datenschutzrechtliche und informationssicherheitstechnische Anforderungen beachtet und umgesetzt werden. Dies erfordert wiederum entsprechende personelle Ressourcen.



Allerdings hat die Polizei ebenso wie viele andere öffentliche Stellen mit einem Personalmangel zu kämpfen – insbesondere in den Bereichen Informationssicherheit und IT-Administration. Dies kann sich in vielerlei Hinsicht negativ auswirken und zu datenschutzrechtlich oder informationssicherheitstechnisch relevanten Vorfällen führen, etwa bei zu großzügigen Zugriffsrechten für Beschäftigte. Auch die nachträgliche Analyse und Aufarbeitung solcher Vorfälle oder die Ableitung geeigneter und angemessener Maßnahmen kann möglicherweise durch fehlende personelle Ressourcen beeinträchtigt sein. So haben wir im Berichtszeitraum feststellen müssen, dass trotz überwiegend großer Bemühungen der Polizei, uns in solchen Fällen einzubeziehen, die angefragten und erforderlichen Informationen zu entsprechenden Sachverhalten nicht immer in befriedigendem Umfang und mit der nötigen Schnelligkeit ermittelt bzw. mitgeteilt wurden.

3 Lernplattform zur Sensibilisierung für Datenschutz

Die komplexen datenschutzrechtlichen Anforderungen umzusetzen, bleibt weiterhin eine große Herausforderung für die Polizei. Ein wichtiger Ansatzpunkt ist die möglichst flächendeckende Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter. Das Polizeipräsidium informierte uns in diesem Zusammenhang über die geplante Einrichtung einer eLearning-Anwendung zum Thema „Datenschutz“. Diese Anwendung soll einen starken Praxisbezug aufweisen und die Nutzerinnen und Nutzer beispielsweise mit Sachverhalten konfrontieren, in denen sie bewerten müssen, ob bestimmte Verarbeitungsvorgänge zulässig sind oder nicht. Wir begrüßen das Vorhaben sehr und haben dem Polizeipräsidium eine große Auswahl an praxisrelevanten Fallbeispielen zur Verfügung gestellt, die aus der bußgeldrechtlichen Praxis des Justiziariats unserer Dienststelle stammen. Hierzu gehören insbesondere Fälle, in denen Polizeibeamtinnen und -beamte zu privaten Zwecken und damit ohne dienstlichen Anlass Daten zu Personen oder Kfz-Kennzeichen in polizeilichen Auskunftssystemen abgefragt sowie in einigen Fällen diese Informationen an Dritte weitergegeben haben. Dadurch verstießen sie gegen das Datenschutzrecht.

Eine missbräuchliche Verwendung von polizeilichen Auskunftssystemen und die in diesem Zusammenhang begangenen Datenschutzverstöße durch Beamtinnen und Beamte der Polizei sind in hohem Maß geeignet, das Vertrauen der Allgemeinheit in die Rechtmäßigkeit des Umgangs mit personenbezogenen Daten durch die damit befassen Stellen zu beeinträchtigen. Auch bloße Unkorrektheiten im Umgang mit personenbezogenen Daten können das Vertrauen der Allgemeinheit in die Verschwiegenheit der entsprechenden Behörden, worauf diese für ihre Arbeit zwingend angewiesen sind, empfindlich schädigen. Ebenso verhält es sich mit dem Ansehen der Polizei als solcher. Daher freuen wir uns, dass das Polizeipräsidium seine Mitarbeiterinnen und Mitarbeiter über eine eLearning-Anwendung für die Einhaltung des Datenschutzrechts zu sensibilisieren beabsichtigt.

4 Kontrolle personengebundener und ermittlungsunterstützender Hinweise in Kriminalakten

Zur Erfüllung ihrer Aufgaben auf dem Gebiet der Strafverfolgung und der Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, führt die Polizei zu einzelnen Personen „Kriminalpolizeiliche personenbezogene Sammlungen“, auch Kriminalakten genannt. Sie können zu Verdächtigen, Beschuldigten eines Ermittlungsverfahrens oder Verurteilten bestehen, aber auch zu gesuchten, vermissten oder gefährdeten Personen.

