Landesbeauftragte
für Datenschutz
und Akteneinsicht

Tätigkeitsbericht 2019
Datenschutz

Titelbild

Motiv:	Informations-, Kommunikations- und Medienzentrum Cottbus der Brandenburgischen Technischen Universität Cottbus-Senftenberg am Standort Cottbus
Architekten:	Herzog & de Meuron
Fertigstellung:	2004
Bildrechte:	imago images / Volker Preußer

Impressum

Herausgeber: Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht Brandenburg
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

Druck: Brandenburgische Universitätsdruckerei
und Verlagsgesellschaft Potsdam mbH

Tätigkeitsbericht Datenschutz

der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zum 31. Dezember 2019

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 2019 ab.

Der Tätigkeitsbericht kann auch aus unserem Internetangebot unter www.LDA.Brandenburg.de abgerufen werden.

Vorwort

Liebe Leserinnen und Leser,

wenn Datenschützerinnen und Datenschützer auf das Jahr 2019 zurückblicken, geht es in erster Linie um die Erfahrungen mit der Datenschutz-Grundverordnung – schließlich war es das erste Kalenderjahr, in dem das neue Datenschutzrecht durchgehend vom 1. Januar bis zum 31. Dezember galt. Zeit also, eine erste echte Jahresbilanz zu erstellen. Ich berichte deshalb über die von meiner Behörde ergriffenen Aufsichtsmaßnahmen, über Prüfungen, ausgewählte Fälle und Beratungen, die einen Querschnitt der Aufgaben darstellen, mit denen meine Mitarbeiterinnen, Mitarbeiter und ich im zurückliegenden Jahr beschäftigt waren.

Zwar haben sich die anfänglichen Unsicherheiten der Verantwortlichen inzwischen gelegt. Viele Regelungsinhalte waren schließlich doch nicht so neu, wie die aufgeregte Debatte zunächst suggerierte. Dennoch zeigen zahlreiche Beschwerden der Bürgerinnen und Bürger, dass Datenschutzvorschriften teilweise noch immer nicht vollständig umgesetzt werden. Auch an der unverändert intensiven Berichterstattung der Medien lässt sich das gestiegene Bewusstsein für die Bedeutung des Datenschutzes ablesen. Berichte über sogenannte Datenpannen finden sich dort fast täglich. Dies hat auch mit den neuen Melde- und Informationspflichten für die Verantwortlichen zu tun. Ob die größere Wahrnehmbarkeit nun bedeutet, dass mehr Datenpannen passieren, oder dass sie in der Vergangenheit einfach nicht bekannt wurden, mag dahinstehen. Auf jeden Fall dürfte die Pflicht, sie den Aufsichtsbehörden zu melden und die Betroffenen zu informieren, zu einer Sensibilisierung der Verantwortlichen beitragen und bewirken, dass diese effektivere Schutzmaßnahmen ergreifen.

Zahlreiche Beschwerden bei den Aufsichtsbehörden zeigen, dass die Einhaltung von Informations- und Auskunftspflichten der Verantwortlichen – insbesondere im Online-Handel bzw. auf Plattformen sozialer Medien und Netzwerke – nach wie vor ein wesentliches Problem darstellt. Gerade hier sind große und internationale Konzerne oftmals marktführend. Für ein angemessenes Datenschutzniveau in der Wirtschaft ist es schon aufgrund der Vorbildwirkung für kleine und mittlere Unternehmen entscheidend, dass gerade diese Global

Player europäische Vorschriften einhalten. Um den Datenschutz hier durchzusetzen, bedarf es konsequenter Entscheidungen der europäischen Aufsichtsbehörden – einschließlich der Verhängung von Geldbußen – ebenso wie einer Rechtsprechung, welche die Ziele des europäischen Verordnungsgebers klar im Blick behält. Erste Beispiele dafür haben wir im Jahr 2019 bereits gesehen.

Auch die öffentliche Verwaltung hat bei der Umsetzung der Datenschutzvorschriften noch erhebliches Potenzial nach oben. Insbesondere fehlen vielen Stellen die erforderlichen personellen und finanziellen Kapazitäten. Diese sind aber eine Voraussetzung dafür, dass Digitalisierungsprojekte, die gegenwärtig eine Hochkonjunktur erleben und uns noch lange beschäftigen werden, gelingen. Staat und Kommunen müssen gerade hier das Grundrecht der Bürgerinnen und Bürger auf den Schutz ihrer personenbezogenen Daten gewährleisten, um eine Akzeptanz für die digitalen Leistungen zu schaffen. Meine Dienststelle wird solche Projekte weiterhin konstruktiv begleiten.

Neben der Datenschutz-Grundverordnung hat die europäische Datenschutzreform noch ein zweites Ergebnis hervorgebracht: Die Datenschutzrichtlinie für Justiz und Inneres. In der öffentlichen Wahrnehmung führte sie bislang zu Unrecht eher ein Schattendasein. Die Richtlinie wird durch das im Juni 2019 in Kraft getretene Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz im Landesrecht umgesetzt. Diese neuen Vorschriften gelten speziell für Polizei- und Justizvollzugsbehörden.

Mit diesem Tätigkeitsbericht komme ich sowohl der Verpflichtung der Datenschutz-Grundverordnung (Teil A) als auch des Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetzes (Teil B) zur Vorlage eines jeweils jährlichen Tätigkeitsberichts nach. Außerdem berichte ich über die personelle und organisatorische Entwicklung meiner Dienststelle (Teil C).

Wie immer wünsche ich Ihnen eine interessante Lektüre.

Dagmar Hartge

Teil A: Bericht nach Art. 59 Datenschutz-Grundverordnung

I Datenschutzverstöße: Maßnahmen und Sanktionen

1 Verfahren bei der Aufsichtsbehörde: Von der Beschwerde bis zur Ahndung des Datenschutzverstoßes

Tagtäglich erreichen uns zahlreiche Beschwerden von Bürgerinnen und Bürgern, die eine Verletzung ihres Rechts auf informationelle Selbstbestimmung vermuten. Sei es, weil sie ungewollt Werbung erhalten, weil sie meinen, von der Videokamera in der Nachbarschaft erfasst zu werden oder weil eine Vertragspartnerin bzw. ein Vertragspartner ihnen keine Auskunft über ihre dort gespeicherten Daten gibt. Die Gründe sind mannigfaltig. Vielfach wird die Geduld der Beschwerdeführerinnen und Beschwerdeführer auf eine harte Probe gestellt, da das Verfahren bereits bei uns erhebliche Zeit in Anspruch nehmen kann. Deshalb sollen an dieser Stelle die Schritte unserer Prüfung näher erläutert werden.

Dem gesetzlichen Auftrag folgend, die Einhaltung datenschutzrechtlicher Bestimmungen zu überwachen und konsequent durchzusetzen, eröffnen wir nach Eingang der Beschwerde im Regelfall ein Verwaltungsverfahren. Dies dient zunächst dazu, den Sachverhalt genau zu ergründen. In einem ersten Schreiben teilen wir dem aus datenschutzrechtlicher Sicht für die Verarbeitung der personenbezogenen Daten Verantwortlichen den Gegenstand der Beschwerde mit und geben ihm im Rahmen einer Anhörung Gelegenheit, zum geschilderten Sachverhalt Stellung zu nehmen, unsere Fragen zu beantworten und Unterlagen einzureichen. Sollte diese Möglichkeit, zur Aufklärung des Sachverhalts freiwillig beizutragen, ungenutzt verstreichen, verpflichten wir den Verantwortlichen, uns die notwendigen Auskünfte zu geben und erlassen gegen ihn einen förmlichen Bescheid. Gemäß Artikel 58 Absatz 1 Buchstabe a Datenschutz-Grundverordnung (DS-GVO) i. V. m. § 40 Absatz 4 Satz 1 Bundesdatenschutzgesetz haben die der Aufsicht unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen auf Verlangen die für die Erfüllung unserer Aufgaben erforderlichen Auskünfte zu erteilen. Eine Auskunft kann nur auf solche Fragen verweigert werden, deren Beantwortung den Verantwortlichen selbst oder einen seiner in § 383 Absatz 1 Nummer 1 bis 3 Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen

Kein Ergebnis ohne Anhörung

würde. In diesem Fall müsste er sich ausdrücklich auf dieses spezielle Auskunftsverweigerungsrecht berufen.

Jetzt sollte der Verantwortliche innerhalb der ihm gesetzten Frist (meist 14 Tage ab Zustellung des Bescheides) reagieren. Tut er dies nicht, so sind wir gezwungen, die Festsetzung eines Zwangsgeldes anzudrohen. Verweigert der Verantwortliche danach immer noch die Mitwirkung, setzen wir ein Zwangsgeld fest, welches gegebenenfalls im Wege des Zwangsvollstreckungsverfahrens beigetrieben wird. Die Höhe des Zwangsgeldes beträgt mindestens 10 und höchstens 50.000 Euro; so bestimmt es das Brandenburgische Verwaltungsvollstreckungsgesetz. In jedem Fall soll einem „Freikaufen“ entgegengewirkt werden. Dies wäre nicht akzeptabel und würde dem Willen des Gesetzgebers, die in Rede stehenden personenbezogenen Daten vor unbefugter Verarbeitung zu schützen, widersprechen.

Zu beachten ist, dass Zwangsmittel so oft und so lange angewendet werden können, bis die Verpflichtung vollständig erfüllt ist. Zudem besteht die Möglichkeit, Ersatzzwangshaft beim zuständigen Verwaltungsgericht zu beantragen, sofern das festgesetzte Zwangsgeld uneinbringlich ist.

Dazu muss es jedoch nicht kommen. Die freiwillige und rechtzeitige Bereitstellung der angefragten Informationen und Unterlagen gibt dem Verantwortlichen letztlich auch immer die Gelegenheit, für ihn günstige Tatsachen der Aufsichtsbehörde glaubhaft zu machen. So kann er beispielsweise nachweisen, dass eine Verantwortung im Sinne der Datenschutz-Grundverordnung für die in Rede stehende Datenverarbeitung nicht besteht oder dass die Daten zu Recht verarbeitet werden, weil eine vertragliche Beziehung zur Beschwerdeführerin oder zum Beschwerdeführer existiert.

Mitunter verweigern Verantwortliche die erforderlichen Auskünfte und drängen uns dazu, stattdessen eine Vor-Ort-Besichtigung durchzuführen. Aus verschiedenen Erwägungen ist dies allerdings nicht immer optimal. Grundsätzlich bestimmt die Behörde Art und Umfang der Ermittlungen. An das Vorbringen und die Beweisanträge der Beteiligten ist sie nicht gebunden. Dadurch ist es dem pflichtgemäßen Ermessen der Behörde überlassen, welche Mittel sie für die Erforschung des Sachverhalts anwendet. Zudem würde eine Vor-Ort-Kontrolle den Verantwortlichen in der Regel nicht davon befrei-

en, der Aufsichtsbehörde Auskünfte zu Gegebenheiten zu erteilen, die durch eine solche nicht ermittelt werden können, beispielsweise, welche Zwecke der Verantwortliche mit der Datenverarbeitung verfolgt.

Hat der Verantwortliche alle erforderlichen Informationen gegeben, bewerten wir, ob datenschutzrechtliche Bestimmungen eingehalten oder verletzt werden. Ergibt sich dabei, dass die Verarbeitungsmodalitäten nicht im Einklang mit den Rechtsvorschriften stehen oder standen, können wir entsprechende Abhilfemaßnahmen ergreifen (beispielsweise eine Verwarnung aussprechen, eine Einschränkung der Verarbeitung anordnen oder anweisen, personenbezogene Daten zu löschen). Artikel 58 Absatz 2 DS-GVO stellt einen umfassenden Katalog von Maßnahmen zur Verfügung.[1] Auch in diesem Verfahrensstadium geben wir den Verantwortlichen die Gelegenheit, zu der von uns beabsichtigten Abhilfemaßnahme Stellung zu nehmen, bevor ein verbindlicher Bescheid erlassen wird. Wie bereits vorstehend im Zusammenhang mit der Verpflichtung zur Auskunft geschildert, kann auch eine angeordnete Maßnahme mittels Zwangsgeld durchgesetzt werden. In schwerwiegenden Fällen leiten wir ein Bußgeldverfahren ein. Das Verfahren richtet sich nach den Vorschriften des Ordnungswidrigkeitengesetzes in Verbindung mit der Strafprozessordnung.

Gemäß Artikel 78 Absatz 2 DS-GVO informieren wir Betroffene, die sich bei uns beschweren, regelmäßig über den Verfahrensstand. Außerdem geben wir ihnen das jeweilige Ergebnis unserer datenschutzrechtlichen Prüfung zur Kenntnis. Sollten sie hiermit nicht einverstanden sein, so steht es ihnen frei, dagegen vor dem zuständigen Gericht zu klagen.

2 Unerwünschte Werbung vier Jahre nach Vertragsanfrage

Im Berichtszeitraum wandte sich ein Bürger an uns, nachdem er eine personalisierte Werbesendung eines Versicherungsunternehmens erhalten hatte. Die dafür verwendeten personenbezogenen Daten stammten aus einer Anfrage, welche er an das Unternehmen gerichtet hatte. Auf dieser Grundlage erstellte die verantwortliche Stelle ein Angebot über den Abschluss eines Versicherungsvertrages. Ein

1 Tätigkeitsbericht 2016/2017, A 2.8.

solcher Vertrag kam letztlich jedoch nicht zustande. Um den späteren Beschwerdeführer doch noch als Kunden zu gewinnen, griff das Unternehmen vier Jahre später auf diese Daten zurück und versandte ein Werbeschreiben, wobei neben den Kontaktdaten auch einzelne Angaben aus der Vertragsanfrage verwendet wurden, um ein passendes, auf den potenziellen Kunden zugeschnittenes Produkt präsentieren zu können.

Eine Verarbeitung personenbezogener Daten ist gemäß Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS GVO) nur dann rechtmäßig, wenn einer der dort genannten Erlaubnistatbestände erfüllt ist. Im vorliegenden Fall hatte die betroffene Person weder ihre Einwilligung zu der erneuten Verarbeitung gegeben (Artikel 6 Absatz 1 Buchstabe a DS-GVO), noch war die Verwendung der Daten für die Erfüllung eines Vertrages erforderlich (Artikel 6 Absatz 1 Buchstabe b DS-GVO). Zu letztgenanntem Zweck ist eine Datenverarbeitung erlaubt, soweit sie objektiv für die Erfüllung oder Durchführung eines konkreten Vertrages oder vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. Vor diesem Hintergrund war die ursprüngliche Verarbeitung personenbezogener Daten zum Zwecke der Angebotserstellung vor vier Jahren legitim. Die nachfolgende, weitere Verarbeitung zu Zwecken der Werbung war es hingegen nicht.

Berechtigte Werbeinteressen bestehen nicht ewig.

Auch konnte die konkrete Datenverarbeitung nicht auf die Rechtsgrundlage zur Wahrung berechtigter Interessen des Verantwortlichen gemäß Artikel 6 Absatz 1 Buchstabe f DS-GVO gestützt werden. Zwar kann nach Erwägungsgrund 47 DS-GVO die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden. Allerdings sind im Rahmen der nach Artikel 6 Absatz 1 Buchstabe f DS-GVO anzustellenden Interessenabwägung auch die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person zu berücksichtigen.

Grundsätzlich hat der Gesetzgeber dem Schutz der personenbezogenen Daten ein besonderes Gewicht beigemessen und verlangt eine Abwägung mit den Interessen des Verantwortlichen oder Dritter an der Beschaffung, Verwendung und Offenlegung solcher Daten. Maßgeblich sind hierbei die vernünftigen Erwartungen der betroffenen Person. Kann diese zum Zeitpunkt der Datenerhebung angesichts

der näheren Umstände nicht absehen, dass eine Datenverarbeitung für einen bestimmten Zweck stattfinden wird, überwiegen die Interessen und Grundrechte der betroffenen Person regelmäßig das Interesse des Verantwortlichen. Liegt der letzte geschäftliche Kontakt – wie in diesem Fall – mehr als vier Jahre zurück und kommt der Vertrag nicht zustande, erwartet die betroffene Person nicht, dass alte Daten aus der Vertragsanbahnung plötzlich wieder für die werblichen Zwecke der Kundengewinnung genutzt werden.

Bei der Prüfung des zugrundeliegenden Prozesses für die Auswahl der Empfänger von Werbesendungen stellten wir sodann fest, dass das Datum des letzten geschäftlichen Kontakts vom Unternehmen durchaus berücksichtigt wird. Die Daten des Beschwerdeführers hätten danach nicht ausgewählt werden dürfen. Aufgrund eines individuellen Bearbeitungsfehlers geschah dies dennoch. Um dem Unternehmen den Verstoß vor Augen zu führen und für den sorgsamen Umgang mit personenbezogenen Daten weiter zu sensibilisieren, sprach die Landesbeauftragte eine Verwarnung nach Artikel 58 Absatz 2 Buchstabe b DS-GVO aus.

3 Veröffentlichung personenbezogener Einwendungen gegen einen Regionalplan

Die Regionalplanung ist ein wesentliches Instrument für die Umsetzung der übergeordneten landesplanerischen Festlegungen aus dem Landesentwicklungsprogramm und den Landesentwicklungsplänen. Mit dem Gesetz zur Regionalplanung und zur Braunkohlen- und Sanierungsplanung wurden fünf Regionale Planungsgemeinschaften im Land Brandenburg gebildet. Bei der Erarbeitung der Regionalpläne durch die Regionalen Planungsgemeinschaften ist eine Beteiligung der Öffentlichkeit nach § 9 Raumordnungsgesetz durchzuführen.

Im Rahmen einer solchen Beteiligung hat die Regionale Planungsgemeinschaft Prignitz-Oberhavel Einwendungen von Bürgerinnen und Bürgern gegen den Regionalplan ins Internet eingestellt und dabei versäumt, die personenbezogenen Daten der Einbringenden unkenntlich zu machen. Darüber beschwerten sich mehrere Betroffene. Auch die Regionale Planungsstelle meldete uns den Vorfall. Sie teilte mit, dass von der unzureichenden Anonymisierung in dem veröffentlichten Bericht circa 3.000 Personen betroffen waren. Der Fehler wurde behoben, indem der Bericht aus dem Internet entfernt und hinreichend anonymisiert neu eingestellt wurde.

Wie wir feststellten, waren die personenbezogenen Daten mehrere Tage frei im Internet einsehbar, ohne dass die genannten Personen hierzu ihre Einwilligung erteilt hatten. Die Namen waren zwar im Dokument mittels grauer Balken auf den ersten Blick verdeckt, sie konnten jedoch durch Markierung des Feldes und Übertragung in ein anderes Programm sichtbar gemacht werden. Um zu verhindern, dass die Identität der betroffenen Personen durch Unbefugte bestimmt werden kann, war diese Form der Aussonderung untauglich.

Untaugliche Schwärzung führt zu Datenübermittlung

Unsere Prüfung des Sachverhalts ergab, dass die von der unrechtmäßigen Veröffentlichung betroffenen Datenkategorien grundsätzlich einem normalen Schutzbedarf unterlagen. Von einem erhöhten Risiko für die Betroffenen war durch die versehentliche Veröffentlichung der Daten im Internet nicht auszugehen. Der nachweisbare Zeitraum der Offenlegung umfasste nur wenige Tage. Dennoch hat die Landesbeauftragte gegenüber der Regionalen Planungsgemeinschaft eine Verwarnung nach Artikel 58 Absatz 2 Buchstabe b Datenschutzgrundverordnung (DS-GVO) ausgesprochen, da diese gegen den Grundsatz der Integrität und Vertraulichkeit gemäß Artikel 5 Absatz 1 Buchstabe f DS-GVO sowie gegen den Grundsatz der Sicherheit der Verarbeitung gemäß Artikel 32 DS-GVO verstoßen hat. Die Gemeinsame Landesplanungsabteilung Berlin-Brandenburg wurde in ihrer Funktion als Rechtsaufsichtsbehörde über die Verwarnung unterrichtet.