Die Akten enthalten fahndungs- oder ermittlungsrelevante Angaben, die die Sachverhaltsaufklärung unterstützen, aber auch Erkenntnisse, die für eine kriminalistische (Sozial-) Prognose oder auch für das taktische Vorgehen und die Eigensicherung der Polizei herangezogen werden können. Durch die ständige Ergänzung mit relevanten Informationen werden die zentral geführten Akten zum „polizeilichen Gedächtnis“ über einzelne Personen. In diese Sammlungen dürfen auch personengebundene Hinweise (PHW) z. B. auf die besondere Gefährlichkeit einer Person oder ermittlungsbezogene Hinweise (EHW) wie z. B. die politische Motivation für eine Tat aufgenommen werden.

Rechtsgrundlage für die Speicherung und Nutzung der kriminalpolizeilichen Sammlungen in Brandenburg ist § 39 Brandenburgisches Polizeigesetz (BbgPolG). Eine Richtlinie des Innenministeriums aus dem Jahr 2006 regelt Details zur Führung kriminalpolizeilicher personenbezogener Sammlungen. Zur Vereinheitlichung der Vergabe der PHW oder EHW bei den Polizeien des Bundes und der Länder hat das Bundeskriminalamt (BKA) Leitfäden in Form von zwei Richtlinien erstellt, die Kriterien für die Vergabe der derzeit 8 PHW und 16 EHW festlegen. Unabhängig von der Kriminalakte wird ein gespeicherter PHW oder EHW bei jedem

**Kein Hinweis
ohne Begründung**

Abruf in polizeilichen Informations- und Auskunftssystemen für alle dazu befugten Beamtinnen und Beamten sichtbar. Es ist daher erforderlich, dass sie sachlich richtig und auf aktuellem Stand sind. Da für die Eintragung eines Hinweises nicht notwendig eine Verurteilung

der oder des Betroffenen vorliegen muss, können sie stigmatisierend wirken und sind deshalb nicht unumstritten.

Gegen Ende des Berichtsjahres führten wir bei der zentralen Kriminalaktenhaltung der Polizeidirektion West in Brandenburg an der Havel eine Stichprobenkontrolle zu ausgewählten personengebundenen und ermittlungsunterstützenden Hinweisen durch. Die Stichprobe wählten wir anhand der von der Polizei speziell für die Prüfung zur Verfügung gestellten Liste aller an einem Stichtag in der Polizeidirektion West gespeicherten Datensätze aus. Geprüft wurden insgesamt 15 Akten mit dem PHW „psychische Verhaltensstörung“ bzw. „Betäubungsmittelkonsument“ sowie dem EHW „politisch motivierte Kriminalität – rechts“, „politisch motivierte Kriminalität – nicht zuzuordnen“ bzw. „Sexualtäter“.

Vor der Vergabe eines PHW bzw. EHW muss in jedem Einzelfall geprüft werden, ob die Voraussetzungen hierfür bei der oder dem Betroffenen erfüllt sind. In der zentralen Kriminalaktenammlung wird der Hinweis in das Merkblatt zur Akte eingetragen, auf dem auch der Zeitpunkt für einen Termin zu notieren ist, an dem die weitere Erforderlichkeit der Speicherung geprüft wird. Auch die begründende Abwägung sollte kurz in der Akte dokumentiert werden.

Bei unserer Stichprobe stellten wir gravierende Dokumentationsmängel fest. In der überwiegenden Anzahl der Fälle enthielten die Kriminalakten keine Abwägungen, die Rückschlüsse auf die Gründe für die Vergabe eines PHW bzw. EHW zuließen. Zwar legte in vielen Fällen die Sachverhaltsschilderung nahe, dass ein vergebener Hinweis damit zusammenhing. Wie die Beamtin bzw. der Beamte den Sachverhalt oder auch Drittinformationen jeweils bewertet hatte, ließ sich jedoch in der Regel aus der Akte nicht nachvollziehen. Im Einzelnen ergab sich Folgendes:

- Beim PHW „psychische Verhaltensstörung“ wurde in drei von vier Fällen auch die BKA-Leitlinie nicht eingehalten, da die danach für eine Vergabe notwendigen Dokumente weder in der Kriminalakte vorhanden waren noch auf ihre Existenz im Aktenrückhalt verwiesen wurde.
- Für den PHW „Betäubungsmittelkonsument“ war das Vergabekriterium, dass von der entsprechenden Person in irgendeiner Form Gefahren für Dritte, insbesondere Polizeibedienstete,

ausgehen müssen, in keinem der Fälle konkret aufgeführt. Es ist aufgrund der Sachverhalte eher anzunehmen, dass der PHW bei regelmäßigem Konsum oder mehrfachen Verstößen gegen das Betäubungsmittelgesetz pauschal angenommen wurde.

- Bei dem EHW „Politisch motivierte Straftat – rechts“ fanden sich in keinem der drei geprüften Fälle Informationen in der Kriminalakte, die eine Vergabe des EHW hätten rechtfertigen können. Da die Sachverhalte jedoch andere Hinweise nahelegten, war eine Fehlerfassung der Personen zu diesem EHW zu vermuten.
- In den drei mit EHW „Sexualtäter“ geprüften Akten lagen in zwei Fällen die Vergabekriterien laut BKA-Leitfaden vor. Sie enthielten auch auf dem Merkblatt zur Akte eine Begründung für die Vergabe. Ein in der Auswahlliste erfasster Altfall enthielt in der Kriminalakte weder eine Dokumentation der Vergabe des EHW noch der Aussonderungsprüfungen.

Positiv stellten wir fest, dass die PHW- und EHW-Aussonderungsprüffristen überwiegend auf den Einzelfall abgestimmt waren und entsprechend der o. g. Richtlinie des Innenministeriums auch von der Regelspeicherzeit abweichende, verkürzte Fristen festgelegt wurden.

Insgesamt ist jedoch festzuhalten, dass in den Kriminalakten keine verlässliche Auskunft zu den Gründen für die Vergabe eines PHW oder EHW aufzufinden war. Die Eintragungen auf dem Merkblatt zu der betroffenen Person waren zudem teils fehler- bzw. lückenhaft. Abwägungen waren nur ausnahmsweise dokumentiert. Ob sich in den Polizeidienststellen vor Ort, in denen der jeweilige Aktenrückhalt aufbewahrt wird, zusätzliche Dokumentationen zu den vergebenen Hinweisen befinden, haben wir bisher nicht überprüft. Wir vertreten jedoch die Auffassung, dass sich die für die Vergabe der PHW bzw. EHW grundlegenden Erwägungen und die Aussonderungsprüffristen klar aus dem Merkblatt einer Kriminalakte ergeben müssen. Dies gilt auch vor dem Hintergrund, dass der Inhalt der Kriminalakte unter bestimmten Voraussetzungen an andere Dienststellen innerhalb der Polizeien des Bundes und der Länder übermittelt werden kann.

Die Ergebnisse unserer Kontrolle haben wir dem Polizeipräsidium mitgeteilt. Wir forderten die Behörde auf, den festgestellten Defizi-

ten in den geprüften Einzelfällen nachzugehen und darüber hinaus Vorsorge zu treffen, dass die Vergabe der PHW und EHW zukünftig eindeutig den Kriterien der Leitfäden entsprechend erfolgt und mit einer kurzen Begründung dokumentiert wird.

5 Geschwindigkeitsübertretung: Abruf personenbezogener Daten aus der Elektronischen Einwohnerakte

Ein Beschwerdeführer machte geltend, dass der Zentraldienst der Polizei seine personenbezogenen Daten im Zusammenhang mit einer Geschwindigkeitsübertretung aus der Elektronischen Einwohnerakte (EWO) des Landesmelderegisters Brandenburg abgerufen und das komplette Ergebnis des Abrufs in der Akte gespeichert hatte. So waren neben seinem Vor- und Nachnamen sowie seiner Wohnadresse auch die alte Wohnanschrift seiner Ehefrau sowie die Angabe, dass der Beschwerdeführer über eine Waffenerlaubnis verfügte, in die Verfassensakte aufgenommen worden. Hiergegen wehrte sich der Beschwerdeführer. Unsere Nachfrage beim Polizeipräsidium des Landes Brandenburg ergab, dass der vom Beschwerdeführer geschilderte Sachverhalt zutreffend war.