4 Videoüberwachung in einer Zahnarztpraxis – Bundesverwaltungsgericht bestätigt Landesbeauftragte

Eine Zahnärztin hatte im für jedermann zugänglichen Empfangs- und Wartebereich ihrer Praxis eine Videoüberwachungskamera installiert. Der vorhandene Empfangstresen blieb, da Personal fehlte, regelmäßig unbesetzt. Um dennoch den Empfangsbereich der Praxis im Blick haben zu können, übertrug die Kamera in Echtzeit das Geschehen auf Monitore in die Behandlungszimmer. Die Bilder wurden nicht gespeichert. An der Praxistür wies ein Schild mit der Aufschrift „videogesichert“ auf die Videoüberwachung hin.

Aufgrund einer Beschwerde prüften wir die Zulässigkeit dieser Datenverarbeitung. Im Ergebnis ordnete die Landesbeauftragte bereits

im Jahr 2012 an, die Kamera so auszurichten, dass der für Patientinnen und Patienten sowie sonstige Besucherinnen und Besucher zugängliche Bereich nicht mehr erfasst wird. Insoweit sahen wir einen Verstoß gegen datenschutzrechtliche Vorschriften gegeben. Hiergegen wehrte sich die Zahnärztin erfolglos durch alle Gerichtsinstanzen. Zuletzt bestätigte das Bundesverwaltungsgericht die Rechtmäßigkeit unserer Anordnung.[2]

So entschieden die Richter, dass der von der Zahnärztin angegriffene Verwaltungsakt allein nach altem Recht, nicht jedoch nach der zwischenzeitlich in Kraft getretenen Datenschutz-Grundverordnung (DS-GVO) beurteilt werden muss. Anzuwenden sei das Recht, das zum Zeitpunkt der letzten Behördenentscheidung Geltung hatte. Im vorliegenden Fall war demgemäß der Erlass des Widerspruchsbescheids im Januar 2013 der für die Beurteilung der Rechtmäßigkeit maßgebliche Zeitpunkt. Die Rechtmäßigkeit unserer Anordnung wurde folglich nach dem bis Mai 2018 geltende Bundesdatenschutzgesetz geprüft.

Die Zahnärztin hatte vorgetragen, die Videoüberwachung sei von berechtigten Interessen gedeckt. Dazu führte sie mögliche Straftaten wie den Diebstahl von im Empfangstresen aufbewahrten Betäubungsmitteln oder von Wertsachen an. Ebenso sei ein Eingreifen in Notfällen möglich, beispielsweise wenn „eingespritzte“ Patientinnen und Patienten nach der Behandlung noch im Wartezimmer sitzen. Überdies diene die Kamera der Senkung der Personalkosten.

Das Gericht folgte der bisherigen Rechtsprechung, wonach die Verhinderung und Aufklärung von Straftaten zwar grundsätzlich ein berechtigtes Interesse darstellen können. Jedoch seien sie nur dann zur Rechtfertigung heranziehbar, wenn sich aus tatsächlichen Erkenntnissen eine Gefährdungslage ergibt, die über das allgemeine Lebensrisiko hinausgeht. Reine Befürchtungen genügen nicht. Zudem könnte vorbeugend darauf verzichtet werden, Betäubungsmittel im unbesetzten Empfangstresen aufzubewahren. Patientinnen und Patienten könnten aufgefordert werden, ihre Wertsachen in die Behandlungsräume mitzunehmen.

Anders als von der Klägerin angenommen, ist die Videoüberwachung auch nicht zulässig, um Patientinnen und Patienten, die nach einer

2 Urteil des Bundesverwaltungsgerichts vom 27. März 2019, 6 C 2.18.

Betäubungsspritze im Wartezimmer sitzen, im Notfall betreuen zu können. Bereits die Vorinstanz hatte deutlich gemacht, dass mildere Mittel diese Zwecke ebenso erfüllen – beispielsweise der Einsatz zusätzlichen Personals oder ein Notfallknopf. Nicht überzeugt zeigte sich das Bundesverwaltungsgericht von dem pauschalen Verweis der Klägerin auf erheblich höhere Personalkosten im Falle des Verzichts auf eine Kamera. Zwar handele es sich durchaus um ein berechtigtes Interesse, Betriebskosten zu senken. Die Zahnärztin habe aber nicht darlegt, dass sie diese Kosten nicht auch durch andere Maßnahmen, beispielsweise durch organisatorische Umstrukturierungen, hätte vermeiden können. Kosteneinsparungen allein können die Zulässigkeit einer Videoüberwachung keinesfalls begründen.

Kosteneinsparung kein Argument für Videoüberwachung

Zwar beurteilte das Bundesverwaltungsgericht den Fall nach der alten Rechtslage, äußerte sich aber auch zur seit Mai 2018 geltenden. Es machte unmissverständlich klar, dass die Zulässigkeitsvoraussetzungen einer Videoüberwachung durch nicht öffentliche Stellen, zu denen auch niedergelassene Ärztinnen und Ärzte zählen, abschließend in Artikel 6 Absatz 1 DS-GVO geregelt sind. Derartige Datenverarbeitungen können nicht auf Artikel 6 Absatz 1 Buchstabe e DS-GVO gestützt werden, denn diese werden – im Gegensatz zu Behörden – nicht zur Erfüllung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt tätig. Demzufolge erfassen die Öffnungsklauseln des Artikels 6 Absatz 2 und 3 DS-GVO, die dem nationalen Gesetzgeber die Möglichkeit geben, weitere Rechtsgrundlagen zu schaffen, nicht die Datenverarbeitungen privater Verantwortlicher. Die nationale Bestimmung in § 4 Absatz 1 Satz 1 Bundesdatenschutzgesetz in der aktuellen Fassung ist daher mit dem Europarecht unvereinbar und im Ergebnis nicht anzuwenden. Nicht öffentliche Stellen können Videokameras in der Regel nur auf der Rechtsgrundlage des Artikel 6 Absatz 1 Buchstabe f DS-GVO betreiben. Auch bei der Beurteilung nach dieser neuen Norm kommt es auf die Abwägung des berechtigten Interesses des Verantwortlichen mit denen der Betroffenen an. Diesbezüglich verwiesen die Richter auf ihre vorherige Argumentation zur alten Rechtslage.

5 Weiträumige Videoüberwachung in einem Kultur- und Gewerbezentrum

Die Hausverwaltung eines Gebäudekomplexes betrieb 14 Videokameras. Die Videobilder wurden für drei Tage gespeichert, außerdem kam eine Nachtsichtfunktion zum Einsatz. Von der Überwachung waren sowohl zahlreiche Gewerbetreibende, Besucherinnen und Besucher des Komplexes als auch Bewohnerinnen und Bewohner eines Mietshauses betroffen. Neben einer Fleischerei und einer Autowerkstatt befanden sich u. a. eine Diskothek und ein Theater im Erfassungsbereich der Kameras. Als Zwecke nannte uns die Hausverwaltung insbesondere eine Besserung der Sicherheitslage, den Schutz vor Diebstahl und Vandalismus sowie die Möglichkeit, Täterinnen und Täter verfolgen zu können.

Gemäß Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) ist eine Datenverarbeitung nur zulässig, wenn die betroffenen Personen eingewilligt haben oder eine andere gesetzliche Erlaubnisnorm erfüllt ist (Verbot mit Erlaubnisvorbehalt). In diesem Fall konnte sich die Zulässigkeit nur aus Artikel 6 Absatz 1 Buchstabe f DS-GVO ergeben. Nach dieser Norm sind die berechtigten Interessen, die der Verantwortliche mit der Datenverarbeitung verfolgt, gegen die Rechte und Interessen der von der Videoüberwachung Betroffenen abzuwägen. Die anderen in Artikel 6 Absatz 1 DS-GVO genannten Voraussetzungen lagen nicht vor. Darüber hinaus kam § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) als Erlaubnisnorm für die Videoüberwachung nicht in Betracht, da für die Anwendung dieser Regelung aus europarechtlichen Gründen kein Raum bleibt.[3]

Videoüberwachung nur mit Augenmaß

Zu den berechtigten Interessen des Artikel 6 Absatz 1 Buchstabe f DS-GVO zählen alle nicht von der Rechtsordnung missbilligten Interessen rechtlicher, wirtschaftlicher oder ideeller Art. Auf reine Blankettformeln, wie der von der Hausverwaltung verfolgte Zweck der „Besserung der Sicherheitslage“, kann die Videoüberwachung jedoch nicht gestützt werden.

3 siehe A I 4

Soweit die Hausverwaltung mit der Videoüberwachung beabsichtigte, die Begehung von Straftaten wie Diebstahl und Sachbeschädigungen zu verhindern und die Taten verfolgen zu können, war zu berücksichtigen, dass zur Erreichung dieser Zwecke Alternativen zur Verfügung standen, wie z. B. eine bessere Beleuchtung und häufigere Kontrollen durch den Hausmeister oder zusätzliches Sicherheitspersonal. Denn höhere Kosten allein — etwa durch den Einsatz von zusätzlichem Personal — führen nicht dazu, dass Alternativmaßnahmen von vornherein außer Betracht bleiben dürfen.

Hinzu kam, dass keine konkret begründete, über dem Durchschnitt liegende Gefahr für die Begehung der befürchteten Delikte bestand. Eine bloße Behauptung oder die allgemeine Vermutung, dass Rechtsverletzungen zu erwarten sind, verleiht dem Interesse des Verantwortlichen kein höheres Gewicht. Auch der Hinweis, dass sich das Gelände in einer Grenzregion befinde, genügte nicht, um eine Gefährdungslage anzunehmen.

Aufseiten der Betroffenen war zu berücksichtigen, dass sie anlasslos erfasst wurden, ihre Bilddaten durch die Speicherung für eine weitere Aufbereitung, Auswertung und Verknüpfung mit anderen Informationen zur Verfügung standen und sie so einem Missbrauchsrisiko ausgesetzt waren. Eine Videoüberwachung ist ein erheblicher Eingriff in die Rechte der betroffenen Personen, wenn diese hierfür keinen ihnen zurechenbaren Anlass, etwa durch Rechtsverletzung, geschaffen haben, sondern als Unbeteiligte mitbetroffen sind. Die Mieterinnen und Mieter des im Erfassungsbereich liegenden Wohnhauses hatten zudem keine Ausweichmöglichkeit und gerieten zwangsläufig in den Erfassungsbereich der Videokameras, ohne sich diesem entziehen zu können.

Im Ergebnis war das Betreiberinteresse bei fast allen Kameras in der Abwägung geringer zu bewerten, als das Interesse der betroffenen Personen, nicht ungewollt Objekt einer Videoüberwachung zu werden.

Hiervon ausgenommen waren allerdings zwei Kameras, mit denen ein großflächiges Wandgemälde, welches dem Gewerbezentrum als Wahrzeichen diente, vor Schmierereien geschützt werden sollte. Da ein konkreter Vorfall nachgewiesen werden konnte und im unmittelbaren Bereich des Gemäldes kaum Personen von der Videoüberwachung betroffen waren, konnte sie auf die Rechtsgrundlage des Arti-

kel 6 Absatz 1 Buchstabe f DS-GVO gestützt werden und war damit erlaubt. Auch die Videokameras, die unmittelbar um die Diskothek das Gelände aus unterschiedlichen Perspektiven filmten, waren nach aktuellen Gewaltvorfällen, die weitere schwere körperliche Auseinandersetzungen befürchten ließen, wegen des überwiegenden Interesses des Verantwortlichen zulässig – allerdings nur während der Öffnungszeiten der Diskothek.

Um die unzulässigen Datenverarbeitungen zu unterbinden, machte die Landesbeauftragte von ihrer Befugnis gemäß Artikel 58 Absatz 2 Buchstabe f DS-GVO Gebrauch, die es ihr als Aufsichtsbehörde gestattet, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen.

Den Betrieb der Kameras, die u. a. das Wohnhaus, ein Bistro, die Fleischerei und Parkplätze erfassten, untersagte die Landesbeauftragte komplett und verpflichtete den Betreiber, dies durch geeignete Maßnahmen sicherzustellen. In Frage kommt hierfür neben einem mechanischen Abdecken der Objektive vor allem der Abbau der Geräte. Bezogen auf die Kameras, die das Wandgemälde filmten, daneben jedoch auch großflächig Parkplätze und Hausfassaden erfassten, wurde dem Verantwortlichen aufgegeben, den Erfassungsbereich auf die unmittelbare Umgebung des Wandgemäldes zu beschränken. In Bezug auf die Kameras, die nach den Gewaltvorfällen der Diskothek zum Einsatz kamen, verpflichtete die Landesbeauftragte die Hausverwaltung, den Betrieb außerhalb der Öffnungszeiten des Clubs zu unterlassen.

Gegen den Bescheid hat der Verantwortliche Klage eingereicht. Die gerichtliche Entscheidung steht noch aus.

6 Videoüberwachung in einem Indoorspielplatz für Kinder

Um in einem Indoorspielplatz für Schutz vor Diebstählen und Einbrüchen zu sorgen, filmte der Verantwortliche mit acht Videokameras vor allem Arbeitsplätze von Beschäftigten sowie die Gastronomiebereiche. Daneben sollten die Kameras der Sicherheit der Kinder dienen. Jedoch erfasste nur eine Kamera einen Bereich, der den Kindern zum Spielen vorbehalten war. Die Bilder wurden zwar gespeichert, aber nicht vom Personal in Echtzeit beobachtet.

Um auch in schwer einsehbaren Bereichen eine Aufsicht zu ermöglichen, kann der Einsatz einer Videokamera grundsätzlich zulässig sein. Das setzt jedoch voraus, dass die Videobilder in Echtzeit gesichtet werden, um bei Gefahr sofort eingreifen zu können. Eine Bildspeicherung ist für diesen Zweck hingegen nicht erforderlich.

Bei den Kameras, die vornehmlich Mitarbeiterinnen und Mitarbeiter an ihrem Arbeitsplatz sowie die Areale mit Gastronomiebetrieb filmten, war sowohl bei den betroffenen Beschäftigten als auch bei den mit Giro- oder Kreditkarte an den Theken bezahlenden Personen und den sich im Barbereich aufhaltenden Gästen von einem nicht unerheblich schweren Eingriff in ihre Datenschutzrechte auszugehen. Demgegenüber war das Interesse des Verantwortlichen an den Videobildern durch keine erheblich über das allgemeine Lebensrisiko hinausgehende Gefährdungslage begründet und daher als gering zu bewerten. Im Ergebnis konnte die Videoüberwachung nicht auf die Rechtsgrundlage des Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) gestützt werden.

Gemäß Artikel 58 Absatz 2 Buchstabe f DS-GVO untersagte die Landesbeauftragte den Betrieb aller Kameras zu Zeiten, in denen der Indoorspielplatz für Gäste geöffnet ist. Ausgenommen war eine Kamera, die einen schwer einsehbaren Bereich im Spielplatzangebot filmte. Bei dieser wurde lediglich die Bildspeicherung untersagt. Damit bleibt es dem Verantwortlichen unbenommen, eine Echtzeitbeobachtung zu Aufsichtszwecken vorzunehmen.

Daneben ordnete die Landesbeauftragte gemäß Artikel 58 Absatz 2 Buchstabe d DS-GVO an, dass der Verantwortliche eine elektronische Protokollierung aller Zugriffe auf das Kamerasystem einzurichten hat. Nach Artikel 5 Absatz 2 DS-GVO ist der Verantwortliche für die Einhaltung der in Artikel 5 Absatz 1 DS-GVO normierten Grundsätze verantwortlich. Dazu gehört auch der Grundsatz der Rechtmäßigkeit der Verarbeitung. Artikel 5 Absatz 2 DS-GVO verlangt außerdem, dass der Verantwortliche die Einhaltung des Grundsatzes nachweisen kann. Eine elektronische Protokollierung aller Zugriffe auf das Kamerasystem ist dafür ein geeignetes Instrument.

Der Verantwortliche ist der Anordnung vollumfänglich nachgekommen und hat dies nachgewiesen.

7 Übersicht über weitere Maßnahmen und Sanktionen

Die Datenschutz-Grundverordnung (DS-GVO) gibt der Landesbeauftragten verschiedene Instrumente an die Hand, mit denen sie Verantwortliche zu einer recht- und ordnungsgemäßen Datenverarbeitung anhalten kann. Sie kann die Verantwortlichen warnen und verwarnen, bestimmte Handlungen oder Unterlassungen erzwingen und eine Datenverarbeitung auch gänzlich verbieten. Ob eine Maßnahme ergriffen wird und, wenn ja, welche, liegt im pflichtgemäßen Ermessen der Landesbeauftragten. Der Grundsatz der Verhältnismäßigkeit ist zu beachten. Er verlangt, dass eine Maßnahme geeignet ist, um das mit ihr bezweckte Ziel zu erreichen. Die Maßnahme muss außerdem in einem angemessenen Verhältnis zum Umfang und Gewicht des festgestellten Verstoßes gegen datenschutzrechtliche Vorschriften stehen und dabei dem Prinzip des mildesten Mittels gerecht werden.

Im Berichtszeitraum hat die Landesbeauftragte in 20 Fällen von den ihr in Artikel 58 Absatz 2 DS-GVO eingeräumten Befugnissen Gebrauch gemacht.[4] Sechs Maßnahmen richteten sich gegen Behörden und sonstige öffentliche Stellen des Landes Brandenburg, 14 Maßnahmen gegen nicht öffentliche Stellen.

Den größten Anteil machten Verwarnungen nach Artikel 58 Absatz 2 Buchstabe b DS-GVO aus. Sie wurden zehnmal ausgesprochen. Mit der Verwarnung wird ein Verstoß gegen Pflichten nach der Datenschutz-Grundverordnung förmlich festgestellt und der Verantwortliche deshalb verwarnt. Weitere Folgen ergeben sich für ihn daraus zunächst nicht; verstößt er jedoch erneut gegen die Datenschutz-Grundverordnung, muss er mit weitergehenden Konsequenzen, insbesondere mit der Einleitung eines Ordnungswidrigkeitenverfahrens rechnen. Verwarnungen wurden u. a. erteilt wegen eines fehlenden Vertrags zur Auftragsverarbeitung, der verspäteten Reaktion auf Auskunftsersuchen und Löschungsbegehren von Betroffenen sowie wegen unzulässiger Übermittlung personenbezogener Daten an Dritte.

Warnungen nach Artikel 58 Absatz 2 Buchstabe a DS-GVO wurden viermal ausgesprochen. In diesen Fällen hat ein Verstoß gegen Da-

4 Die Einleitung von Bußgeldverfahren bleibt hierbei außer Betracht, siehe A I 8.

tenschutzvorschriften noch nicht stattgefunden, die entsprechende Datenverarbeitung ist jedoch beabsichtigt. Wie bei der Verwarnung ergeben sich für den jeweiligen Verantwortlichen aus der Warnung noch keine unmittelbaren Folgen. Nimmt er die Datenverarbeitung jedoch trotz der Warnung auf, muss er mit einem Bußgeldverfahren rechnen, da von einem vorsätzlichen Handeln in Kenntnis der Rechtswidrigkeit auszugehen ist.

Die Landesbeauftragte hat insgesamt sechs Anordnungen erlassen. In drei Fällen wurde die Überwachung mit Videokameras nach Artikel 58 Absatz 2 Buchstabe f DS-GVO teilweise untersagt.[5] In einem Fall erhielt ein Unternehmen gemäß Artikel 58 Absatz 2 Buchstabe c DS-GVO die Anweisung, einem Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen; zweimal wies die Landesbeauftragte gemäß Artikel 58 Absatz 2 Buchstabe d DS-GVO Verantwortliche an, Bearbeitungsvorgänge auf bestimmte Weise und innerhalb einer bestimmten Frist mit der Datenschutz-Grundverordnung in Einklang zu bringen. Dies betraf die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten und das Einstellen einer Datenschutzerklärung auf der Webseite eines Verantwortlichen.