Für den Abruf von Einwohnermeldedaten steht berechtigten Bediensteten der Polizei Brandenburg ein Zugang über das Polizeiauskunftssystem (POLAS) zur Verfügung. Bei POLAS handelt es sich um das automatisierte Abrufverfahren der Polizei, das hauptsächlich Recherchen im Zusammenhang mit Strafsachen dient. Das System bietet jedoch auch die Möglichkeit, Auskünfte aus anderen Datenbanken wie dem Zentralen Verkehrsinformationssystem oder der Elektronischen Einwohnerakte einzuholen.

Wie sich herausstellte, ist es aus technischen Gründen nicht möglich, den Datenumfang vor dem Abruf einer Person aus der EWO einzuschränken. Dadurch erhält die bzw. der Bedienstete der Polizei eine komplette Auskunft der darin gespeicherten Daten. Erst nach dem Abruf kann die Polizeibeamtin bzw. der Polizeibeamte die für die Bearbeitung des Sachvorgangs nicht relevanten personenbezogenen Daten abwählen. Nur dieser „bereinigte“ Abruf darf ausgedruckt und zur Akte genommen werden. Aufgrund unseres Hinweises wird mit Einführung des künftigen Vorgangs- und Auskunftssystems der Polizei Brandenburg die Möglichkeit bestehen, vor dem Abruf der Meldedaten der betroffenen Person die Abfrage entsprechend des Abrufgrundes und der für den Sachvorgang relevanten Angaben einzuschränken.

In dem Beschwerdefall war der Ausdruck des kompletten Ergebnisses der EWO-Abfrage und dessen Einbeziehung in den Anlass gebenden Sachvorgang unter dem Gesichtspunkt der Datensparsamkeit für die Bearbeitung einer Straßenverkehrsordnungswidrigkeit nicht erforderlich. Aufgrund des vorliegenden Sachverhalts sensibilisierte das Polizeipräsidium seine Mitarbeiterinnen und Mitarbeiter sowie jene des Zentraldienstes der Polizei für einen datenschutzgerechten Umgang mit den polizeilichen Auskunftssystemen. Darüber hinaus wies es auf die Einhaltung der Anforderungen an die Dokumentation der erlangten Daten hin. Künftig soll dies fester Bestandteil der dienstlichen Belehrung sein.

6 Zahlen und Fakten

Im Berichtszeitraum setzte sich die Tendenz des Vorjahres fort: Insgesamt wandten sich erneut weniger Bürgerinnen und Bürger mit schriftlichen Beschwerden über konkrete Datenschutzverletzungen durch Polizei und Staatsanwaltschaften an uns. Wir verzeichneten 23 Eingaben, die sich – bis auf eine Ausnahme – alle auf die Polizei bezogen. Darüber hinaus meldeten sich Personen häufig telefonisch mit datenschutzrechtlichen Anfragen allgemeiner Art oder ließen sich ihre Rechte, z. B. bei Auskunftersuchen zu gespeicherten Daten, erläutern. Viele wollten auch Abläufe bei der polizeilichen Datenverarbeitung, Speicherfristen, Voraussetzungen für Datenerhebungen und Verfahren bei Polizei und Staatsanwaltschaft klären. Für öffentliche Stellen wurden wir auf Anfrage insgesamt 12 Mal sowohl in rechtlicher Hinsicht als auch bezüglich technisch-organisatorischer Maßnahmen beratend tätig. Hervorzuheben ist auch der regelmäßige Kontakt zu dem für Digitalisierungsprojekte bei der Polizei zuständigen Stab, durch den wir sowohl über einzelne Fachverfahren als auch digitale Sicherheitstechnologien und Langzeitprojekte der Polizei informiert werden.

Zwei Gesetzesvorhaben, die sich mit umfangreichen Änderungen des brandenburgischen Polizeirechts befassen, begleiteten wir beratend und mit Stellungnahmen. Dabei kam es zu einem regen und konstruktiven Austausch mit dem verantwortlichen Referat im Ministerium des Innern und für Kommunales.

Im Berichtszeitraum erhielten wir von den verantwortlichen Stellen der Polizei insgesamt 20 Meldungen über Verletzungen der Sicherheit personenbezogener Daten gemäß § 29 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz. Zwei davon stufen wir als so gravierend ein, dass weitergehende Nachforschungen erforderlich waren. Sie dauerten zum Redaktionsschluss dieses Berichts noch an.

Die Landesbeauftragte hat gegenüber Polizei und Staatsanwaltschaften im Berichtszeitraum weder Warnungen oder Beanstandungen nach dem Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz ausgesprochen noch von ihren

Abhilfebefugnissen gemäß der Datenschutz-Grundverordnung Gebrauch gemacht.





Die Dienststelle

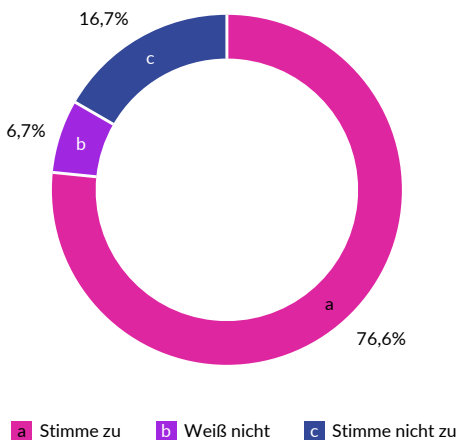
1	Öffentlichkeitsarbeit	141
2	Pressearbeit	145
3	Personal und Organisation der Dienststelle	148

1 Öffentlichkeitsarbeit

Am 30. Januar 2023 führte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz), der auch die Landesbeauftragte angehört, eine zentrale Veranstaltung anlässlich des 17. Europäischen Datenschutztags durch. Sie befasste sich mit dem Thema „Data Act und die Zukunft des Datenschutzes“. Impulse setzten zwei Beiträge der finnischen Datenschutzbeauftragten sowie eines Mitglieds des Europäischen Parlaments. Im Rahmen einer Podiumsdiskussion debattierten Behördenbeschäftigte, Parlamentsmitglieder sowie Vertreterinnen und Vertreter von Verbänden den Data Act – einen Gesetzesvorschlag der Europäischen Kommission. Dieser bezweckt, datengestützte Dienstleistungen innerhalb der Europäischen Union zu fördern, indem der Zugang zu nicht personenbezogenen Daten geregelt wird. Die damit einhergehende Ökonomisierung solcher Daten ist Teil einer umfassenderen europäischen Datenstrategie. Ausgerichtet wurde die Veranstaltung vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Namen der Datenschutzkonferenz.

Nach pandemiebedingter fünfjähriger Pause fand im Berichtsjahr erneut der Brandenburg-Tag statt: Als Ausrichterkommune lud die im südbrandenburgischen Elbe-Elster-Kreis gelegene Sängerstadt Finsterwalde am 2. und 3. September 2023 zum Landesfest ein. Wie schon auf früheren Brandenburg-Tagen war die Landesbeauftragte auch hier wieder mit einem Informationsstand vertreten. Unser Angebot umfasste neben Dialog, Informationsmaterial und kleinen Werbeartikeln mit plakativen Botschaften zum Datenschutz auch ein kurzes Quiz und eine Mitmachaktion „Stimmungsbarometer“. Das Quiz war dem Thema „Gerätesicherheit“ gewidmet. Mit drei Fragen zu Passwortwahl, Updates und öffentlich verfügbarem WLAN stellte es das Wissen hierzu spielerisch auf die Probe. Quer durch alle Altersgruppen fand das Thema große Resonanz und bot Anknüpfungspunkte für weitere Gespräche. Unser Stimmungsbarometer lud dazu ein, Stellung zu der Aussage „Wir brauchen mehr Datenschutz!“ zu nehmen. Dabei konnte zwischen den drei Antwortoptionen „Stimme zu“, „Weiß nicht“ und „Stimme nicht zu“ gewählt werden. Auch dieses Angebot wurde gut angenommen: Von 252 Teilnehmerinnen und Teilnehmern stimmten 193 der Aussage zu; 42 stimmten nicht zu; die übrigen 17 zeigten sich unentschlossen.

Wir brauchen mehr Datenschutz!