Insgesamt lässt sich feststellen, dass die Datenschutzverletzungen, von denen wir durch Beschwerden Betroffener, Anfragen der Verantwortlichen oder Prüfungen erfahren, nicht zwingend Maßnahmen und Sanktionen der Aufsichtsbehörde nach sich ziehen. Vielfach führt bereits ein erstes Anhörungsschreiben an den Verantwortlichen dazu, dass er einen Verstoß umgehend abstellt, oder, falls dieser nicht mehr rückgängig gemacht werden kann, Einsicht zeigt und uns die von ihm getroffenen Vorkehrungen darlegt, mit denen er zukünftige Verstöße unterbindet.

8 Bericht der Bußgeldstelle

Im diesjährigen Berichtszeitraum führten wir Ordnungswidrigkeitenverfahren wegen datenschutzrechtlicher Verstöße sowohl gegen nicht öffentliche Stellen als auch gegen Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen durch. In 11 Fällen schlossen wir das Verfahren mit der Festsetzung einer Geldbuße ab. Im Wesentlichen kam hierbei noch die alte Rechtslage zur Anwendung, da die begangenen Ordnungswidrigkeiten zumeist vor dem 25. Mai 2018 beendet worden waren. Wir befassten uns unter anderem mit unzulässigen

5 siehe u. a. A I 5 und 6

Videoüberwachungen, nicht ordnungsgemäß abgeschlossenen Auftrags(daten)verarbeitungsverträgen nach alter und neuer Rechtslage und dem mangelhaften Umgang mit Patienten- und Mitarbeiterdaten.

Unabhängig von den folgenden drei exemplarisch aufgeführten Fällen waren auch in diesem Berichtszeitraum mehrere unbefugte Abrufe aus dienstlich genutzten Datenbanken durch Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen (insbesondere durch Polizeibedienstete) zu verzeichnen. An dieser Stelle sei erneut darauf hingewiesen, dass ein solcher Abruf nur gestattet ist, wenn eine dienstliche Notwendigkeit vorliegt. Private Gründe können eine solche Abfrage nicht rechtfertigen und werden als Ordnungswidrigkeit verfolgt.

8.1 Videoüberwachung im Schwimmbad

Der Betreiber eines Schwimmbads verstieß gegen datenschutzrechtliche Vorgaben, indem er im Schwimmbad in unzulässiger Weise mittels Videokameras die sich darin aufhaltenden Personen (u.a. Gäste, Mitarbeiterinnen und Mitarbeiter) filmte und die Aufnahmen speicherte. Darüber hinaus unterließ er es über mehrere Jahre, eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten zu bestellen und versäumte den rechtzeitigen Abschluss eines ordnungsgemäßen Auftragsverarbeitungsvertrages mit dem Dienstleistungsunternehmen, das mit der Wartung der Videoüberwachungsanlage beauftragt war.

Gäste und Beschäftigte unter Beobachtung

Jeder der genannten Sachverhalte stellte einen eigenständigen Verstoß gegen das zum damaligen Zeitpunkt anwendbare Bundesdatenschutzgesetz (BDSG) dar. Bezüglich der Videoüberwachung handelt ordnungswidrig, wer nach § 43 Absatz 2 Nummer 1 BDSG (vorsätzlich oder fahrlässig) unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Davon ist das Filmen und anschließende Speichern der Aufnahmen umfasst. Unbefugt ist die Datenerhebung bzw. -verarbeitung dann, wenn sie weder auf eine Einwilligung der betroffenen Personen noch auf eine andere Rechtsgrundlage gestützt werden kann. Eine Einwilligung in die Videoüberwachung lag nicht vor. Die jeweils in Betracht kommenden Rechtsgrundlagen waren größtenteils schon deswegen nicht einschlägig, weil es an der Erforderlichkeit der Videoüberwa-

chung zu den vom Betreiber angeführten Zwecken fehlte. Darüber hinaus überwogen die Interessen der betroffenen Personen, beim Besuch des Schwimmbades oder bei der Verrichtung ihrer Arbeitstätigkeiten mittels Videokameras nicht gefilmt zu werden. Der Betreiber erkannte dies unter Außerachtlassung der erforderlichen Sorgfalt nicht. Er hätte sich allerdings vor der Installation der Videokameras rechtlichen Rat über deren Zulässigkeit einholen können. Insofern beging er die Ordnungswidrigkeit fahrlässig.

Darüber hinaus unterließ er es fahrlässig, rechtzeitig eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten für das Schwimmbad zu bestellen, obwohl diese Verpflichtung gesetzlich verankert ist. Schließlich versäumte es der Betreiber ebenfalls fahrlässig, mit dem mit der Wartung der Videoüberwachungsanlage betrauten Dienstleistungsunternehmen einen ordnungsgemäßen Vertrag zur Auftragsdatenverarbeitung abzuschließen. Ein solcher ist immer dann erforderlich, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden. Hierzu gehört auch der Einsatz eines Dienstleistungsunternehmens, das Wartungen vornimmt und bei dem nicht ausgeschlossen werden kann, dass es auf personenbezogene Daten zugreift. Der Abschluss eines Vertrages unterblieb im vorliegenden Fall. Die Landesbeauftragte verhängte in der Summe für alle genannten Verstöße ein Bußgeld in Höhe von 12.000 Euro.

8.2 Erteilung von Auskünften unter fremdem Logo

Ein Unternehmen verstieß gegen das in der Datenschutz-Grundverordnung (DS-GVO) festgelegte Gebot, einen Auftragsverarbeitungsvertrag schriftlich abzuschließen, obwohl es im Rahmen der Auskunftserteilung nach Artikel 15 DS-GVO einen Dienstleister einsetzte, der Zugriff auf die für die Auskunftserteilung notwendigen personenbezogenen Daten der Antragstellerinnen und Antragsteller hatte. Die Korrespondenz im Rahmen der Auskunftserteilung wurde unter dem Logo des Dienstleisters durchgeführt. Die Antragstellerinnen und Antragsteller wussten nicht, dass es sich hierbei um den Dienstleister des Unternehmens handelte. Insofern konnten sie nicht erkennen, wer der Verantwortliche der Datenverarbeitung war. Das Unternehmen kontaktierte die betroffenen Personen nach Antragstellung zur Auskunftserteilung zunächst nur in englischer Sprache.

Nach Artikel 28 Absatz 9 DS-GVO ist der Vertrag zur Auftragsverarbeitung schriftlich zu schließen. Die Regelung verfolgt damit Dokumentations-, Beweissicherungs- und Authentizitätssicherungszwecke. Die Schriftform soll sicherstellen, dass die Parteien, die in dem Dokument genannt sind, sich zu den eingegangenen Verpflichtungen mit dem konkreten Inhalt bekennen. Es wird insofern auf eine höhere Rechtssicherheit abgezielt. Nach Artikel 83 Absatz 4 Buchstabe a DS-GVO wird bei einem Verstoß gegen das Gebot, einen Auftragsverarbeitungsvertrag schriftlich abzuschließen, eine Geldbuße von bis zu 10 Millionen Euro oder im Falle eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem welcher der Beträge höher ist. Das Unternehmen führte diesen Verstoß fahrlässig herbei.

Artikel 83 Absatz 5 DS-GVO eröffnet einen noch höheren Bußgeldrahmen für Verstöße, die in seinem Katalog aufgeführt sind. Danach werden Geldbußen von bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher der Beträge höher ist. Hiervon umfasst sind Verstöße gegen die Rechte der betroffenen Person gemäß Artikel 12 DS-GVO. Diese Norm verpflichtet den Verantwortlichen, geeignete Maßnahmen zu treffen, um der betroffenen Person zum Beispiel alle Mitteilungen gemäß dem Artikel 15 DS-GVO (also im Rahmen der Auskunftserteilung) in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln. Das Unternehmen hat dadurch, dass es die Antragstellerinnen und Antragsteller nicht darüber aufklärte, dass es sich bei dem eingesetzten Dienstleister um einen Auftragsverarbeiter handelte und dass, trotz Erteilung der Auskunft unter dem Logo des Dienstleisters, das Unternehmen selbst für die Datenverarbeitung verantwortlich blieb, gegen den in Artikel 12 DS-GVO niedergelegten Transparenzgrundsatz verstoßen. Die Regelung soll sicherstellen, dass die Datenverarbeitung der personenbezogenen Daten des Betroffenen, etwaige Risiken, Garantien und Betroffenenrechte sowie die Aufklärung des Betroffenen, wie er bestehende Rechte geltend machen kann, für den Betroffenen verständlich dargestellt werden. Nur wenn dies geschieht, kann dem Grundsatz der Datenhoheit jeder einzelnen Person Rechnung getragen werden.

Auskunftserteilung nur in verständlicher Form

Gleichzeitig hat das Unternehmen dadurch, dass es die Antragstellerinnen und Antragsteller zunächst in englischer Sprache kontaktierte, gegen den in Art. 12 DS-GVO niedergelegten Grundsatz der Verständlichkeit verstoßen. Wenn sich ein Unternehmen mit seinem Angebot an den deutschsprachigen Markt richtet, muss die Auskunftserteilung (zumindest auch) auf Deutsch erfolgen.

Wegen der genannten Verstöße verhängte die Landesbeauftragte ein Bußgeld in der Gesamtsumme von 50.000 Euro. Hierbei wurde insbesondere die Kooperation des Unternehmens im Bußgeldverfahren mildernd berücksichtigt.

8.3 Sicherung von Patientendaten als Freundschaftsdienst

Ein Mediziner beauftragte einen Bekannten mit der Sicherung der personenbezogenen Daten, die in seiner Arztpraxis anfielen. Davon waren sowohl die Daten von Patientinnen und Patienten als auch von Mitarbeiterinnen und Mitarbeitern umfasst. Der Bekannte speicherte die zu sichernden Daten auf einem Computer an seinem Arbeitsplatz in einem Unternehmen, wo sie vom Arbeitgeber entdeckt wurden. Der Mediziner war für die (unbeabsichtigte) Offenlegung der Daten aus seiner Praxis an den Arbeitgeber seines Bekannten verantwortlich.

Zwar ist es grundsätzlich erlaubt, die Datensicherung, die dem Mediziner ansonsten selbst obliegen würde, an einen Dienstleister auszulagern. Bei einem Auftragsdatenverarbeitungsverhältnis behält der Auftraggeber im Außenverhältnis aber die volle datenschutzrechtliche Verantwortlichkeit für den Umgang mit den personenbezogenen Daten. Der Auftragnehmer ist sozusagen nur der „verlängerte Arm“ des Auftraggebers. Sein Handeln wird dem Auftraggeber zugeordnet. Er ist deshalb unter anderem verpflichtet, sich während der Datenverarbeitung durch den Auftragnehmer regelmäßig über die weisungsgemäße Ausführung des Auftrages und die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Bloßes Vertrauen, dass der Auftragnehmer mit den ihm überlassenen Daten ordnungsgemäß umgehen wird, ist nicht ausreichend. Bei Beachtung der erforderlichen Sorgfalt hätte der Mediziner den Umfang seiner Pflichten als Auftraggeber erkennen und die unbefugte Datenübermittlung an den Arbeitgeber seines Bekannten vermeiden können. Die Landesbeauftragte verhängte gegen den Mediziner ein Bußgeld in vierstelliger Höhe.

II Anlasslose Prüfungen

1 Facebook-Fanpages öffentlicher Stellen

Im letzten Tätigkeitsbericht[6] hatten wir ein Urteil des Europäischen Gerichtshofs[7] vorgestellt, nach dem Betreiberinnen und Betreiber sogenannter Facebook-Fanpages grundsätzlich im Wege der gemeinsamen Verantwortung gemäß Artikel 26 Datenschutz-Grundverordnung eine Mitverantwortung für beim Betrieb anfallende Datenverarbeitungsprozesse tragen. Weiterhin haben wir die zahlreichen rechtlichen und praktischen Probleme aufgezeigt, denen der Betrieb einer Facebook-Präsenz aus datenschutzrechtlicher Sicht begegnet. Wir hatten angemahnt, dass Betreiberinnen und Betreiber von Facebook-Seiten zu prüfen haben, ob der Betrieb dieser Seite unter den Bedingungen der gemeinsamen Verantwortung gerechtfertigt werden kann. Außerdem hatten wir nach Veröffentlichung der Entscheidung im Juni 2018 die Ministerien des Landes Brandenburg über das Urteil informiert und auf die rechtlichen Konsequenzen im Zusammenhang mit der Unterhaltung einer Fanpage hingewiesen. Auch baten wir darum, die jeweils nachgeordneten Behörden entsprechend zu informieren.

Im Berichtsjahr haben wir damit begonnen, unter Berücksichtigung der sich weiterentwickelnden Rechtsprechung und der Hinweise der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) zu prüfen, ob die Anforderungen an den Fanpage-Betrieb bei öffentlichen Stellen des Landes eingehalten werden. Zu diesem Zweck haben wir im Rahmen unserer Kontrollbefugnisse eine Reihe von Behörden, von denen wir annahmen, dass sie eine Fanpage betreiben, angeschrieben.

Eine Stelle konnte glaubhaft darlegen, dass die über sie existierende Facebook-Seite nicht von ihr selbst, sondern von einem interessierten Dritten eingerichtet wurde. Diese Seite blieb im Weiteren unberücksichtigt. Nicht berücksichtigt haben wir ferner von Facebook automatisch generierte Dossiers zu weiteren Behörden, da insoweit deren Verantwortlichkeit nicht gegeben ist. Ebenfalls nicht Gegenstand der Untersuchung waren Facebook-Seiten einzelner Amts- oder Mandatsträgerinnen und -träger, die diese als natürliche Personen betreiben.

6 Tätigkeitsbericht Datenschutz 2018, IV. 1.

7 Urteil des Europäischen Gerichtshofs vom 5. Juni 2018, C-210/16.

Mittels eines Fragebogens forderten wir die Verantwortlichen auf darzulegen, wie sie nach dem Stand der Rechtsprechung ihre Pflichten aus der gemeinsamen Verantwortung wahrzunehmen beabsichtigen, auf welcher Rechtsgrundlage die Datenverarbeitung vorgenommen wird und welche Abreden sie mit Facebook über die Verteilung der zu erfüllenden Pflichten getroffen haben.

Die Auswertung der Stellungnahmen wird indes noch Zeit in Anspruch nehmen, da inzwischen neue Rechtsprechung vorliegt, welche sich zwar nicht unmittelbar mit Fanpages beschäftigt, aber dennoch Einfluss auf den Umfang der Pflichten der Betreiberinnen und Betreiber haben kann. So hat der Europäische Gerichtshof in einem Urteil[8] seine Ausführungen zum Rechtsinstitut der gemeinsamen Verantwortung präzisiert. Der Sachverhalt des vorliegenden Urteils und der unserer Prüfung zugrunde liegende sind allerdings nicht vollständig vergleichbar. Denn im aktuellen Urteil ist Streitgegenstand nur ein auf einer Webseite eingebundenes sog. Social Plugin (auch "Facebook-Button"). Dennoch lassen sich einzelne Überlegungen des Gerichts auch auf Fanpagebetreiberinnen und -betreiber übertragen. Hierzu läuft die Klärung innerhalb der Gremien der Datenschutzkonferenz, an der wir uns aktiv beteiligen.

Facebook-Fanpages weiter in der Diskussion

Wir sind jenseits der bereits im Tätigkeitsbericht Datenschutz 2018 benannten rechtlichen Einzelfragen überzeugt, dass öffentliche Stellen aufgrund ihrer besonderen Bindung an Recht und Gesetz die Nutzerinnen und Nutzer, die sich über ihre Tätigkeit informieren wollen, nicht in die Lage bringen sollten, ihre Daten an Facebook übermitteln zu müssen. Es ist daran zu erinnern, dass – wie etliche Nachprüfungen verschiedenster in- und ausländischer Stellen klar ergeben haben – die Verarbeitungspraxis von Facebook bewusst intransparent organisiert ist. Das derzeitige Geschäftsmodell des Unternehmens schließt es grundsätzlich aus, die Übermittlung von Nutzerdaten zur Verarbeitung durch Facebook zu Werbezwecken sowie diese Verarbeitung selbst in Einklang mit dem geltenden europäischen Recht zu bringen. An einem solchen System sollten sich – ganz abgesehen von allen Einzelfragen, die sich aus der gemeinsamen Verantwortung ergeben – öffentliche Stellen mit ihrer Vorbildfunktion nicht beteiligen.

8 Urteil des Europäischen Gerichtshofs vom 29. Juli 2019, C-40/17.

2 Nutzung der Schul-Cloud in zwei Pilotschulen

Bereits in unserem vorletzten Tätigkeitsbericht[9] informierten wir ausführlich über unsere Beratungen anlässlich der Einführung von Online-Lernplattformen an Schulen sowie über die rechtlichen Voraussetzungen. Im Rahmen eines vom Bundesministerium für Bildung und Forschung geförderten Projekts entwickelt das Hasso-Plattner-Institut in Potsdam eine solche cloudbasierte Lernplattform (Schul-Cloud). Die erste bundesweite Pilotphase beschränkte sich auf MINT-EC-Schulen. MINT-EC ist das nationale Excellence-Netzwerk von Schulen mit Sekundarstufe II und ausgeprägtem Profil in Mathematik, Informatik, Naturwissenschaften und Technik (MINT). Von den brandenburgischen MINT-EC-Schulen nehmen bisher fünf Gymnasien an diesem Pilotprojekt teil.

Neben dieser bundesweiten Schul-Cloud existiert in Brandenburg inzwischen eine landesspezifische Variante, an der sich mit Beginn des Schuljahres 2019/2020 insgesamt 50 Schulen beteiligen. Beide Installationen verwenden dieselbe Software. Bei der brandenburgischen Variante fanden vorläufige landesspezifische datenschutzrechtliche Anpassungen statt, die u. a. die Einwilligung Minderjähriger und das Freigabeverfahren betrafen. So muss bei minderjährigen Schülerinnen und Schülern sichergestellt sein, dass bis zu deren Volljährigkeit zusätzlich auch die Eltern einwilligen.

Die beabsichtigte Teilnahme zahlreicher weiterer Pilotschulen zum Schuljahr 2019/2020 veranlasste uns, die Umsetzung der technischen und organisatorischen Maßnahmen beim Einsatz einer solchen Schul-Cloud stichprobenartig vor Ort zu prüfen. Wir wählten zwei Gymnasien aus, die die MINT-EC-Cloud nutzen. Die rechtlichen Anforderungen (wie z. B. das Einwilligungserfordernis der Eltern bei minderjährigen Schülerinnen und Schülern in Brandenburg) konnten hier nicht vollständig eingehalten werden, weil es sich bei dieser Version um eine bundesweite Anwendung handelt. Im Ergebnis unserer Prüfung ist vorgesehen, sämtliche MINT-EC-Schulen des Landes in die brandenburgische Variante der Schul-Cloud zu übernehmen.

9 Tätigkeitsbericht 2016/2017, B 13.1.1.

In Zusammenarbeit mit der Landesbeauftragten hat das Hasso-Plattner-Institut den teilnehmenden Schulen Muster aller erforderlichen datenschutzrechtlichen Unterlagen zur Nutzung der Schul-Cloud (Einwilligungserklärungen, Vertrag zur Auftragsdatenverarbeitung nach Artikel 28 Datenschutz-Grundverordnung, Verzeichnis der Verarbeitungstätigkeiten etc.) zur Verfügung gestellt. Diese Muster waren durch die Schulleitungen schulspezifisch zu ergänzen und anzupassen. Darüber hinaus mussten sie die Verträge mit dem Hasso-Plattner-Institut schließen und die Freigabe für das Verfahren nach dem Brandenburgischen Datenschutzgesetz erklären.

Lernplattformen in Schulen auf dem Vormarsch

Im Ergebnis unserer Prüfungen stellten wir fest, dass die Anforderungen an eine ordnungsgemäße Dokumentation zwar grundsätzlich erfüllt waren, jedoch die notwendigen, individuellen datenschutzrechtlichen Umsetzungsschritte durch die Verantwortlichen teilweise unterblieben sind. Den Schulen konnte nicht zugutegehalten werden, dass sich das Projekt noch in der Pilotphase befindet, denn die datenschutzrechtlichen Anforderungen sind bereits vor der ersten Nutzung zu erfüllen.

Kritisch sahen wir auch den so genannten „Lernstore“ der Schul-Cloud, der auf externe Anbieterinnen und Anbieter von Lerninhalten weiterleitet, die jedoch nicht in jedem Fall selbst die datenschutzrechtlichen Anforderungen einhalten. Wir haben das Hasso-Plattner-Institut aufgefordert, diese Verweise zu deaktivieren. Zukünftig sollen nur solche externen Angebote freigeschaltet werden, die vom Ministerium für Bildung, Jugend und Sport freigegeben wurden.

Die Datenverarbeitung für die Nutzung der Schul-Cloud basiert zurzeit auf einer freiwilligen Einwilligung der Schülerinnen und Schüler bzw. ihrer Eltern. Diese ist jedoch jederzeit widerruflich, mit der Folge, dass die betroffenen Kinder und Jugendlichen die Plattform nicht mehr nutzen dürften. Wir hatten deshalb mehrfach angeregt, eine Rechtsvorschrift im Brandenburgischen Schulgesetz zu verankern, um eine rechtssichere Befugnisnorm für die Datenverarbeitung im Kontext von Online-Lernplattformen zu schaffen.

3 Veröffentlichung personenbezogener Daten im Rahmen der Kommunal- und Landtagswahl

Im letzten Tätigkeitsbericht[10] haben wir über eine durch uns angeregte Entschließung des Landtages vom April 2018 berichtet. Darin wird die Landesregierung aufgefordert, die Landes- und Kommunalwahlverordnung dahingehend zu ändern, in öffentlichen Wahlbekanntmachungen nicht mehr die vollständige Anschrift der Wahlbewerberin oder des Wahlbewerbers, sondern nur noch deren bzw. dessen – unzweifelhaft auch für die Wahlentscheidung relevanter – Wohnort anzugeben. Dieser Aufforderung ist die Landesregierung mit Erlass zweier Verordnungen[11] gefolgt.

Die Kommunalwahlen am 26. Mai 2019 sowie – in weit geringerem Maße – die Landtagswahl am 1. September 2019 brachten dennoch eine große Anzahl von Beschwerden, Anzeigen und Hinweisen bei der Landesbeauftragten mit sich. Sie betrafen ganz überwiegend die Frage, welche personenbezogenen Daten der Kandidatinnen und Kandidaten von der Internet-Veröffentlichung nach § 98a Brandenburgisches Kommunalwahlgesetz umfasst sind.

Zunächst erhielten wir in erheblichem Umfang Meldungen von Landkreisen, kreisfreien Städten, Ämtern und Gemeinden nach Artikel 33 Datenschutz-Grundverordnung, dass Internet-Veröffentlichungen von Wahlbewerberdaten entgegen den neuen Vorschriften erfolgt waren. Daneben erreichten uns Beschwerden von Kandidatinnen und Kandidaten und Anzeigen aus der Bevölkerung zum selben Problem. Soweit gegen die neuen Vorschriften zur Veröffentlichung der Anschrift von Wahlbewerberinnen und -bewerbern verstoßen wurde, beriefen sich die Gemeinden darauf, dass sie von der Änderung der Vorschriften noch keine Kenntnis hatten. Die von der Landesregierung im Zuge der Änderungen versandten Rundschreiben waren offenbar nicht überall zur Kenntnis genommen worden.

10 Tätigkeitsbericht Datenschutz 2018, V 1.5.

11 Dritte Verordnung zur Änderung der Brandenburgischen Kommunalwahlverordnung vom 26. Oktober 2018 (GVBl. II Nr. 71), Zweite Verordnung zur Änderung landeswahlrechtlicher Vorschriften vom 22. März 2019 (GVBl. II Nr. 23).

Wir nahmen die hohe und kaum handhabbare Anzahl von Meldungen, Beschwerden und Anzeigen sowie den Umstand, dass die fehlerhaften Veröffentlichungen offenkundig ganz überwiegend darauf beruhten, dass die Verantwortlichen sich der geänderten Vorschriften nicht bewusst waren, zum Anlass, eine Umfrage unter den Gemeinden mit der Bitte um Prüfung durchzuführen. Wir gingen – wie sich herausstellte, zu Recht – davon aus, dass Gemeinden, die wir auf die Problematik hinweisen, einen möglichen eigenen Fehler in angemessener Zeit selbst korrigieren.

Nach den Kommunalwahlen erhielten wir Beschwerden von Personen, die einen Wahleinspruch geltend gemacht hatten, aber nicht namentlich in den Veröffentlichungen der Gemeinde genannt werden wollten. Zuständig für die Prüfung von Wahleinsprüchen ist die Gemeindevertretung, die darüber in öffentlicher Sitzung entscheidet.

Gemäß § 36 Absatz 4 Brandenburgische Kommunalverfassung (BbgKVerf) hat jeder das Recht, Beschlussvorlagen der in öffentlichen Sitzungen zu behandelnden Tagesordnungspunkte einzusehen. Gemäß Satz 2 der Vorschrift kann die Hauptsatzung „das Nähere regeln“ – also auch bestimmen, dass diese vor der Sitzung online zur Verfügung stehen.

Datensparsamkeit auch im Rahmen von Wahlen

Wir vertreten die Auffassung, dass insbesondere bei der Veröffentlichung von Beschlussvorlagen im Internet Vorsicht geboten ist. Das verwendete Formular sollte nur insoweit personenbezogene Daten enthalten, wie dies zur Vorbereitung auf die Sitzung und das Verständnis des Vorgangs erforderlich ist. Dies umfasst unzweifelhaft Gegenstand und Begründung der Beschwerde, regelmäßig aber nicht ihre Urheberin oder ihren Urheber. Einen Anspruch auf Einblick in Anlagen zu den Beschlussvorlagen – z. B. in die ungeschwärzten Originalschreiben von Einspruchsführenden – durch die Öffentlichkeit vermittelt § 36 Absatz 4 BbgKVerf nach unserer Überzeugung nicht. Dies lässt die Befugnis zur Einsicht in alle personenbezogenen Daten durch mit der Vorlage befasste Mitglieder der Gemeindevertretungen sowie die Gemeindeverwaltung im Rahmen der Erforderlichkeit zur Aufgabenerfüllung selbstverständlich unberührt.

§ 39 Absatz 3 BbgKVerf bestimmt, dass Beschlüsse der Gemeindevertretung oder deren wesentlicher Inhalt in ortsüblicher Weise der Öffentlichkeit zugänglich zu machen sind. Eine Online-Veröffentlichung – auch im öffentlich zugänglichen Teil eines Ratsinformationssystems – ist unbestritten möglich und im Sinne der Transparenz auch zu begrüßen. Auch insoweit sollte jedoch kritisch geprüft werden, ob Namen und sonstige personenbezogene Daten von Einspruchsführenden wirklich zum wesentlichen Inhalt des Beschlusses gehören. Aus hiesiger Erfahrung ist dies bei Wahleinsprüchen regelmäßig zu verneinen, da grundsätzlich Gründe für den Einspruch geltend gemacht werden, die auch andere Bürgerinnen und Bürger hätten vorbringen können. Dies gilt besonders für die den Wahleinsprüchen oft zu entnehmenden weiteren Kontaktdaten. Selbst wenn es ausnahmsweise auf den Namen der einspruchsführenden Person ankommen sollte, wäre in der Sitzung, in der über den Einspruch entschieden wird, in Betracht zu ziehen, ob zur Wahrung der Rechte eine Namensnennung trotzdem unterbleiben muss.

In beiden Phasen der Veröffentlichung, also vor und nach einer Wahl, ist es somit notwendig, dass die Verantwortlichen das Gebot der Erforderlichkeit einer Veröffentlichung für das Verständnis des Sachverhalts im Auge behalten.

4 Überprüfung der Datenschutzinformationen in ausgewählten Arztpraxen

Veranlasst durch zahlreiche Anfragen von Medizinerinnen und Medizinern, die sich nach Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) erkundigten, wie sie ihre Informationspflichten als Verantwortliche erfüllen sollen[12], baten wir ausgewählte Praxen in den kreisfreien Städten, uns ein Exemplar ihrer Datenschutzinformation nach Artikel 13, 14 DS-GVO für ihre Patientinnen und Patienten zu überlassen.

Etwa die Hälfte der vorgelegten Unterlagen erfüllte die Anforderungen der Datenschutz-Grundverordnung. Meist nutzten diese Arztpraxen Musterformulare. Soweit wir bei den Datenschutzinformationen Verbesserungsbedarf erkannten, bestand dieser z. B. darin, dass unzureichende Informationen mit Einwilligungserklärungen

12 Tätigkeitsbericht Datenschutz 2018, I 2.4.

vermischt wurden. Aufgrund unserer Beratung wurden beide Formulare entsprechend den gesetzlichen Anforderungen separat gefasst.

Mehrfach sahen die Datenschutzinformationen vor, dass Behandelte diesen zustimmen oder sie als „gelesen und verstanden“ bestätigen sollten. Wir wirkten auf das Streichen solcher Erklärungen bzw. Bestätigungen hin, da die Patientinnen und Patienten nicht verpflichtet sind, die Informationen zur Kenntnis zu nehmen oder ihnen zuzustimmen.

Ein Informationsblatt benannte als Datenschutzaufsichtsbehörde die eines anderen Bundeslandes. Aufgrund unseres Hinweises wurde die Angabe geändert.

Am Rande der Prüfung stellten wir fest, dass gelegentlich Einwilligungen in die Speicherung oder Verarbeitung der Daten zu Behandlungs- oder Abrechnungszwecken erbeten wurden. Wir wiesen darauf hin, dass die zivilrechtliche Dokumentationspflicht der Medizinerinnen und Mediziner unabhängig vom Willen der Patientin oder des Patienten besteht. Bereits die Datenschutz-Grundverordnung sieht eine datenschutzrechtliche Befugnis für die Verarbeitung zu Behandlungszwecken grundsätzlich vor. Auch regelt das Sozialgesetzbuch – jedenfalls bei gesetzlich Versicherten – die Übermittlungen zu Abrechnungszwecken. Insgesamt konnten wir anlässlich unserer Umfrage die Praxisinhaberinnen und -inhaber sensibilisieren zu prüfen, in welchen Fällen eine Einwilligungserklärung oder Entbindung von der ärztlichen Schweigepflicht tatsächlich notwendig ist.

5 Umfrage bei Unternehmen zu Datenschutz-Management und Personaldatenverarbeitung

Große Industrieunternehmen im Land sind bezogen auf die Anzahl ihrer Mitarbeiterinnen und Mitarbeiter hinsichtlich der bei uns eingehenden Beschwerden zur Verarbeitung personenbezogener Daten der Beschäftigten deutlich unterrepräsentiert. Wir haben deshalb im Berichtszeitraum eine Umfrage unter derartigen Unternehmen durchgeführt, um uns einen Eindruck von der dortigen Umsetzung der Anforderungen der Datenschutz-Grundverordnung (DS-GVO) zu verschaffen. Wir wählten stichprobenartig insgesamt 15 Unternehmen aus, die auf den Internetseiten des Wirtschaftsministeriums und der Wirtschaftsförderung Brandenburg GmbH als „Leuchttürme“ im

Land benannt werden. Sie entstammen den Branchen Bergbau und Kraftwerke, metallerzeugende und metallverarbeitende Industrie, Turbinentechnik, Fahrzeugbau, chemische und optische Industrie. Insgesamt arbeiten in den ausgewählten Unternehmen über 28.000 Beschäftigte.

Alle Beteiligten erhielten einen Fragebogen zum Datenschutz-Management und zur Personaldatenverarbeitung im Unternehmen. In insgesamt sechs Themenkomplexen sollten sie sich z. B. zum Datenschutzbeauftragten, zur Datenschutzorganisation, zur Sensibilisierung von Beschäftigten für den Datenschutz, zu den eingesetzten (automatisierten) Verfahren der Personalverwaltung, der Lohn- und Gehaltszahlung sowie der Zeitwirtschaft, zu technischen und organisatorischen Maßnahmen im Unternehmen sowie zur Auftragsverarbeitung äußern. Wir baten darüber hinaus um Auszüge aus dem Verzeichnis der Verarbeitungstätigkeiten zur Personaldatenverarbeitung sowie um eine Kopie der Informationen für Beschäftigte nach Artikel 13 DS-GVO.

Große Unternehmen gut aufgestellt?

Zwei Drittel der Unternehmen antworteten innerhalb der gesetzten Frist von vier Wochen. Nach einer weiteren Woche lagen uns 80 % der Antworten vor. In einem Unternehmen war unser Schreiben mit dem Fragebogen zunächst verloren gegangen – die Antwort erreichte uns nach 12 Wochen. In einem weiteren Fall trug das Unternehmen vor, als reiner Produktionsstandort keine eigenen Entscheidungen zu Mitteln und Zwecken der Verarbeitung personenbezogener Daten zu treffen und verwies auf die Konzernzentrale in einem anderen Bundesland. Wir besprachen den Sachverhalt mit den Kollegen der dortigen Datenschutzbehörde und stimmten zu, die Fragen konzernweit und zentral unter deren Aufsicht zu klären.

Alle Unternehmen hatten eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten benannt. In etwa einem Drittel der Fälle war sie bzw. er im Unternehmen selbst beschäftigt, bei einem weiteren Drittel in einem anderen Unternehmen der Gruppe bzw. des Konzerns angestellt. Die verbleibenden Unternehmen hatten einen externen Dienstleister vertraglich gebunden, um die Funktion der bzw. des Datenschutzbeauftragten auszulagern. Alle befragten Unternehmen veröffentlichten entsprechend der gesetzlichen Vorschriften die Kontaktdaten ihrer Beauftragten.

Circa die Hälfte der benannten Datenschutzbeauftragten hatte eine juristische Berufsausbildung, die andere Hälfte entweder einen technischen oder einen betriebswirtschaftlichen Hintergrund. Alle Beauftragten besuchten Datenschutzfortbildungen, zum Teil erwarben sie ein Zertifikat. Ein Drittel von ihnen führte im Unternehmen oder in der Unternehmensgruppe auch andere Aufgaben aus; Interessenskonflikte waren für uns dabei jedoch nicht offensichtlich.

Positiv hervorzuheben ist, dass es in allen befragten Unternehmen zentrale Richtlinien zum Datenschutz, zur Einbeziehung der bzw. des Datenschutzbeauftragten sowie zum Umgang mit Auskunfts-, Berichtigungs- und Löschansprüchen Betroffener gab. Die ganz überwiegende Zahl hatte auch einheitliche Vorgaben zum Verhalten bei Verletzungen des Datenschutzes und zur Erfüllung der Melde- und Informationspflichten nach Artikel 33 bzw. 34 DS-GVO. Circa 80 % der Unternehmen gab an, Beschäftigte regelmäßig in Fragen des Datenschutzes zu sensibilisieren.

Alle Unternehmen, die an der Umfrage teilnahmen, verarbeiten die Personalstammdaten, die Lohn- und Gehaltsdaten sowie die Daten der Zeiterfassung automatisiert. Lediglich in einem Fall werden die Personalakten noch in Papierform geführt, ansonsten dominiert die elektronische Personalakte. Im Hinblick auf die vorgelegten Auszüge aus den Verzeichnissen der Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO ist festzustellen, dass die Mehrzahl der Unternehmen sich darin nur auf die unbedingt erforderlichen Informationen beschränkte und auch deren Granularität recht grob war, insbesondere bezüglich der Kategorien der verarbeiteten Daten. Empfänger von Daten wurden oftmals nur exemplarisch angegeben; Löschfristen für Daten lediglich pauschal benannt und nicht mit konkreten Zeitangaben hinterlegt. Gleiches beobachteten wir bei den Informationen für Beschäftigte nach Artikel 13 DS-GVO. Hier kam ergänzend hinzu, dass in Einzelfällen die Rechtsgrundlagen der Datenverarbeitung nicht konkret benannt oder die Rechte Betroffener nach Artikel 15 ff. DS-GVO ungenügend erläutert wurden. Ein Unternehmen legte mehr Wert auf die ausführliche Darstellung der Ausnahmen, in denen Betroffene keine Ansprüche gegen den verantwortlichen Datenverarbeiter haben, als auf die Rechte selbst.

Einzelne Unternehmen hatten es versäumt, die Auszüge aus dem Verzeichnis der Verarbeitungstätigkeiten für die Personaldatenverarbeitung sowie die diesbezüglichen Informationen für Beschäftigte beizulegen, obwohl sie angaben, dass entsprechende Unterlagen vorliegen. Wir werden insoweit um eine Ergänzung der Antworten bitten.

Hinsichtlich der technischen und organisatorischen Maßnahmen, die in den befragten Unternehmen bei der Personaldatenverarbeitung umgesetzt werden, interessierten uns insbesondere Mechanismen der Authentisierung von Benutzern, Rollen- und Rechtekonzepte, die Protokollierung von Zugriffen und die Vorkehrungen für die Datensicherung. Die ganz überwiegende Zahl der Unternehmen gab in diesen Punkten zufriedenstellend Auskunft – die aufgeführten Maßnahmen waren angemessen und geeignet, die Risiken der Datenverarbeitung zu beherrschen. Lediglich in Bezug auf die Verschlüsselung personenbezogener Daten mussten wir in ungefähr der Hälfte der Unternehmen Nachholbedarf feststellen: Mehrfach wurde angegeben, auf die Verschlüsselung zu verzichten, obwohl Beschäftigtendaten an die Konzernzentrale oder an externe Dienstleister übertragen wurden. Nur 57 % der Unternehmen verschlüsselte personenbezogene Daten auch im internen Datennetz.

Im Ergebnis unserer Umfrage ist festzustellen, dass die beteiligten Unternehmen grundsätzlich die Anforderungen der DS-GVO erfüllen. Einige haben Mängel selbst festgestellt und diese bereits behoben oder sich realistische Ziele für die Beseitigung gesetzt. In einzelnen Fällen werden wir auf die Unternehmen erneut zugehen, um Unterlagen nachzufordern bzw. spezielle Defizite aufarbeiten zu lassen. Auffällig ist, dass diejenigen Unternehmen, die Teil einer Unternehmensgruppe sind, von Synergieeffekten durch zentrale Vorgaben, Dokumente und Umsetzungen technischer oder organisatorischer Maßnahmen erheblich profitieren. Bei allen Beteiligten der Umfrage behalten wir uns eine Kontrolle vor Ort vor.

III Ausgewählte Fälle

1 Ermittlungen eines Jobcenters in der Nachbarschaft

Aufgrund einer Beschwerde wurden wir darauf aufmerksam, dass das Jobcenter Ostprignitz-Ruppin zur Klärung des Bestehens einer Bedarfsgemeinschaft Zeugenfragebögen an mehrere Nachbarinnen und Nachbarn versandt hat. Die Beschwerdeführenden leben getrennt und sind Eltern gemeinsamer Kinder. Die Beschwerdeführerin bezieht Sozialleistungen. In dem entsprechenden Zeugenfragebogen wurden neben deren Namen auch die vollständigen Namen der gemeinsamen Kinder genannt. Eine besondere Brisanz erhielt das Vorgehen des Jobcenters dadurch, dass mehr als ein Dutzend Personen aus beiden Wohnorten der Eltern in dem Fragebogen dazu aufgefordert wurden, teilweise intime Fragen aus deren Privatleben zu beantworten; beispielsweise, ob das Schlafzimmer gemeinsam genutzt werde. Eine vor Versendung des Fragebogens durchgeführte Überprüfung durch den Bedarfsermittlungsdienst ergab, dass keine Bedarfsgemeinschaft besteht. Das Jobcenter begründete seine weitergehenden Ermittlungen damit, dass es im Rahmen des dazugehörigen anhängigen Gerichtsverfahrens vom Gericht aufgefordert worden war, die Nachbarinnen und Nachbarn zu befragen.

Ob eine Bedarfsgemeinschaft besteht und dementsprechend die daran anknüpfenden Voraussetzungen einer Leistungsgewährung vorliegen, unterliegt durchaus der staatlichen Prüfung. Sofern dem Jobcenter konkrete Anhaltspunkte für das Bestehen einer Bedarfsgemeinschaft vorliegen, ist es berechtigt, eine weitergehende Aufklärung zu betreiben. Allerdings ist die Befugnis des Jobcenters zur Ermittlung nicht grenzenlos.