Die kritischen Stimmen beschrieben Datenschutz häufig als unliebsamen Mehraufwand. Einige sprachen dabei aus der Sicht von Verantwortlichen einer Datenverarbeitung, andere aus der Perspektive betroffener Personen. So klagten etwa manche im Gesundheitswesen Beschäftigte über administrative Mehrlasten bei der Verarbeitung von Patientendaten; Kritik aus Betroffenenperspektive galt vielfach der Cookie-Abfrage beim Besuch von Websites. Im Gespräch zeigte sich dann aber oft, dass Stein des Anstoßes gar nicht der Datenschutz war – als Grundrecht wurde Datenschutz vielmehr allgemein befürwortet. Lediglich die oftmals umständliche und bürokratische Art seiner Umsetzung war Anlass für Kritik. Hier bedarf es also anscheinend noch mancher Nachbesserung. Die Mehrheit der Standgäste bewertete Datenschutz hingegen uneingeschränkt positiv. Viele äußerten, teils eingefasst in Berichte von erlebten Datenschutzverletzungen und daraus entstandenen Schäden, auch den Wunsch nach weiterer Stärkung des Datenschutzes. Aus den Gesprächen mit den Besucherinnen und Besuchern unseres Informationsstandes haben wir zahlreiche Anregungen für unsere tägliche Arbeit mitgenommen.

Die Landesbeauftragte hat das bereits im Jahr 2018 veröffentlichte Faltblatt „Videoüberwachung in der Nachbarschaft“ im Berichtszeitraum überarbeitet und neu herausgegeben. Es zeigt Kamerabetrei-

berinnen und -betreibern auf, unter welchen Voraussetzungen eine Videoüberwachung erlaubt ist, und gibt Hinweise, welche Möglichkeiten betroffene Personen haben, um sich gegen aus ihrer Sicht unzulässige Kameras zu wehren.

Der Gerichtshof der Europäischen Union entscheidet in zahlreichen Fällen über grundlegende Fragen zur Auslegung der Datenschutz-Grundverordnung. Seinen Urteilen kommt für die Datenschutzpraxis eine hohe Bedeutung zu. Vor diesem Hintergrund weist die Landesbeauftragte auf ausgewählte Entscheidungen des Europäischen Gerichtshofs auf einer Schwerpunktseite ihres Internetangebots hin. Das Angebot wird ständig erweitert.

Die Datenschutzkonferenz hat im Berichtsjahr zwei Dokumente mit Anwendungshinweisen herausgegeben, die im Internetangebot der Landesbeauftragten abrufbar sind: Das Papier „Übermittlung personenbezogener Daten aus Europa an die USA“ vom 4. September 2023 befasst sich mit dem Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023. Es richtet sich sowohl an Verantwortliche und Auftragsverarbeiter in Deutschland, die personenbezogene Daten an die USA übermitteln, als auch an betroffene Personen. Die Anwendungshinweise beleuchten insbesondere die Reichweite und den Anwendungsbereich der Neuregelung, den Einsatz alternativer Instrumente für Übermittlungen an die USA sowie Umfang und Durchsetzung von Rechten betroffener Personen gegenüber Stellen in den USA.

Durch die Ausarbeitung von Verhaltensregeln (Code of Conduct) lassen sich die Vorgaben der Datenschutz-Grundverordnung für besondere Kategorien von Verantwortlichen branchen- bzw. verbandspezifisch konkretisieren. In ihren Anwendungshinweisen „Kernelemente der Überwachungsaufgaben von Überwachungsstellen für Verhaltensregeln nach Art. 40 DS-GVO“ vom 23. November 2023 erläutert die Konferenz anhand praktischer Beispiele die wesentlichen Gesichtspunkte, die in solche Verhaltensregeln aufzunehmen sind.

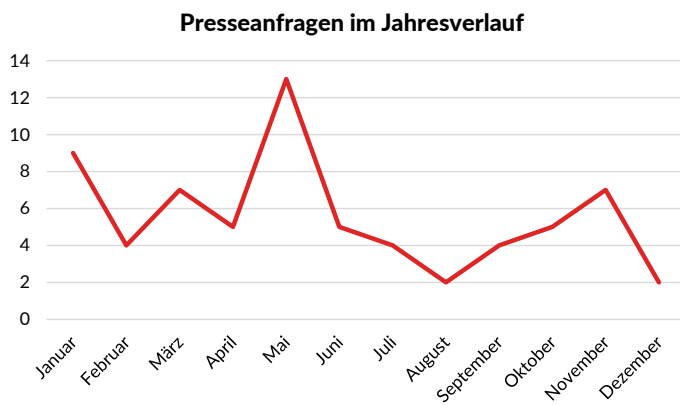
Außerdem hat die Landesbeauftragte im Berichtsjahr wieder die neuen Leitlinien des Europäischen Datenschutzausschusses in ihrem Internetangebot veröffentlicht. Sie bezwecken die Förderung eines gemeinsamen Verständnisses der EU-Datenschutzvorschriften. Im