Die Erhebung personenbezogener Daten mittels Zeugenfragebögen muss mit Blick auf den Grundsatz der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c Datenschutz-Grundverordnung (DS-GVO) auf das erforderliche Maß begrenzt sein. Das bedeutet, dass jede einzelne angeforderte Information über die betroffene Person für das Jobcenter im Rahmen der Leistungsbewilligung unerlässlich sein muss. Auch die Übermittlung personenbezogener Daten der Beschwerdeführerin und des Beschwerdeführers an Dritte muss wegen des Sozialgeheimnisses nach § 35 Erstes Buch Sozialgesetzbuch (SGB I) auf das Erforderliche beschränkt bleiben. Das Jobcenter hat diese Grenze erheblich überschritten.

Die Vorgehensweise, zahlreiche Personen in mehreren Wohnorten und mehreren Hausaufgängen zu befragen, vermittelte uns den Eindruck, dass das Jobcenter Personen in der Nachbarschaft der Beschwerdeführerin und des Beschwerdeführers nicht gezielt für eine Zeugenbefragung ausgewählt hat, sondern eher wahllos möglichst viele Informationen zum Vorliegen einer Bedarfsgemeinschaft erhalten wollte.

Das Jobcenter hat keine ausreichende datenschutzrechtliche Abwägung vor Versendung der Zeugenfragebögen vorgenommen. Denn unabhängig von richterlichen Vorgaben hat es bei seiner Prüfungspflicht die Grenzen der Erforderlichkeit zu wahren. Auch die Übermittlung von personenbezogenen Daten der gemeinsamen Kinder war zur Klärung der Frage des Vorliegens einer Bedarfsgemeinschaft nicht erforderlich, zumal gerade Kinder nach der Datenschutz-Grundverordnung zu einem besonders schützenswerten Personenkreis zählen.

Daher erfolgte die Befragung sämtlicher Nachbarinnen und Nachbarn durch das Jobcenter nicht zielgerichtet, sondern „ins Blaue hinein“ und würde bei einer in gleicher Weise durchgeführten Zeugenbefragung wegen der Anzahl der befragten Personen und des Umfangs der erfragten und übermittelten Informationen aus datenschutzrechtlicher Sicht voraussichtlich als unzulässig zu bewerten sein. Aufgrund der festgestellten Mängel beabsichtigt die Landesbeauftragte, gegenüber dem Jobcenter eine Warnung nach Artikel 58 Absatz 2 Buchstabe a DS-GVO auszusprechen, um das Jobcenter damit aufzufordern, künftig von seiner üblichen Praxis Abstand zu nehmen. Zum Zeitpunkt des Redaktionsschlusses dieses Berichts war das Verfahren noch nicht abgeschlossen.

2 Arbeitsteilung zwischen Ausländerbehörde und privatem Wachschutz

Durch eine Beschwerde haben wir erfahren, dass in der Ausländerbehörde des Landkreises Potsdam-Mittelmark personenbezogene Daten von Ausländerinnen und Ausländern durch Beschäftigte des vor Ort vom Landkreis eingesetzten privaten Wachschutzunternehmens vermutlich ohne rechtliche Befugnis verarbeitet wurden. Eine daraufhin durchgeführte unangekündigte Vor-Ort-Prüfung hat den Inhalt dieser Vermutung bestätigt. Wir stellten fest, dass Mitarbeiterinnen und Mitarbeiter des Wachschutzunternehmens bereits vor

dem Eingang eine Art „Einlasskontrolle“ durchführten, Kundinnen und Kunden aufforderten, ihre Ausweise vorzuzeigen und anschließend Wartenummern ausgaben. Auch im Wartebereich verlangte der Wachschutz beständig Ausweispapiere zur Ansicht. Er ging auf Anliegen der Kundinnen und Kunden ein und beantwortete Fragen.

In einem Fall konnten wir eine fachliche Beratung durch einen Wachschutzmitarbeiter unmittelbar mitverfolgen, bei welcher er Auskunft über die Unzuständigkeit der hiesigen Ausländerbehörde erteilte und stattdessen die für das Anliegen der Kundin zuständige Behörde nannte. Wir konnten ebenfalls beobachten, wie der Wachschutz mehrfach persönliche Unterlagen an sich nahm, um diese zu kopieren und minutenlang damit verschwand.

Wiederholt war auch zu beobachten, dass Beschäftigte des Wachschutzunternehmens die zuvor erhaltenen Dokumente den jeweils zuständigen Sachbearbeiterinnen und Sachbearbeitern übergaben. Diese routiniert wirkende Interaktion zwischen Wachschutz und Ausländerbehörde zeigte, wie eng die Arbeitsabläufe verknüpft waren. In einer anschließenden Stellungnahme teilte uns die Ausländerbehörde zudem mit, dass sie über die datenschutzrechtlichen Missstände in Form der unzulässigen Datenverarbeitung durch das private Unternehmen bereits informiert gewesen sei.

Der uns vorgelegte Vertrag zwischen dem Landkreis und dem Wachschutzunternehmen belegte endgültig, dass das Unternehmen keinerlei Befugnisse im Bereich der Datenverarbeitung besitzt. Es soll lediglich die Sicherheit in der Ausländerbehörde gewährleisten. Der Vertrag enthielt keine Regelung, welche die Beschäftigten des Wachschutzes zur Verarbeitung personenbezogener Daten der Kundinnen und Kunden in der Ausländerbehörde berechtigen würde. Sie obliegt ausschließlich den jeweils zuständigen Sachbearbeiterinnen und Sachbearbeitern.

Die Beschäftigten des Wachschutzes haben ihre vertraglich festgelegten Kompetenzen mit Wissen der Ausländerbehörde weit überschritten. Dementsprechend waren dieses arbeitsteilige Vorgehen sowie dessen Duldung durch den Landkreis aus datenschutzrechtlicher Sicht unzulässig. Im Ergebnis beabsichtigt die Landesbeauftragte, den Landkreis deswegen nach Artikel 58 Absatz 2 Buchstabe b Datenschutz-Grundverordnung zu verwarnen. Zum Zeitpunkt des

Redaktionsschlusses dieses Berichts befindet sich das Verfahren in der Phase der Anhörung.

3 Aushang von Unterschriftenlisten im Schaukasten

Zu Beginn des Berichtsjahres informierte uns eine Bürgerin, im Bereich der Amtsverwaltung Britz-Chorin-Oderberg finde eine Auseinandersetzung zwischen der Verwaltung und einzelnen Bürgerinnen und Bürgern um das Schicksal einer gemeindlichen Immobilie statt. Die Beschwerdeführerin hatte gemeinsam mit anderen in dieser Sache eine Stellungnahme verfasst, zu deren Unterstützung Namen und Unterschriften Gleichgesinnter gesammelt und Stellungnahme sowie Unterschriftenliste in der Amtsverwaltung abgegeben. Die Verwaltung hatte daraufhin eine Entgegnung verfasst und mit dieser auch die Stellungnahme der Beschwerdeführerin nebst Unterschriftenliste im Mitteilungskasten des betroffenen Ortsteils veröffentlicht. Auf Drängen der Initiatorinnen und Initiatoren der Stellungahme und nach einem Bericht in einer Lokalzeitung wurde die Veröffentlichung der Unterschriftenliste nach wenigen Tagen wieder zurückgenommen.

Wir baten das Amt um Auskunft, insbesondere um Bestätigung oder Korrektur des Sachverhalts. In der Sache legten wir dar, dass das Amt zwar ein umfassendes Mandat gemäß § 13 Brandenburgische Kommunalverfassung (BbgKVerf) hat, die Bevölkerung effektiv über wichtige Gemeindeangelegenheiten zu informieren. Wir bezweifelten jedoch, dass der Aushang der Unterschriftenliste erforderlich war. Zwar handelt es sich bei einer Unterschriftenkampagne, den mit ihr verfolgten Zielen und dem Zuspruch, den sie erhalten hat, ohne Weiteres um eine wichtige Gemeindeangelegenheit. Jedoch genügt zur Information über den Umfang der Unterstützung durch die Bürgerinnen und Bürger regelmäßig die Angabe der Gesamtzahl der (validen) Unterschriften ohne Namensnennung.

Aus der Antwort des Amtes wurde deutlich, dass die Veröffentlichung ursprünglich – bis zu ihrer Rücknahme – auf eine Einwilligung nach Artikel 6 Absatz 1 Buchstabe a und Artikel 7 Datenschutz-Grundverordnung (DS-GVO) gestützt werden sollte. Die Unterschreibenden hätten dadurch, dass sie unbestritten offensiv, z. B. durch Medienkontakte, in die Öffentlichkeit getreten seien und das Amt ausdrücklich zu einer Stellungnahme bewegen wollten, signalisiert,

dass sie offenbar gegenüber den Initiatorinnen und Initiatoren auch ein Einverständnis oder gar den Wunsch geäußert hätten, dass ihre Daten im Schaukasten veröffentlicht werden. Aus den vorliegenden Materialien ergab sich ein Hinweis auf eine solche Willenserklärung indes nicht. Das Amt sah das eigene Handeln in der Rückschau selbst kritisch.

In Ermangelung einer gesetzlichen Rechtsgrundlage kann aus konkludentem Verhalten nicht auf das Vorliegen einer Einwilligung geschlossen werden. Eine solche bedarf vielmehr einer aktiven Handlung. Der bloße, auch erkennbare und aktive Wille dazu, das mit einer Unterschriftenliste verfolgte Sachthema in der Öffentlichkeit zu halten, ist nicht ausreichend für eine Einwilligung in die Veröffentlichung personenbezogener Daten. Da das Amt allerdings bereits im Antwortschreiben zu erkennen gegeben hatte, dass Unterschriftenlisten in Zukunft datenschutzkonform behandelt werden und der Aushang nur für verhältnismäßig kurze Zeit erfolgt war, sahen wir von Maßnahmen ab und baten lediglich abschließend um Mitteilung, wie in Zukunft mit gleichgelagerten Fällen umgegangen wird. Das Amt teilte daraufhin mit, dass Petitionen nur noch in der Form veröffentlicht würden, dass die Anzahl der Unterschreibenden und ggf. der Grad ihrer Betroffenheit (z. B. „Anwohner“) erkennbar sein werde. Für ein weitergehende Veröffentlichungen, soweit sie nicht anderweitig gesetzlich vorgesehen sind, würden in Zukunft informierte Einwilligungen eingeholt.

4 Übermittlung von E-Mail-Adressen durch Versandhändler an Postdienstleister

Im Rahmen der Abwicklung von Online-Bestellungen werden E-Mail-Adressen zunächst für die allgemeine Kommunikation mit den Kundinnen und Kunden verwendet, beispielsweise um Bestellbestätigungen, Rechnungen und nicht zuletzt Versandbestätigungen elektronisch versenden zu können. Darüber hinaus übermitteln einige Händlerinnen und Händler die zur Verfügung gestellte E-Mail-Adresse jedoch auch an das mit dem Versand beauftragte Postdienstleistungsunternehmen. Dies erfolgt regelmäßig mit dem Ziel, Kundinnen und Kunden detailliertere Informationen über den Sendungsverlauf und das avisierte Zustelldatum zur Verfügung stellen zu können. Zu der Übermittlung der E-Mail-Adressen erreichten uns im Berichtszeitraum wiederholt Beschwerden.

Wie jede Verarbeitung personenbezogener Daten erfordert auch eine solche Übermittlung der E-Mail-Adresse eine Rechtsgrundlage, zumal dem Postdienstleistungsunternehmen in diesen Fällen nicht nur diese, sondern auch Name und Anschrift der Empfängerin oder des Empfängers vorliegen. Die Verantwortlichen argumentierten regelmäßig, dass die Information über den Sendungsstatus auch im Interesse der Empfängerinnen und Empfänger liege, etwa um den Erhalt der Sendung am Tag der Zustellung entsprechend organisieren zu können. Verkannt wird dabei jedoch, dass die Zustellinformation auch unmittelbar durch den Onlinehandel selbst weitergegeben bzw. ein Link zur Sendungsverfolgung in die Versandbestätigung eingebunden werden kann. Dies stellt eine objektiv zumutbare Alternative zur Übermittlung an das zustellende Unternehmen dar, weshalb es bereits an der Erforderlichkeit der Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen fehlt. Die Übermittlung kann insoweit nicht auf Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung gestützt werden. Sofern die Kundin oder der Kunde eine derartige Übermittlung wünscht, kommt als Rechtsgrundlage nur eine vorherige, informierte Einwilligung in Betracht.

Eine Übermittlung ohne tragfähige Rechtsgrundlage stellt dagegen einen bußgeldbewährten Verstoß dar. Über die Einleitung eines Ordnungswidrigkeitenverfahrens entscheidet die Bußgeldstelle im jeweiligen Einzelfall.

5 Verbreitung von Schadsoftware und Umleitung von E-Mails durch mangelhafte Pflege eines Webservers

Die Software Drupal ist ein quelltextoffenes Content Management System (CMS) zur Erstellung und Pflege von Websites. Ende März 2018 wiesen die Entwicklerinnen und Entwickler auf eine kritische Sicherheitslücke in ihrer Software hin, stellten Updates bereit und empfahlen Verantwortlichen, ihre Installationen möglichst schnell zu aktualisieren. Betroffen waren laut Mitteilung mehr als eine Million Websites weltweit. Die Sicherheitslücke ermöglichte es Angreifenden, mit geringem Aufwand Schadcode in eine Drupal-Installation einzuschleusen, die gesamte Website und das zu Grunde liegende Serversystem zu kompromittieren, Daten von dort auszulesen, zu modifizieren oder zu löschen. Sie war derart schwerwiegend, dass sogar für sehr alte Softwareversionen, die oftmals noch im Einsatz waren, ein Update bereitgestellt wurde.

Drupalgeddon und Crypto-Jacking durch Webauftritt

Im November 2018 meldete uns ein brandenburgisches Unternehmen eine Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) – eine so genannte Datenpanne. Die auf dem CMS Drupal basierende Website des Unternehmens wurde derart kompromittiert, dass einerseits Daten der Nutzerinnen und Nutzer (z. B. Anmeldungen für Veranstaltungen) sowie administrative Daten (z. B. zur Pflege der Website) ausgelesen werden konnten. Weiterhin war eine unbefugte Modifikation der Serverkonfiguration aufgefallen, wodurch ausgehende E-Mails über andere Systeme umgeleitet wurden. Andererseits gelang es im Zuge des Angriffs, die Website so zu verändern, dass bei jedem Besuch automatisch eine Schadsoftware heruntergeladen und ausgeführt wurde. Diese Schadsoftware zweckentfremdete die Computer der Nutzerinnen bzw. Nutzer, indem sie diese für komplizierte Berechnungen im Kontext digitaler Währungen (das so genannte Schürfen oder Crypto Mining) missbrauchte.

Festzustellen waren insoweit also Verletzungen bzw. zumindest erhebliche Gefährdungen der Vertraulichkeit, Integrität und Verfügbarkeit bei der Verarbeitung personenbezogener Daten über die Webpräsenz des Unternehmens. Für Besucherinnen und Besucher der Website kam hinzu, dass durch das unbefugte Schürfen digitaler Währungen deren physikalische Ressourcen widerrechtlich genutzt wurden und es zu einem erheblichen Verlust an Leistungen bzw. zu einem dauerhaften Ausfall von Hardware hätte kommen können.

Bereits in der Meldung der Datenpanne teilte das Unternehmen mit, dass vermutlich ein versäumtes Softwareupdate Ursache des Vorfalls gewesen ist. Auf unsere Nachfrage hin stellte sich heraus, dass der mit der Wartung beauftragte externe IT-Dienstleister das CMS Drupal bereits seit Anfang 2017 nicht mehr aktualisiert hatte. Nach Auslaufen des damaligen Vertrages Ende 2017 wurde die Website durch das Unternehmen weiter angeboten, ohne jedoch für eine technische Pflege der zu Grunde liegenden Software zu sorgen. Erst Ende Oktober 2018 änderte sich die Situation mit der Verpflichtung eines neuen Dienstleisters, der die erforderlichen Aktualisierungen durchführte. Ein Vertrag zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO wurde mit der neuen Wartungsfirma erst nachträglich auf

unsere explizite Aufforderung hin geschlossen, zum Zeitpunkt der Datenschutzverletzung existierte ein solcher nicht.

Zusammenfassend ist festzuhalten, dass die Ursache der Verletzung des Schutzes personenbezogener Daten in der mangelnden Sorgfalt des Unternehmens beim Betrieb der Website und bei der Gestaltung der Auftragsverarbeitung lag. Als Verantwortlicher hätte es u. a. technische und organisatorische Maßnahmen gemäß Artikel 32 DS-GVO entweder selbst umsetzen oder eine Dienstleisterin bzw. einen Dienstleister damit beauftragen und die Auftragsausführung kontrollieren müssen. Wegen der Verstöße gegen mehrere Vorschriften der Datenschutz-Grundverordnung wurde der Sachverhalt an die Bußgeldstelle abgegeben, die ihrerseits ein Ordnungswidrigkeitenverfahren gegen das Unternehmen einleitete.

6 Zwischen Schein und Sein – ein Datenschutzverein mit Datenschutzmängeln?

Im ersten Quartal des Berichtsjahres erreichte uns eine Reihe von Beschwerden und Hinweisen aus dem ganzen Bundesgebiet, insbesondere von kleinen Unternehmen, Einzelhandelskaufleuten und Privatpersonen. Diese wurden von einem Verein mit Sitz im Land Brandenburg abgemahnt, weil sie auf ihren Webseiten zwar personenbezogene Daten verarbeiteten (z. B. über Kontaktformulare), jedoch keine hinreichenden Maßnahmen zur Verschlüsselung dieser Daten bei der Übertragung über das Internet umgesetzt hatten. Der Verein, dessen Ziel gemäß seiner Satzung u. a. die Wahrung von Verbraucherinteressen war, prüfte die Webauftritte, ermittelte aus dem dort vorhandenen Impressum den jeweiligen Verantwortlichen und mahnte das Verhalten ab. Insbesondere sollten die betroffenen Unternehmerinnen und Unternehmer, Kaufleute und Privatpersonen kurzfristig eine strafbewehrte Unterlassungs- und Verpflichtungserklärung unterzeichnen, die eine Vertragsstrafe in Höhe von 4.000 Euro vorsah, wenn weiter keine verschlüsselte Datenübertragung für die jeweiligen Webseiten installiert werden würde. Darüber hinaus forderte der Verein den Ersatz von entstandenen Kosten in Höhe von 285,60 Euro.

Aus datenschutzrechtlicher Sicht ist zunächst festzuhalten, dass Betreiberinnen und Betreiber von Webauftritten stets personenbezogene Daten verarbeiten und damit als Verantwortliche den Anforde-

rungen der Datenschutz-Grundverordnung (DS-GVO) unterliegen. Artikel 32 Absatz 1 DS-GVO verlangt von jedem Verantwortlichen und ggf. seinen Auftragsverarbeitern die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu erreichen. Hierzu gehört insbesondere eine Verschlüsselung dieser Daten nach dem Stand der Technik – sie wird unter Buchstabe a der genannten Vorschrift explizit als Maßnahme genannt. Insoweit hatte der Verein tatsächlich eine Rechtsverletzung festgestellt.

Wir hatten allerdings die begründete Vermutung, dass bei der Abmahntätigkeit des Vereins weniger die Wahrung von Verbraucherinteressen als vielmehr das „schnelle Geld“ im Vordergrund stand. Genährt wurde diese Vermutung u. a. aus den in den Beschwerden geschilderten Begleitumständen des Agierens des Vereins, Mängeln in seinem eigenen Webauftritt und den fehlenden Informationen für abgemahnte Personen nach Artikel 13 DS-GVO. Wir wollten deshalb prüfen, ob der Verein selbst die Anforderungen der Datenschutz-Grundverordnung einhält. Aufgrund unserer begrenzten Zuständigkeit kümmerten wir uns dabei nur um die Verarbeitung personenbezogener Daten, jedoch nicht um andere Aspekte seiner Tätigkeit.