Jahr 2023 hatten die Leitlinien die Anwendung des Artikels 65 Absatz 1 Buchstabe a Datenschutz-Grundverordnung, die Berechnung von Bußgeldern, den Einsatz von Technologien zur Gesichtserkennung auf dem Gebiet der Strafverfolgung, das Recht betroffener Personen auf eine Datenauskunft, die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters bei grenzüberschreitender Datenverarbeitung, die Meldung von Datenschutzverletzungen, die Zertifizierung als Instrument für Übermittlungen, das Vermeiden irreführender Designeffekte in sozialen Medien sowie das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V Datenschutz-Grundverordnung zum Inhalt. Üblicherweise erscheinen diese Dokumente des Europäischen Datenschutzausschusses zunächst in englischer Sprache und werden nach ihrer Veröffentlichung in andere Sprachen der Europäischen Union übersetzt. Wir sind weiterhin bestrebt, die deutsche Übersetzung zur Verfügung zu stellen, sobald sie vorliegt.

2 Pressearbeit

Im Berichtszeitraum haben wir 67 Medienanfragen zum Datenschutz beantwortet. Das überstieg die Vorjahreszahl um etwa 18 %. Eine deutliche Häufung der Anfragen zeigt sich im Mai des Jahres 2023. Grund hierfür dürfte das große Interesse an einem europäischen Aufsichtsverfahren gegenüber einem internationalen Konzern, der in Brandenburg eine Produktionsstätte betreibt, gewesen sein. Dieses hat die Landesbeauftragte zuständigkeitshalber an die niederländische Datenschutzaufsichtsbehörde abgegeben.³² Weiterhin interessierten sich die Medien vor allem für die Datenverarbeitung durch Unternehmen. Knapp die Hälfte der insgesamt eingegangenen Anfragen richtete sich darauf, während weniger als ein Drittel öffentliche Stellen betraf.

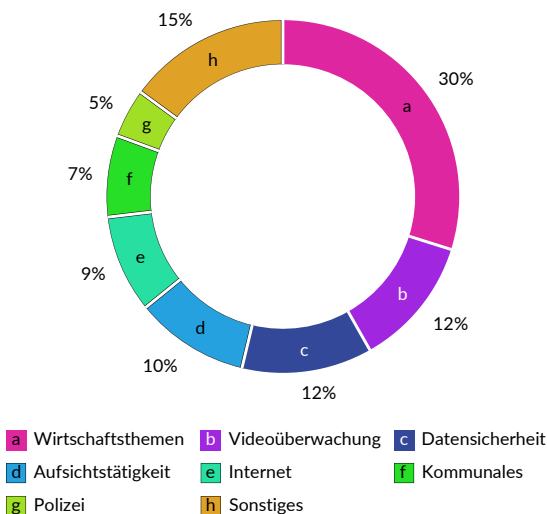


Interesse an Datenschutzthemen im Zusammenhang mit der Corona-Pandemie spiegelte sich im Berichtsjahr erwartungsgemäß so gut wie überhaupt nicht mehr in den Anfragen wider. Eindeutiger Schwerpunkt waren klassische Wirtschaftsthemen mit etwa 30 %.

³² Siehe A IV 1.

Dazu gehörte auch das Interesse an dem bereits erwähnten europäischen Verfahren. Die Themen Videoüberwachung und Datensicherheit folgten mit großem Abstand. Auch interessierte die Tätigkeit der Landesbeauftragten als Aufsichtsbehörde – hier waren beispielsweise statistische Angaben zu Sanktionsmaßnahmen gefragt. Der Datenschutz im Internet, kommunale Themen sowie die Datenverarbeitung durch Polizeibehörden standen zu geringeren Anteilen im Fokus der Medien.

Schwerpunkte der Presseanfragen



Die im Vorjahr festgestellte Tendenz zu mehr Nachfragen von Online-Medien hat sich im Jahr 2023 nicht weiter fortgesetzt. Mit 18 % waren sie an der Gesamtzahl der Anfragen beteiligt – das entspricht in etwa dem Ergebnis aus dem Jahr 2022. Anfragen von Fernsehsendern kamen im Berichtsjahr auf einen nur geringfügig höheren Anteil; Print-Medien waren mit 39 % annähernd konstant vertreten. Festzustellen ist allerdings, dass die Abgrenzung zwischen den einzelnen Arten der Medien zunehmend schwerfällt, da viele ihre Berichterstattung inzwischen in unterschiedlicher Weise anbieten.