Zunächst wollten wir uns vor Ort ein Bild von den Verarbeitungstätigkeiten des Vereins machen, fanden jedoch an dessen eingetragenem Sitz nur fast leere Geschäftsräume vor. Auch Mitarbeiterinnen bzw. Mitarbeiter oder Verantwortliche trafen wir nicht an. Die Zustellung unseres ersten Schreibens scheiterte – die Post informierte uns über einen Nachsendeauftrag an eine Adresse in einem anderen Bundesland. Wir leiteten ein förmliches Verwaltungsverfahren gegen den Verein ein und baten zunächst um Auskunft u. a. zu den dortigen Prozessen der Verarbeitung personenbezogener Daten, zu den Informationen nach Artikel 13 DS-GVO für betroffene Abgemahnte, zu Verträgen mit Auftragsverarbeitern sowie zu den umgesetzten technischen und organisatorischen Maßnahmen. Darüber hinaus forderten wir die entsprechenden Dokumente (z. B. die Verträge zur Auftragsverarbeitung nach Artikel 28 DS-GVO sowie das Verzeichnis der Verarbeitungstätigkeiten des Vereins nach Artikel 30 DS-GVO) an.

Die ersten Antworten des Vereins auf unsere Fragen waren jeweils sehr kurz, unvollständig und nicht abschließend. Eine Dokumenta-

tion von technischen und organisatorischen Maßnahmen wurde zunächst genauso wenig übersandt wie ein Verzeichnis der Verarbeitungstätigkeiten. Auch rechtskräftige Verträge zur Auftragsverarbeitung mit dem Internetdienstleister bzw. mit Anbieterinnen und Anbietern von in der Webseite eingebundenen Anwendungen konnten nicht vorgelegt werden. Wir erließen deshalb einen Bescheid, mit dem wir den Verein zu einer vollständigen, abschließenden und aussagekräftigen Auskunft verpflichteten. Nach fruchtlosem Ablauf der Frist zur Beantwortung verhängten wir zusätzlich ein Zwangsgeld, um unsere Forderung durchzusetzen.

Dann ging alles recht schnell: Wir erhielten ein Schreiben vom Verein, das weder die konkrete Urheberin bzw. den konkreten Urheber erkennen ließ, noch eine Unterschrift trug. Es sollte als Antwort auf unseren Auskunftsbescheid zeitlich bereits vor der Verhängung des Zwangsgeldes verschickt worden sein, hatte uns jedoch nicht erreicht. In dem Schreiben hieß es, eine Übersendung der von uns angeforderten Unterlagen könne nicht erfolgen, da die Festplatte, auf der diese gespeichert waren, defekt sei. Gleichzeitig wurde uns mitgeteilt, dass die Vereinsvorsitzenden nicht mehr für den Verein tätig seien. Im Übrigen werde der Verein aufgelöst – dies konnten wir anhand der Einträge im Vereinsregister nachvollziehen.

Wer Datenschutz fordert, sollte ihn auch selbst einhalten

Die datenschutzrechtlichen Mängel in der Vereinstätigkeit waren offensichtlich. Auch der (behauptete) Defekt der Festplatte, auf der wichtige Geschäftsdaten abgelegt gewesen sein sollen, hätte den Verein nicht davon entbunden, seiner Pflicht nach Artikel 5 Absatz 2 DS-GVO zur Dokumentation und zum Nachweis der Einhaltung der Anforderungen der Datenschutz-Grundverordnung nachzukommen – hier hätte es einer Datensicherung (im Zweifel auf Papier) bedurft. Die handelnden Personen entzogen sich durch die Vereinsauflösung jedoch ihrer Verantwortung: Mangels einer Rechtsnachfolge und wegen erheblicher rechtlicher Unsicherheiten im Hinblick auf eine mögliche persönliche Haftung der Vorsitzenden konnten wir weder unsere Forderungen vollstrecken noch ein Ordnungswidrigkeitenverfahren wegen der Rechtsverstöße einleiten. Im Ergebnis bleibt festzustellen: Wir sind zwar nicht in der Lage nachzuweisen, dass unsere obige Vermutung wahr ist; es spricht jedoch einiges dafür.

IV Ausgewählte Beratungen

1 Stellungnahmen zu Gesetzen und anderen Regelungen

1.1 Gesetz zur Änderung des Brandenburgischen Verfassungsschutzgesetzes

Im April 2019 erhielten wir die Gelegenheit, gegenüber dem Ausschuss für Inneres und Kommunales des Landtages Brandenburg eine Stellungnahme zu dem Entwurf für ein Drittes Gesetz zur Änderung des Brandenburgischen Verfassungsschutzgesetzes (BVerfSchG)[13] abzugeben. Ziel der Reform war es, neben der Schaffung eines einheitlichen Rechtsrahmens für die Arbeit der Sicherheitsbehörden Konsequenzen aus den Erkenntnissen der parlamentarischen Untersuchungsausschüsse in Bund und Ländern zur Aufarbeitung der Mordserie des sogenannten „Nationalsozialistischen Untergrunds“ zu ziehen. Zudem galt es, das Gesetz an Vorgaben des Bundesverfassungsgerichts zum Antiterrorgesetz[14] und zum Bundeskriminalamtgesetz[15] anzupassen.

Bereits im Jahr 2018 wurde das Brandenburgische Verfassungsschutzgesetz an die neuen Datenschutzbestimmungen angepasst. Da unsere damaligen datenschutzrechtlichen Hinweise leider nicht vollständig berücksichtigt worden waren, thematisierten wir diese erneut. Darüber hinaus benannten wir eine Reihe von Defiziten, die die Gesetzesnovelle mit sich brachte. Neben zahlreichen weiteren Aspekten, wie beispielsweise die Aufweichung des Zweckbindungsgrundsatzes, sahen wir vor allem folgende Punkte kritisch:

1.1.1 Rechte der Betroffenen

Wer nicht weiß, dass er Ziel verfassungsschutzbehördlicher Maßnahmen war, kann seine Rechte als betroffene Person nicht wahrnehmen. Ohne Kenntnis eines heimlichen Eingriffs, sei es durch Observation, Abhören oder Aufzeichnen, ist auch effektiver Rechtsschutz kaum möglich. Informationspflichten sind damit zentrale Elemente des Datenschutzes, die eine hinreichende Transparenz von Datenverarbeitungsprozessen für die betroffenen Personen gewährleisten

13 Landtags-Drucksache 6/10948 vom 26. März 2019.

14 Urteil des Bundesverfassungsgerichts vom 24. April 2013, 1 BvR 1215/07.

15 Urteil des Bundesverfassungsgerichts vom 20. April 2016, 1 BvR 966/09.

sollen. Nur durch Information können die Bürgerinnen und Bürger Kenntnis darüber erlangen, dass ihre Daten verarbeitet werden. Zudem benötigen sie diese Kenntnis, um (weitere) Betroffenenrechte wirksam ausüben zu können. Insoweit hängt das Anliegen, Datenverarbeitungsprozesse für die betroffene Person hinreichend transparent zu halten, auch eng mit der Rechtsschutzgarantie zusammen.

Fällt der Zweck einer Maßnahme weg oder ist dieser erreicht, sind Betroffene nach unserer Auffassung über diese grundsätzlich zu unterrichten. Mögliche Geheimhaltungsinteressen können allenfalls rechtfertigen, im Einzelfall von einer Benachrichtigung abzusehen, nicht aber Betroffenengruppen hiervon generell auszuklammern. Das Argument des Gesetzgebers, dass eine generelle Informationspflicht mit Blick auf die Ressourcen der Verfassungsschutzbehörde nicht möglich sei, da sie dann ihre operativen Aufgaben nicht mehr wahrnehmen könne, überzeugt in keiner Weise. Die Informationen können durchaus standardisiert vorbereitet und erteilt werden.

Auch haben wir kritisiert, dass der Gesetzentwurf eine Benachrichtigungspflicht lediglich bei Maßnahmen vorsah, die länger als eine Woche oder mehr als 14 Tage innerhalb eines Monats andauern. Leider wurden unsere Bedenken nicht berücksichtigt.

1.1.2 Schutz von Minderjährigen

Der Gesetzentwurf bestimmte, dass personenbezogene Daten von Kindern und Jugendlichen vor Vollendung des 14. Lebensjahrs nicht verarbeitet werden dürfen. Dies sollte jedoch nicht gelten, „soweit minderjährige Personen von der Datenverarbeitung unvermeidbar als Dritte betroffen“ sind. Gegen diese Ausnahmeregelung hatten wir aus mehreren Gründen erhebliche Bedenken. Es war unklar, in welchen Fällen die Kinder „unvermeidbar als Dritte betroffen“ sind. Eine Erläuterung des unbestimmten Rechtsbegriffs ergab sich weder aus dem Normtext selbst noch aus der Gesetzesbegründung. Außerdem wäre es möglich, personenbezogene Daten von Kindern, die das 14. Lebensjahr noch nicht erreicht haben, zu verarbeiten, soweit sie im Zusammenhang mit Straftaten und verfassungsfeindlichen Bestrebungen stehen, obwohl sie nicht selbst Ziel der verfassungsschutzrechtlichen Maßnahmen sind. Damit wären diese Kinder sogar weniger geschützt, als jene, die nicht Dritte sind und für die der Minderjährigenschutz des § 1 Absatz 2 Jugendgerichtsgesetz i. V. m. § 19 Strafgesetzbuch gilt. Unsere Anregung, hier Nachbes-

serungen vorzunehmen, wurde nicht beachtet. Auch unser Hinweis, dass Daten Dritter, insbesondere minderjähriger Dritter grundsätzlich nur in nicht recherchierbarer Form gespeichert werden sollten und dies durch die Normierung entsprechender technischer Maßnahmen zu gewährleisten sei, fand keine Berücksichtigung im weiteren Gesetzgebungsverfahren.

Weiterhin kritisierten wir, dass nach dem Gesetzentwurf die Verarbeitung von personenbezogenen Daten über eine minderjährige Person im Alter von 14 und 15 Jahren zulässig wäre, „wenn nach den Umständen des Einzelfalles nicht ausgeschlossen werden kann, dass die Erhebung zur Abwehr einer Gefahr für Leib oder Leben erforderlich ist." Inwieweit diese Datenerhebung im Zusammenhang mit den Aufgaben der Verfassungsschutzbehörde stehen soll, ist nicht ersichtlich. Nach dem Wortlaut handelt es sich hier um eine Maßnahme der Gefahrenabwehr. Aber weder die operative Gefahrenabwehr noch die Verhütung konkreter Straftaten ist Aufgabe der Verfassungsschutzbehörde. Im Übrigen erschließt sich nicht, weshalb – wie bei anderen Fallvarianten der Norm – nicht wenigstens tatsächliche Anhaltspunkte als Tatbestandsvoraussetzung gewählt wurden, sondern es stattdessen genügen sollte, dass eine Gefahr „nicht ausgeschlossen werden kann." Dies steht zugleich im Widerspruch zu § 3 Absatz 1 Satz 2 BbgVerfSchG, der eindeutig bestimmt, dass das Vorliegen tatsächlicher Anhaltspunkte Voraussetzung für das Tätigwerden der Verfassungsschutzbehörde ist.

1.1.3 Erweiterung der Auskunftspflichten

Künftig sollen unter anderem die Betreiberinnen und Betreiber einer Videoüberwachungsanlage im Sinne des § 4 Absatz 1 Bundesdatenschutzgesetz (BDSG) verpflichtet sein, der Verfassungsschutzbehörde Aufzeichnungen zur Verfügung zu stellen, wenn dies zur Aufklärung von Bestrebungen und Tätigkeiten im Sinne von § 3 Absatz 1 BbgVerfSchG mit erheblicher Bedeutung erforderlich ist.

Nach dem Wortlaut des Gesetzes trifft diese Verpflichtung prinzipiell jeden Verantwortlichen, der öffentlich zugänglichen Raum per Video überwacht. Dies kann im Extremfall dazu führen, dass Privatpersonen, die über ihren Gartenzaun (versehentlich) den öffentlichen Straßenraum (und sei es nur um ein paar Zentimeter) miterfassen, verpflichtet wären, familiäre Aufzeichnungen preiszugeben, die

unter anderen Umständen nicht einmal in den Anwendungsbereich der Datenschutz-Grundverordnung fallen würden. Problematisch ist zudem, dass beispielsweise bei Schwimmbädern (sofern dies großflächige Anlagen im Sinne des § 4 Absatz 1 Satz 2 BDSG sind) auch Aufnahmen herausverlangt werden können, die leicht bis gar nicht bekleidete Personen betreffen. Und all dies würde auch für den Fall gelten, dass die Aufnahmen selbst gegen datenschutzrechtliche Regelungen verstoßen und eigentlich unverzüglich gelöscht werden müssten. Unsere Bedenken wurden im weiteren Gesetzgebungsverfahren nicht berücksichtigt.

Zudem sah die Gesetzesbegründung zwar vor, dass die Verpflichtung auf Betreiberinnen und Betreiber einer Videoüberwachungsanlage von öffentlich zugänglichen großflächigen Anlagen zu beschränken sei, insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, sowie von Fahrzeugen und öffentlich zugänglichen Einrichtungen des öffentlichen Luft-, Schienen-, Schiffs- und Busverkehrs. Aber unserer Empfehlung, diese Klarstellung im Gesetzestext zu verankern und so für die Anwenderinnen und Anwender unmissverständlich zu machen, wurde nicht gefolgt.

1.1.4 Eingeschränkte Aufsichtsbefugnisse der Landesbeauftragten

Unsere datenschutzrechtlichen Aufsichtsbefugnisse sind weiterhin ohne erkennbaren Grund stark eingeschränkt. Zwar kann die Landesbeauftragte gegenüber der Verfassungsschutzbehörde Warnungen und Verwarnungen aussprechen. Sie ist aber beispielsweise nicht befugt, die Verfassungsschutzbehörde anzuweisen, Verarbeitungsvorgänge innerhalb eines bestimmten Zeitraums in Einklang mit den datenschutzrechtlichen Regelungen zu bringen. Ebenso wenig kann sie die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung der Verarbeitung anordnen.

Die Beschränkung unserer Aufsichtsbefugnisse ist nicht nachvollziehbar. Die Begründung, es würden nur die bisherigen Aufsichtsbefugnisse fortgeschrieben, überzeugt hier nicht. Vielmehr sollte die Landesbeauftragte gegenüber der Verfassungsschutzbehörde die gleichen Befugnisse haben wie gegenüber allen anderen Behörden im Land Brandenburg. Denn auch die Verfassungsschutzbehörde ist – wie jede öffentliche Stelle – an Recht und Gesetz gebunden

und verpflichtet, datenschutzrechtliche Regelungen einzuhalten. Dies muss überprüfbar und – sofern notwendig – durchsetzbar sein und entspricht dem allgemeinen gesetzlichen Auftrag der Landesbeauftragten gemäß § 18 Brandenburgisches Datenschutzgesetz. Die Einbindung der Landesbeauftragten ist insbesondere vor dem Hintergrund erforderlich, dass eine Transparenz der Datenverarbeitung sowie individueller Rechtsschutz bei heimlichen Überwachungsmaßnahmen ohnehin nur sehr eingeschränkt sichergestellt werden können. Der Gewährleistung einer effektiven aufsichtsrechtlichen Kontrolle kommt daher umso größere Bedeutung zu. Dies setzt eine mit wirksamen Befugnissen ausgestattete Aufsichtsbehörde voraus.

Zwar gibt es verschiedene Kontrollgremien, die unter anderem die Recht- und Ordnungsmäßigkeit der Tätigkeit der Verfassungsschutzbehörde prüfen. Diese Kontrolltätigkeiten zielen jedoch gerade nicht auf eine speziell datenschutzrechtliche Prüfung der Vorgänge ab. Angesichts der eingeschränkten Betroffenenrechte und der demgegenüber stark ausgeweiteten Befugnisse der Verfassungsschutzbehörde ist eine datenschutzrechtliche Kontrolle zur Wahrung der Rechte der Betroffenen dringend erforderlich.

1.2 eID- und IT-Basiskomponentenverordnung zum Brandenburgischen E-Government-Gesetz

In unserem letzten Tätigkeitsbericht haben wir über die Beteiligung der Landesbeauftragten bei der Erarbeitung des Brandenburgischen E-Government-Gesetzes (BbgEGovG) berichtet.[16] Bereits damals hielten wir es für erforderlich, die Verordnungsermächtigungen des Gesetzes zu nutzen, um konkrete Regelungen zum Datenschutz zu treffen. Mit der eID- und IT-Basiskomponentenverordnung (eIDIT-BV)[17] wurde im Berichtszeitraum ein erstes Ergebnis erzielt. Wie schon beim Brandenburgischen E-Government-Gesetz hat uns das Ministerium des Innern und für Kommunales frühzeitig eingebunden.

Durch die eID- und IT-Basiskomponentenverordnung werden Ausführungsbestimmungen zur elektronischen Identitätsfeststellung in

16 Tätigkeitsbericht Datenschutz 2018, V 1.2.

17 Verordnung über Einzelheiten der elektronischen Identitätsfeststellung und den Einsatz von IT-Basiskomponenten im Land Brandenburg vom 9. Juli 2019 (GVBl. II Nr. 48).

Verwaltungsverfahren gemäß § 3 Absatz 3 BbgEGovG (eID-Service) sowie zum Einsatz von IT-Basiskomponenten gemäß § 11 BbgEGovG getroffen. Dies umfasst auch die Festlegung der Verantwortlichkeiten nach der Datenschutz-Grundverordnung (DS-GVO). § 1 eIDITBV regelt, dass der Brandenburgische IT-Dienstleister für Behörden des Landes in Verwaltungsverfahren, bei denen die Feststellung der Identität der betroffenen Person elektronisch erfolgt, als Diensteanbieter im Sinne des Personalausweisgesetzes tätig wird und im Rahmen der Erfüllung dieser Aufgabe personenbezogene Daten aus dem elektronischen Personalausweis (eID-Funktion) verarbeiten (also auslesen und übermitteln) darf. Er stellt diese Leistungen auch Kommunen und anderen öffentlichen Stellen des Landes zur Verfügung.

In Bezug auf die Bereitstellung von IT-Basiskomponenten gemäß § 11 BbgEGovG (wie z.B. Landesverwaltungsnetz, elektronische Vergabeplattform, virtuelle Poststelle oder elektronische Bezahlplattform) grenzt § 2 eIDITBV die Aufgaben der beteiligten öffentlichen Stellen ab: Der Brandenburgische IT-Dienstleister entscheidet eigenständig über die Einrichtung und den Betrieb der IT-Basiskomponenten. Werden diese von einer Behörde genutzt, ist sie zuständig für die von ihr im Rahmen der Erfüllung einer Fachaufgabe verarbeiteten personenbezogenen Daten. Bei der Umsetzung der datenschutzrechtlichen Pflichten wird die nutzende Behörde vom Brandenburgischen IT-Dienstleister unterstützt. Dies betrifft z. B. die Bereitstellung der Informationen für das Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO, für eine evtl. durchzuführende Datenschutz-Folgenabschätzung gemäß Artikel 35 DS-GVO oder für das IT-Sicherheitskonzept nach Artikel 32 DS-GVO und § 4 Brandenburgisches Datenschutzgesetz. Für die Gewährleistung der Rechte betroffener Personen nach Artikel 12 ff. DS-GVO bleibt in jedem Fall die nutzende Behörde verantwortlich. Dies ist sachgerecht, da sie auch für die Erfüllung der jeweiligen Fachaufgabe zuständig ist. Insgesamt werden somit Festlegungen zur Ausgestaltung der gemeinsamen Verantwortung gemäß Artikel 26 DS-GVO zwischen dem Brandenburgischen IT-Dienstleister und den die IT-Basiskomponenten nutzenden Behörden getroffen und unsere früheren Hinweise aus der Stellungnahme zum Entwurf des Brandenburgischen E-Government-Gesetz berücksichtigt.

E-Government: gemeinsam zum Ziel

Im Rahmen der Bestimmung des Geltungsbereiches der eID- und IT-Basiskomponentenverordnung ergaben sich Fragen hinsichtlich

deren Anwendung für die polizeiliche Gefahrenabwehr, da diese – anders als die Strafverfolgung – nicht aus dem Geltungsbereich des Brandenburgischen E-Government-Gesetzes ausgenommen wurde. Um Widersprüchen zu den für die polizeiliche Datenverarbeitung maßgeblichen datenschutzrechtlichen Regelungen zu entgehen, regten wir nach Rücksprache mit dem Zentraldienst der Polizei eine entsprechende Ausnahmeregelung für die Nutzung von IT-Basiskomponenten im Rahmen der polizeilichen Gefahrenabwehr an. Dem hat der Verordnungsgeber entsprochen.

Mit der eID- und IT-Basiskomponentenverordnung wurden die rechtlichen Regelungen für das Verfahren zum elektronischen Identitätsnachweis sowie für die Einrichtung und Nutzung von IT-Basiskomponenten bei der Erbringung von Verwaltungsdienstleistungen im Land Brandenburg konkretisiert. Der Brandenburgische IT-Dienstleister ist nun gefordert, alle in § 11 Absatz 1 BbgEGovG genannten IT-Basiskomponenten zeitnah bereitzustellen und deren Nutzung durch die öffentlichen Stellen im Land zu ermöglichen.

1.3 Änderung der Meldeordnung der Landesapothekerkammer Brandenburg

Nach dem Heilberufsgesetz (HeilBerG) sind Ärztinnen und Ärzte, Apothekerinnen und Apotheker, Tierärztinnen und Tierärzte sowie Zahnärztinnen und Zahnärzte jeweils in Kammern organisiert. Es handelt sich dabei um Körperschaften des öffentlichen Rechts mit eigenem Satzungsrecht. Die Kammern sind verpflichtet, ein Verzeichnis ihrer Mitglieder zu führen. Die Mitglieder haben ihrerseits die Pflicht, alle für die Erfüllung der Aufgaben der Kammern erforderlichen Angaben zu machen und entsprechende Nachweise zu erbringen. Welche Daten für das Verzeichnis konkret anzugeben sind, regelt § 5 Absatz 2 HeilBerG und ergänzend eine Satzung der jeweiligen Kammer.

Für die Apothekerinnen und Apotheker sind die entsprechenden Ergänzungen in der als Satzung ausgestalteten Meldeordnung der Landesapothekerkammer Brandenburg festgelegt. Das Ministerium für Arbeit, Soziales, Frauen, Familie und Gesundheit gab uns die Gelegenheit, zu einer anstehenden Änderung dieser Meldeordnung Stellung zu nehmen. Hierbei waren uns die folgenden drei Punkte besonders wichtig:

1.3.1 Daten des Heilberufsausweises für das Kammerverzeichnis

Der Satzungsentwurf sah vor, dass die Apothekerinnen und Apotheker Angaben zu ihrem elektronischen Heilberufsausweis wie z. B. die ausstellende Behörde, den Gültigkeitszeitraum und den gewählten qualifizierten Vertrauensdiensteanbieter für das Kammerverzeichnis abzugeben haben. Dies wurde mit der Pflicht der Kammer zur Ausstellung von Heilberufsausweisen und zur Sperrung der Authentifizierungsfunktion des Ausweises beim Wegfall der Berufsausübungsbefugnis begründet.

Hiergegen äußerten wir Bedenken.

Die Verarbeitung von Patientendaten zu Versorgungszwecken mittels elektronischer Gesundheitskarte dürfen nur bestimmte Berufsgruppen vornehmen. Deren Zugriff auf die Karte erfolgt regelmäßig über einen elektronischen Heilberufsausweis, der über eine Möglichkeit zur sicheren Authentifizierung der Ausweisinhaberin bzw. des Ausweisinhabers und über eine qualifizierte elektronische Signatur verfügt. Das Fünfte Buch Sozialgesetzbuch sieht dementsprechend vor, dass in den Ländern Stellen bestimmt werden, die für die Ausgabe des Heilberufsausweises zuständig sind, und Stellen, welche zuvor die Zugehörigkeit zu einer der berechtigten Berufsgruppen bestätigen. Es regelt zugleich Übermittlungsbefugnisse von der für die Bestätigung zuständigen Stelle an die Ausgabestelle und macht damit deutlich, dass insoweit zwei verschiedene Aufgaben bestehen.

Das Kammerverzeichnis führen die Heilberufskammern aufgrund von Landesrecht, um einen Überblick über ihre Mitglieder zu haben. Eine Vermischung dieser rein landesrechtlichen Aufgabe mit den beiden o. g. Aufgaben aus dem Sozialgesetzbuch sahen wir erst recht als problematisch an.

Wir gingen außerdem davon aus, dass der Heilberufsausweis von den Apothekerinnen und Apothekern bei der zuständigen Landesapothekerkammer zu beantragen ist. In diesem Zusammenhang sind alle erforderlichen Angaben zu machen, sodass wir eine weitere, rein vorsorgliche Erhebung dieser Daten für das Kammerverzeichnis für nicht erforderlich hielten.

1.3.2 Angaben zu Beschäftigten

Die Meldeordnung verpflichtete die Kammermitglieder bereits bisher, jährlich personenbezogene Daten zu ihren Beschäftigten zu übermitteln. Wir hatten dies in der Vergangenheit akzeptiert, sofern sich die Kammer auf der Grundlage ihrer allgemeinen Datenerhebungsbefugnis direkt an die betroffenen Personen wandte und für das Kammerverzeichnis ausschließlich Angaben zur eigenen Person verlangte. Dies lässt sich mit der Pflicht zur Führung des Verzeichnisses rechtfertigen, da es gepflegt werden muss und auf aktuellem Stand zu halten ist. Allerdings werden durch die jährlichen Personalmeldungen an die Apothekerkammer überwiegend personenbezogene Daten anderer Personen erhoben, die teilweise nicht einmal selbst der Meldepflicht nach dem Heilberufsgesetz unterliegen. Den unserer Ansicht nach unzulässigen Umfang dieser Personalmeldungen hatten wir schon früher erfolglos gegenüber dem Ministerium kritisiert. Nunmehr bat es uns angesichts der Geltung der Datenschutz-Grundverordnung und Änderungen im Heilberufsgesetz selbst um eine Prüfung dieses Punktes.

Nach der beispielhaften Aufzählung in § 5 Absatz 2 Satz 3 Nr. 2 HeilBerG ist – getrennt nach Berufsgruppen – nur die Zahl der Beschäftigten eines selbstständigen Apothekers mitzuteilen. Zwar kann die Satzung Näheres bestimmen, eine Erweiterung hat sich aber an den im Gesetz genannten Beispielen zu orientieren. Die Angabe der Namen der Beschäftigten halten wir für nicht hinnehmbar, da der Gesetzgeber mit der Wahl des eher statistischen Merkmals „Anzahl der berufsspezifischen Mitarbeiterinnen und Mitarbeiter nach Berufsgruppen“ deutlich gemacht hat, dass es beim Kammerverzeichnis insoweit nicht um konkrete personenbezogene Daten geht. Dies schließt nicht aus, dass die Kammer für andere Zwecke oder Aufgaben als die Führung des Verzeichnisses von den Apothekerinnen und Apothekern personenbezogene Angaben ihrer Beschäftigten erheben darf.

Nach der bislang geltenden Meldeordnung sind sowohl selbstständige als auch angestellte Apothekerinnen und Apotheker meldepflichtig. Durch die jährliche Personalmeldung sind Doppelmeldungen zwangsläufig vorprogrammiert.

Das Verlangen, regelmäßig umfassende Personalmeldungen abzugeben, erweckt den Eindruck, dass angestellten Apothekerinnen

und Apothekern letztlich unterstellt wird, gegen Meldepflichten zu verstoßen. Vorsorgliche Datenerhebungen verletzen aber den datenschutzrechtlichen Grundsatz der Erforderlichkeit. Eine Datenerhebung ist erst dann erforderlich, wenn konkrete Anhaltspunkte für einen Gesetzesverstoß vorliegen. Sollten Verstöße tatsächlich ein bedenkliches Ausmaß annehmen, könnte zum einen der Gesetzgeber nach Abwägung aller Interessen eine regelmäßige Datenerhebung bei anderen Personen oder Stellen und einen Datenabgleich einführen. Eine generelle doppelte Meldepflicht durch Kammermitglieder und ihre Arbeitgeberinnen und Arbeitgeber ist demgegenüber nicht erforderlich und widerspricht dem Grundsatz der Datensparsamkeit.

Darüber hinaus könnte die Landesapothekerkammer Brandenburg in Kenntnis der nach dem Heilberufsgesetz von der Apothekenleitung anzugebenden Zahl der Beschäftigten, die selbst Apothekerinnen oder Apotheker sind, auch prüfen, ob die Meldepflichten als Berufspflicht erfüllt werden. Hierzu ließe sich die Zahl der gemeldeten Beschäftigten mit den Einzelmeldungen der angestellten Apothekerinnen und Apotheker einer Apotheke vergleichen, um ggf. Unstimmigkeiten festzustellen. Eine solche Vorgehensweise würde den Vorgaben im Heilberufsgesetz entsprechen und wäre durch die Datenverarbeitungsbefugnisse der Kammer gedeckt.

1.3.3 Übermittlung von Ausbildungsverträgen

Die geltende Meldeordnung verlangt außerdem, dass bei der Einstellung von Auszubildenden für den Beruf des oder der pharmazeutisch-kaufmännischen Angestellten der Kammer der Ausbildungsvertrag vorzulegen ist. Ebenso wie das Ministerium hatten auch wir Vorbehalte gegen diese Satzungsregelung. Aus dem Berufsbildungsgesetz, einem Bundesgesetz, ergibt sich, dass die Apothekerkammer ein gesondertes Verzeichnis der Berufsausbildungsverhältnisse zu führen hat. Ausbildende und Auszubildende sind danach gesetzlich verpflichtet, die für die Eintragung erforderlichen Tatsachen auf Verlangen der Kammer mitzuteilen. Ausbildende sind nach dem Berufsbildungsgesetz darüber hinaus grundsätzlich verpflichtet, auf Verlangen der Kammer die für die Überwachung notwendigen Auskünfte zu erteilen. Auch enthält das Berufsbildungsgesetz in Verbindung mit der Datenschutz-Grundverordnung ausreichende Rechtsgrundlagen für die Datenverarbeitung. Eine Pflicht zur Vorlage von Ausbildungsverträgen in der Meldeordnung zu regeln, ist folglich nicht notwendig. Hierfür gibt es zudem auch keine Satzungsermächtigung.

Ob unsere Bedenken und Anregungen aufgegriffen werden, bleibt abzuwarten.

2 Beratung im öffentlichen Bereich

2.1 Meldedaten zur Gratulation und ähnlichen Zwecken?

Glückwünsche und Grüße der Verwaltung, insbesondere zu Jubiläen älterer Mitbürgerinnen und Mitbürgern, stellen eine wichtige Quelle des gesellschaftlichen Zusammenhalts in Ortsteilen und kleinen Gemeinden dar. Oft drängt sich bei den kommunalen Verantwortungsträgerinnen und -trägern der Eindruck auf, der Datenschutz stehe diesen kleinen Aufmerksamkeiten entgegen. Im Berichtszeitraum erhielt die Landesbeauftragte – besonders von Ortsvorsteherinnen und Ortsvorstehern sowie ehrenamtlichen Bürgermeisterinnen und Bürgermeistern amtsangehöriger Gemeinden – viele Anfragen zur Verarbeitung von Meldedaten zum Zwecke von Gratulationen, Begrüßungen und Ähnlichem. Wir legen daher im Folgenden unsere ständige Auskunftspraxis zu den rechtlichen Grundlagen, Möglichkeiten und Grenzen der genannten Datenverarbeitung dar.

Herzlichen Glückwunsch! Ihre Bürgermeisterin

In der Regel besteht der Wunsch, Meldedaten zu verarbeiten, um Einwohnerinnen und Einwohnern zu gratulieren. Dabei handelt es sich um Datenverarbeitungsvorgänge, die – wie alle Grundrechtseingriffe – einer Rechtsgrundlage bedürfen. An der Qualität als Eingriff ändert sich auch dann nichts, wenn beabsichtigt ist, den Betroffenen etwas „Gutes“ zu tun – ob die Datenverarbeitung zum Zweck der Gratulation tatsächlich willkommen ist, können letztlich nur die Betroffenen selbst entscheiden.

Für die Gratulation anlässlich Alters- und Ehejubiläen bestehen mehrere gesetzliche Vorschriften:

Gemäß § 50 Absatz 2 Bundesmeldegesetz (BMG) darf die Meldebehörde Mandatsträgerinnen und Mandatsträgern auf Antrag Name und Anschrift von Personen mitteilen, deren Alters- und Ehejubiläen bevorstehen. Als Altersjubiläum gilt jedes volle Jahrfünft ab dem 70. Geburtstag und jeder Geburtstag nach dem vollendeten 100. Lebensjahr. Ehejubiläen sind alle auf das 50. Jubiläum folgenden

Jahrestage. Beantragen Mandatsträgerinnen und Mandatsträger eine solche Datenübermittlung, muss dies in der Regel nicht weiter begründet werden. Ist die betroffene Person mit der Übermittlung nicht einverstanden, kann sie gemäß § 50 Absatz 5 BMG widersprechen.

Neben den Datenübermittlungen auf Antrag besteht die Möglichkeit der automatisierten Übermittlung nach §§ 14 und 15 Absatz 2 Meldedatenübermittlungsverordnung (MeldDÜV). § 14 MeldDÜV nimmt Bezug auf die Definition von Alters- und Ehejubiläen in § 50 Absatz 2 BMG und bestimmt, dass die Landrätinnen und Landräte – bei besonders hohen Jubiläen auch die Staatskanzlei – Meldedaten zu solchen Anlässen automatisiert erhalten, ohne dass dies beantragt werden muss. Gemäß § 15 Absatz 2 MeldDÜV dürfen unter denselben Voraussetzungen Daten auch automatisiert und damit ohne vorheriges Ersuchen den ehrenamtlichen Bürgermeisterinnen und Bürgermeistern sowie Ortsvorsteherinnen und Ortsvorstehern übermittelt werden.

Daneben haben die Bürgermeisterinnen und Bürgermeister amtsangehöriger Gemeinden gemäß § 15 Absatz 1 MeldDÜV Anspruch auf automatisierte Übermittlung von Meldedaten zur Erfüllung wiederkehrender eigener Aufgaben. Schließlich können ganz allgemein innerhalb derselben öffentlichen Stelle (hier: zwischen der Gemeindeverwaltung und einem Ortsteil) gemäß § 37 Absatz 1 in Verbindung mit § 34 Absatz 1 BMG Daten auf Anfrage weitergegeben werden, wenn dies für die Erfüllung der Aufgaben der empfangenden Stelle erforderlich ist.

Nachfolgend gehen wir auf einige Fragen ein, die uns regelmäßig gestellt werden:

- Muss die Meldebehörde personenbezogene Daten auch für Gratulationen zu „nicht runden Geburtstagen“ weitergeben?

Dieses Anliegen fällt nicht unter die oben genannten Vorschriften, die abschließend Anlässe zulässiger Übermittlungen aufführen. § 34 Absatz 1 BMG macht deutlich, dass ein weitergehender Anspruch auf Übermittlung von Meldedaten nur begründet werden kann, wenn sie zur Erfüllung einer der beantragenden Stelle übertragenen Aufgabe erforderlich ist. Es handelt sich bei der Gratulation indes um eine freiwillig übernommene Aufgabe, die das Kommunalrecht

Gemeinden und Ortsteilen bzw. ihren Amtsträgerinnen und Amtsträgern freistellt, aber nicht auferlegt.

Die Meldebehörde ist in solchen Fällen grundsätzlich nicht verpflichtet, die Daten herauszugeben. Müsste sie dies bereits bei jedem Geburtstag, so bedürfte es der Regelung in § 50 Absatz 2 BMG nicht. Sollen auch „krumme" Geburtstage berücksichtigt werden, empfiehlt es sich daher, den Jubilarinnen und Jubilaren die Möglichkeit zu geben, sich selbst – unter Hinweis auf die Zwecke und die Möglichkeit des Widerrufs – in einen Geburtstagskalender einzutragen.

- Darf die Gemeinde Geburtstage von Jubilarinnen und Jubilaren – ggf. bis auf Widerruf – im Amtsblatt veröffentlichen?

Grundsätzlich ist die Ehrung ein persönlicher Vorgang zwischen der Gemeinde und den Geburtstagskindern. Daher ist vor einer von der Gemeinde oder einem Ortsteil beabsichtigten Veröffentlichung eine informierte Einwilligung einzuholen. Denn nicht alle wünschen die mit der Veröffentlichung im Amtsblatt verbundene Publizität – dies gilt insbesondere, wenn zur örtlich verteilten Druckversion noch eine Internetveröffentlichung kommt. Die Umsetzung der Idee vieler Gemeinden und Ortsteile, die Geburtstage bis zu einem Widerspruch ins Amtsblatt aufzunehmen, wäre folglich unzulässig. Hinzuweisen ist allerdings auf § 50 Absatz 2 BMG, der der Presse und dem Rundfunk einen Auskunftsanspruch zu Jubiläen vermittelt. Diese dürfen – vorbehaltlich anderer Persönlichkeitsrechte – auch ohne Einwilligung die Jubiläen veröffentlichen, da das materielle Datenschutzrecht für journalistische Tätigkeit der Presse nicht gilt (vgl. § 16a Brandenburgisches Pressegesetz in Verbindung mit § 29 Brandenburgisches Datenschutzgesetz).

- Vor Einführung der Datenschutz-Grundverordnung hat die Meldebehörde Daten zu Jubiläen herausgegeben, seitdem verweigert sie dies. Hat das neue Datenschutzrecht hieran etwas geändert?

Nein. Die durch die Datenschutz-Grundverordnung eingetretenen Neuerungen berühren die vorstehenden Rechtsfragen nicht. Die letzte tatsächliche Änderung der Rechtslage erfolgte durch die Melderechtsreform im Jahr 2015 – allerdings waren die Neuerungen auch damals eher gradueller Natur (u. a. geringfügige Änderung

der konkreten Jubiläen, Ausweitung des Empfängerkreises nach der Meldedatenübermittlungsverordnung).

- Manche Anlässe, wie die Begrüßung von neu zugezogenen Bürgerinnen und Bürgern, die Durchführung von Veranstaltungen usw. verfolgen einen ähnlichen Zweck wie die Geburtstagsgratulation. Kann die Herausgabe von Meldedaten auf dieselbe Rechtsgrundlage gestützt werden?

Nein. Die Regelungen des § 50 Absatz 2 BMG sowie der §§ 14 und 15 Absatz 2 MeldDÜV sind insoweit abschließend.

2.2 Handy-Parken: Mit dem Smartphone zum Parkschein

Die Verwendung von Smartphones und Apps im Alltag nimmt zunehmend auf die Gestaltung von Verwaltungsleistungen Einfluss. So stellen Diensteanbieterinnen und Diensteanbieter beispielsweise im Rahmen der Parkraumbewirtschaftung Verfahren zur elektronischen Abwicklung des Bezugs und der Bezahlung eines Parkscheins mittels Smartphone bereit (sogenanntes Handy-Parken). Im Berichtszeitraum baten uns mehrere brandenburgische Gemeinden um eine datenschutzrechtliche Prüfung des Betreibermodells und der Ausgestaltung des Verfahrens.

Bevor jemand das Handy-Parken nutzen kann, muss sie oder er einen privatrechtlichen Vertrag mit einer Diensteanbieterin oder einem Diensteanbieter schließen und die zugehörige App auf dem Smartphone installieren. Mit Hilfe der App können ein elektronisches Parkticket bezogen und die Kosten gegenüber der Diensteanbieterin oder dem Diensteanbieter beglichen werden. Die hierbei anfallenden personenbezogenen Daten (wie Name, Anschrift, Kontaktdaten, Kfz-Kennzeichen, Mobilfunknummer, je nach gewünschter Zahlungsweise Bankverbindung oder Kreditkartendaten, Login-Daten, Beginn, Ende und Dauer eines Parkvorgangs, gewählte Parkzone, gebuchte Parkgebühr und ggf. Zahlungsverhalten) dürfen für die Erbringung des Service verarbeitet werden. Daneben bedarf es für Kontrollzwecke und die Prüfung eines ordnungsgemäßen Parkvorgangs auch eines Zugangs des kommunalen Aufgabenträgers zu den Daten – jedoch beschränkt auf den für diesen (Kontroll-) Zweck erforderlichen Umfang (z.B. Kfz-Kennzeichen, Datum und Zeitraum des Parkvorgangs, Parkzone und gebuchte Parkgebühr).