Verändert hat sich im Vorjahresvergleich die regionale Herkunft der Anfragen: Nach 58 % im Vorjahr stammten im Berichtsjahr nur mehr etwa 52 % der Anfragen aus den Ländern Brandenburg oder Berlin und nach 33 % im Jahr 2022 nunmehr 36 % aus anderen Bundesländern oder von überregional tätigen Medien. 12 % der Anfragen wurden von internationalen Medien gestellt; zuvor waren dies lediglich 9 %. Auch diese Tendenz führen wir auf das bundesweit und international große Interesse an dem genannten europäischen Verfahren zurück.



3 Personal und Organisation der Dienststelle

Die Personalsituation der Dienststelle war im Berichtsjahr so schwierig wie noch nie zuvor in meiner 18-jährigen Amtszeit. Insgesamt standen der Landesbeauftragten planmäßig 42 Stellen zur Verfügung. Allerdings waren im Jahr 2023 5 Weggänge von Mitarbeiterinnen und Mitarbeitern zu verkräften. Sie betrafen die Bereiche Recht und Verwaltung. Auch waren, wie im Vorjahr, mehrere Elternzeiten, verschiedene Arbeitszeitverkürzungen und Langzeiterkrankungen zu kompensieren.

Nachbesetzungen bzw. Vertretungen mussten durch eine Vielzahl von Ausschreibungsverfahren gefunden werden. Einzelne waren schon beim ersten Mal erfolgreich, die Mehrzahl jedoch erst nach einer wiederholten Ausschreibung.

Verschärft wurde die Situation im Berichtsjahr durch einen hohen Krankenstand in unserer Behörde – ein Phänomen, das nach Darstellung der Krankenkassen auch Arbeitnehmerinnen und Arbeitnehmer anderer Branchen betraf. Bei dem ohnehin schon bestehenden Personalmangel war die Vertretung der Ausfallzeiten eine erhebliche Herausforderung. Als Folge verlängerten sich die Zeiten für die Bearbeitung von Beschwerden oder für die Durchführung von Kontrollen deutlich. Beschwerdeführerinnen und Beschwerdeführern waren die Verzögerungen nur selten zu vermitteln, sie entsprechen auch nicht den gesetzlichen Anforderungen bzw. den Ansprüchen meiner Behörde. Außerdem fielen Beratungen datenschutzrechtlich Verantwortlicher aus und wichtige interne Projekte mussten verschoben werden.

Mein außerordentlicher Dank gilt deshalb wieder allen Beschäftigten meiner Dienststelle, die durch Vertretungen erhebliche Mehrarbeit geleistet haben.

Auch die angespannte Raumsituation der Dienststelle hat sich im Berichtsjahr nicht verbessert. Nachdem bereits in der Vergangenheit Funktionsräume zu Büros umgebaut wurden, musste ich inzwischen die wenigen hierfür geeigneten Räume doppelt belegen. Weiterer Spielraum besteht nicht. Auf Ausschreibungen zur Kompensation von Arbeitszeitverkürzungen sowie auf Angebote für Referendarin-

nen und Referendare muss ich deshalb verzichten. Die Gebäude sind darüber hinaus in einem Zustand, der häufig Reparaturen erfordert. Den Anforderungen an die Barrierefreiheit genügen sie nach wie vor nicht einmal ansatzweise. In mangelhaftem Zustand ist auch die Einfriedung der Dienststelle. Hierdurch gelang es Kleinmachnower Wildschweinen regelmäßig, auf die Liegenschaft zu gelangen und die Grünflächen zu zerstören. In Einzelfällen kam es auch zu unangenehmen Begegnungen für Mitarbeiterinnen und Mitarbeiter. Vor diesem Hintergrund ist es sicher verständlich, dass ich weiterhin den Umzug meiner Behörde nach Potsdam anstrebe – in barrierefreie Räumlichkeiten auf einer schwarzwildfreien Liegenschaft.



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