Parken: smart und datenschutzgerecht

Grundsätzlich gehen wir davon aus, dass für das Verfahren des Handy-Parkens aus datenschutzrechtlicher Sicht die jeweilige Gemeinde und die Diensteanbieterin oder der Diensteanbieter gemeinsam über Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheiden und insoweit eine gemeinsame Verantwortung nach Artikel 26 Datenschutz-Grundverordnung (DS-GVO) vorliegt. In einer schriftlichen Vereinbarung, hier dem Betreibervertrag, sind u. a. die Modalitäten der Datenverarbeitung für die Zwecke der Parkraumbewirtschaftung, des Bezugs und der Abrechnung von Parkscheinen, der Überweisung der gesammelten Gebühren durch die Diensteanbieterin oder den Diensteanbieter an die Gemeinde sowie der Kontrolle der Parkvorgänge durch sie festzulegen. Jede der beteiligten Stellen hat dabei eine eigene Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten: Bei der Diensteanbieterin oder dem Diensteanbieter ist die Verarbeitung zur Erfüllung des privatrechtlichen Vertrages mit der betroffenen Person erforderlich und somit durch Artikel 6 Absatz 1 Buchstabe b DS-GVO legitimiert. Die Gemeinde nimmt mit der Parkraumbewirtschaftung eine Aufgabe im öffentlichen Interesse wahr und kann im Rahmen von Kontrollen in erforderlichem Umfang die personenbezogenen Daten der Parkenden auf Basis von Artikel 6 Absatz 1 Buchstabe e DS-GVO verarbeiten.

Im Rahmen des Betreibervertrages als Festlegung im Sinne von Artikel 26 DS-GVO muss eine klare Zuteilung der datenschutzrechtlichen Zuständigkeiten und eindeutige Abgrenzung der jeweiligen Aufgaben und Befugnisse der Beteiligten erfolgen. Dies bezieht sich beispielsweise auch auf die Pflichten zur Information der betroffenen Personen bei der Erhebung der Daten nach Artikel 13 und 14 DS-GVO, die Gewährleistung der Betroffenenrechte auf Auskunft, Berichtigung und Löschung nach Artikel 15 ff. DS-GVO oder die Melde- und Benachrichtigungspflichten nach Artikel 33 und 34 DS-GVO im Falle von Verletzungen des Datenschutzes. Da die Gemeinde keinen direkten Einfluss auf die technischen Einzelheiten der Diensteerbringung und die Details der Abwicklung der privatrechtlichen Vereinbarung mit den betroffenen Personen hat, ist die jeweilige Diensteanbieterin bzw. der Diensteanbieter hier allein datenschutzrechtlich verantwortlich. Umgekehrt ist die Gemeinde für die Verarbeitungsprozesse bei der Prüfung von Parkvorgängen und ggf. bei der Einleitung von Sanktionen eigenständig zuständig.

Über einen Zugang bei der Diensteanbieterin bzw. dem Diensteanbieter kann die Gemeinde durch Eingabe des Kennzeichens eines im Parkraum befindlichen Kraftfahrzeugs feststellen, ob für dieses Fahrzeug aktuell ein elektronischer Parkschein gelöst wurde. Diese Zugriffe und Datenübermittlungen sind datenschutzrechtlich zulässig und vertraglich zwischen allen drei Beteiligten separat zu vereinbaren. Datenschutzrechtlich kritisch ist es jedoch, wenn eine Abfrage seitens der Gemeinde zu einem Kfz-Kennzeichen erfolgt, obwohl weder ein herkömmlicher papierner Parkschein noch ein Hinweis auf die Teilnahme am Handy-Parken im Kraftfahrzeug existieren. In diesem Fall erfolgt eine unberechtigte Übermittlung des Kfz-Kennzeichens als personenbezogenes Datum an die Diensteanbieterin oder den Diensteanbieter, da keine Rechtsgrundlage für die Datenweitergabe vorliegt, wenn kein privatrechtlicher Vertrag mit der oder dem Parkenden besteht.

Insofern ist es erforderlich, dass alle, die am Handy-Parken teilnehmen, eine entsprechende Vignette im Fahrzeug hinterlassen. Die Gemeinde darf nur für Kennzeichen dieser Fahrzeuge eine entsprechende Anfrage bei der Diensteanbieterin oder dem Diensteanbieter zu Kontrollzwecken stellen. Bei Fahrzeugen ohne Vignette und ohne herkömmlichen papiernen Parkschein ist grundsätzlich der Verdacht einer Ordnungswidrigkeit gegeben.

2.3 Fortführung des Projekts zur internetbasierten Zulassung von Kraftfahrzeugen

Bereits im vorletzten Tätigkeitsbericht[18] informierten wir über die erfolgreiche Zusammenarbeit zwischen den Landkreisen und kreisfreien Städten, dem Brandenburgischen IT-Dienstleister, dem Ministerium des Innern und für Kommunales sowie unserer Behörde im Projekt zur internetbasierten Kfz-Zulassung (iKfz). Diese wurde im Berichtszeitraum fortgesetzt.

Seit dem 1. Oktober 2019 besteht für die Kraftfahrzeug-Zulassungsbehörden die Pflicht, im Rahmen des Projekts iKfz Verwaltungsleistungen für den aus zulassungsrechtlicher Sicht gesamten Lebenszyklus eines Fahrzeuges – von der Neuzulassung bis zur Außerbetriebsetzung – auch über das Internet anzubieten. Auf Basis der Erfahrungen der ersten beiden Phasen zur internetbasierten

18 Tätigkeitsbericht 2016/2017, B 11.5.

Abmeldung und Wiederzulassung von Kraftfahrzeugen konnte diese dritte Stufe des Projekts in Brandenburg fast termingerecht umgesetzt werden; der erste Landkreis nahm den Produktivbetrieb im Dezember 2019 auf, weitere folgen zu Beginn des Jahres 2020.

Neben der Erweiterung des Umfangs der angebotenen Verwaltungsleistungen der Zulassungsbehörden waren auch die nach dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) erforderlichen datenschutzrechtlichen Anpassungen des Verfahrens vorzunehmen. Diese betrafen insbesondere die Erfüllung der Informationspflichten gegenüber den betroffenen Personen und die umfassende Gewährleistung der Betroffenenrechte. Darüber hinaus mussten das IT-Sicherheitskonzept mit den technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Informationssicherheit im Verfahren fortgeschrieben und die jeweiligen Maßnahmen in der weiterentwickelten technischen Infrastruktur umgesetzt werden.

Online zum Kfz-Kennzeichen

Um die iKfz-Verwaltungsleistungen zu erbringen, verwenden die Zulassungsbehörden in den Landkreisen und kreisfreien Städten die auf Grundlage des Brandenburgischen E-Government-Gesetzes durch den Brandenburgischen IT-Dienstleister bereitgestellten IT-Basiskomponenten elektronisches Identitätsmanagement (eID-Service), elektronische Bezahlplattform (ePayBL) sowie das Landesverwaltungsnetz. Durch die Nutzung des landesweit angebotenen eID-Service kann auf die zwischen den kommunalen Aufgabenträgern abgeschlossene delegierende öffentlich-rechtliche Vereinbarung nach § 5 des Gesetzes über die kommunale Gemeinschaftsarbeit im Land Brandenburg verzichtet werden. Diese war bislang erforderlich, um einem ausgewählten Landkreis die Aufgabe des elektronischen Identitätsnachweises zu übertragen. Der Brandenburgische IT-Dienstleister ist im Verfahren darüber hinaus Auftragsverarbeiter gemäß Artikel 28 DS-GVO für den Betrieb des Portals der internetbasierten Kfz-Zulassung für die jeweiligen Landkreise und kreisfreien Städte.

Als große Herausforderung für eine fristgemäße Inbetriebnahme des Verfahrens und die Implementierung der datenschutz- und informationssicherheitstechnischen Maßnahmen erwies sich die späte Ver-

öffentlichung der Mindestsicherheitsanforderungen des Kraftfahrt-Bundesamtes für die Anbindung dezentraler Portale in der dritten Stufe des Projekts iKfz. Diese Publikation lag in der finalen Version erst Mitte November 2019 vor – also nach dem Zeitpunkt, ab dem alle Prozesse der Kfz-Zulassung bereits im Internet unterstützt werden sollten.

Auch in der aktuellen Phase des Projekts zur internetbasierten Kfz-Zulassung wirkten wir in den entsprechenden Gremien beratend mit, gaben Hinweise zur Anpassung der Verfahrensunterlagen an die Datenschutz-Grundverordnung und nahmen Einsicht in das verfahrensspezifische IT-Sicherheitskonzept des Brandenburgischen IT-Dienstleisters als Auftragsverarbeiter. Die intensive Kooperation aller Beteiligten ermöglichte es, dass der erste Landkreis die datenschutzrechtliche Freigabe gemäß § 4 Brandenburgisches Datenschutzgesetz zügig erteilen konnte. Die dort gemachten Erfahrungen sowie die im Projekt erstellten Dokumente bilden den Grundstein für den flächendeckenden iKfz-Betrieb im Land Brandenburg, da die weiteren Landkreise und kreisfreien Städte hiervon profitieren und nach Anpassung an die örtlichen Besonderheiten ihre Verfahren jeweils selbst mit erheblich geringerem Aufwand freigeben können.

Die vertrauensvolle Zusammenarbeit zwischen den verantwortlichen Stellen, dem Brandenburgischen IT-Dienstleister und der Landesbeauftragten im Projekt iKfz zeigt abermals, wie die flächendeckende Implementierung von E-Government-Verfahren im Land Brandenburg zu einem positiven Abschluss gebracht werden kann. Vor dem Hintergrund der Bemühungen der Landesregierung zur Umsetzung des Online-Zugangsgesetzes und der Entwicklung und Bereitstellung digitaler Verwaltungsleistungen empfehlen wir eine Fortführung der engen Kooperation und eine Übertragung der Erfahrungen auf andere Projekte.

3 Beratung im nicht öffentlichen Bereich

3.1 Veränderte Schwerpunkte im nicht öffentlichen Bereich

Mit dem Wirksamwerden der Datenschutz-Grundverordnung hatten sich im vorhergehenden Berichtszeitraum einige Beratungsschwerpunkte herauskristallisiert. Insbesondere zur Fotografie, zum Datenschutz in den Vereinen sowie zur Benennung eines Datenschutzbeauftragten wurde die Landesbeauftragte vielfach konsultiert. Im

aktuellen Berichtszeitraum erreichten uns zu den vorgenannten Themen zwar immer noch diverse Anfragen – es wurde jedoch auch deutlich, dass der Beratungsbedarf sich zunehmend hin zu spezielleren Fragestellungen verschiebt. Erfreulicherweise hat unser Austausch mit betroffenen Personen und Verantwortlichen gezeigt, dass die Beteiligten vermehrt besser einzuordnen wissen, welche rechtlichen Aspekte bei der Datenverarbeitung zu beachten sind. Betroffene sind zunehmend gut informiert darüber, welche Rechte ihnen zustehen; verantwortliche Daten verarbeitende Stellen wiederum haben sich mit den Anforderungen der Datenschutz-Grundverordnung besser vertraut gemacht. Es war vielmehr häufig der konkrete Umfang der Rechte und Pflichten, über den sich die Akteurinnen und Akteure nicht klar waren.

So erreichten uns viele Anfragen und Beschwerden zur Umsetzung des Rechts auf Auskunft. Dabei ging es nicht mehr nur darum, ob und in welcher Frist ein Verantwortlicher reagieren muss, sondern verstärkt um Details. Hierzu zählte etwa die Frage, wann Auskunftsdokumente als vollständig gelten oder unter welchen Umständen Auskünfte nicht erteilt werden müssen, zum Beispiel, weil Rechte Dritter beeinträchtigt werden könnten. Da sich zu diesen Gesichtspunkten noch keine gefestigte Rechtsprechung gebildet hat und die Sachverhalte große Unterschiede aufweisen können, war unsere Beratung häufig zwangsläufig darauf beschränkt, die Beteiligten über die bestehenden Normen zu informieren, aus denen sich Ausnahmen oder Einschränkungen ergeben können.

Bei vielen Beschwerden hat sich zudem gezeigt, dass Betroffene sehr pauschal die Löschung aller ihrer Daten einfordern – und viele Verantwortliche hierauf viel zu pauschal reagieren. Wir haben daher vielfach gegenüber beiden Beteiligten aufklärend tätig werden müssen. Beispielsweise muss im Rahmen eines Löschbegehrens gegenüber einer ehemaligen Vertragspartnerin bzw. einem Vertragspartner zwischen den unterschiedlichen Datenkategorien, die im Laufe des Vertragsverhältnisses ausgetauscht oder generiert wurden, differenziert werden (Kontaktdaten, Kommunikationsinhalte, Rechnungsinformationen, Nutzungsdaten usw.). Denn ein Anspruch auf Löschung besteht im Zeitpunkt einer Kündigung nicht gleichermaßen hinsichtlich aller Datenkategorien. So kann etwa der Umstand, dass gegenseitige Forderungen noch nicht vollumfänglich ausgeglichen sind oder eine gesetzliche Aufbewahrungspflicht, wie sie in § 257

Handelsgesetzbuch zu finden ist, der sofortigen Löschung bestimmter Daten entgegenstehen.

3.2 Fax- und E-Mail-Kommunikation im Gesundheitsbereich

Die Landesärztekammer Brandenburg berichtete uns von Unsicherheiten bei ihren Mitgliedern im Hinblick auf die Nutzung der Fax-Kommunikation zur Übermittlung von Gesundheitsdaten, z. B. von einem Hausarzt zu einer Fachärztin zur weiteren Behandlung. Insbesondere interessierte sich die Kammer für Hinweise unserer Behörde zur Nutzung von Fax-Geräten sowie die Möglichkeit für Patientinnen und Patienten, die Datenübermittlung per Fax durch eine Einwilligung zu legitimieren.

Gesundheitsdaten zählen gemäß Artikel 9 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) zu den besonderen Kategorien personenbezogener Daten. Ein Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit der Daten kann u. U. erhebliche Risiken für Betroffene bis hin zu einer Lebensgefahr nach sich ziehen. Insofern sind an die Gewährleistung der genannten Sicherheitsziele und die Umsetzung entsprechender technischer und organisatorischer Maßnahmen hohe Anforderungen zu stellen. Zu beachten ist auch, dass die unbefugte Offenbarung von Patientendaten durch Ärztinnen bzw. Ärzte und anderes medizinisches Personal nach § 203 Strafgesetzbuch geahndet werden kann.

Artikel 24 und 32 DS-GVO verlangen von dem Verantwortlichen (hier: einer niedergelassenen Ärztin bzw. einem Arzt oder einer Institution im Gesundheitswesen wie z. B. einem Krankenhaus) und ggf. der Auftragsverarbeiterin bzw. dem Auftragsverarbeiter die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung erfolgt und ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Bei der Auswahl der Maßnahmen sind nach den genannten Vorschriften der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Artikel 32 Absatz 1 Buchstabe a DS-GVO benennt explizit die Verschlüsselung als eine Maßnahme, Buchstabe b dieser Vorschrift verlangt, u. a. die Vertraulichkeit der Verarbeitung auf Dauer sicherzustellen. § 22 Absatz 2 Bundesdatenschutzgesetz ent-

hält ähnliche Vorgaben, die sich ausdrücklich auf die Verarbeitung besonderer Kategorien personenbezogener Daten beziehen.

Geeignete Formen der sicheren Übermittlung von Gesundheitsdaten sind z. B. die persönliche Übergabe, der Versand per Briefpost oder Kurier in verschlossenem Umschlag sowie die Kommunikation mittels Ende-zu-Ende-verschlüsselter E-Mail. Die Nutzung unverschlüsselter E-Mails oder die Kommunikation per Telefax in (heute standardmäßig anzutreffenden) IP-basierten Netzen entsprechen grundsätzlich nicht den genannten datenschutzrechtlichen Anforderungen. Einerseits wird damit den hohen Risiken für Betroffene nicht in ausreichendem Umfang entgegengewirkt, andererseits ist eine Verschlüsselung der E-Mail-Kommunikation seit Jahren Stand der Technik und mit vertretbarem Aufwand zu implementieren.

Allenfalls im absoluten Ausnahmefall – etwa bei unmittelbar drohenden gesundheitlichen Schäden für eine Patientin oder einen Patienten oder bei eingeschränkter Erreichbarkeit im Ausland – wäre ein Verzicht auf die genannten Formen der sicheren Übermittlung von Gesundheitsdaten tolerabel. In diesem Fall müsste allerdings durch zusätzliche Maßnahmen bestmöglich verhindert werden, dass Vertraulichkeit, Integrität oder Verfügbarkeit bei der Kommunikation verletzt werden. Solche Maßnahmen können insbesondere darin bestehen,

- die Kommunikationsgeräte so aufzustellen und zu benutzen, dass Unbefugte medizinische Daten nicht zur Kenntnis nehmen können,

- die Zielnummer bzw. -adresse vorab fest zu speichern und vor dem Versand nochmals sorgfältig abzugleichen, um Fehlversendungen auszuschließen,

- auf telefonischem Weg sowohl der Empfängerin bzw. dem Empfänger die unmittelbar bevorstehende Kommunikation anzukündigen als auch der Absenderin bzw. dem Absender den erfolgreichen Abschluss der Übertragung zu bestätigen und

- vorhandene geräte- bzw. softwarespezifische Sicherheitsfunktionen zu nutzen (z. B. Abruf des Faxes nur nach Eingabe eines Passworts, Kontrolle von Sende- und Empfangsprotokollen, Ver-

schlüsselung des internen Gerätespeichers, Verzicht auf Fernwartungsfunktionen).

Die Regelungen der Datenschutz-Grundverordnung sehen nicht vor, dass betroffene Patientinnen und Patienten auf die Umsetzung technisch-organisatorischer Maßnahmen verzichten können. Die Verpflichtung, ein den Risiken angemessenes und dem Stand der Technik entsprechendes Schutzniveau bei der Datenübermittlung zu gewährleisten, trifft den Verantwortlichen unmittelbar und kann nicht durch eine Einwilligung der betroffenen Person abbedungen werden. Hiervon zu unterscheiden ist allerdings eine Entbindung der Ärztin bzw. des Arztes von der Schweigepflicht. Diese würde eine Offenlegung der Patientendaten gegenüber Dritten erlauben.

4 16. Jahrestreffen mit den behördlichen Datenschutzbeauftragten

Auch im zurückliegenden Berichtsjahr konnten wir die behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Städte und Gemeinden wieder zu einer ganztägigen Beratung in unserer Dienststelle begrüßen.

Das nunmehr 16. Jahrestreffen diente dem informativen und kritischen Erfahrungsaustausch. Es sollte nicht nur die Arbeit der ohnehin bereits gut vernetzten behördlichen Datenschutzbeauftragten erleichtern. Vielmehr hatte es auch zum Ziel, Einblicke in die Arbeitsweise der Kommunen und der Datenschutzaufsichtsbehörde zu vermitteln, offene datenschutzrechtliche Fragen anzusprechen und zur Lösung datenschutzbezogener Probleme aus dem Arbeitsalltag beizutragen.

Hauptsächliches Thema der Veranstaltung waren Rechtsfragen rund um die Informationspflichten der Verantwortlichen. Auf dem Jahrestreffen gelang es beispielsweise, Antworten darauf zu finden, wann eine Information über die Datenverarbeitung im Sozialbereich unterbleiben kann oder inwieweit eine Information nach Artikel 13 bzw. 14 Datenschutz-Grundverordnung (DS-GVO) zum Beispiel um einen Hinweis auf Mitwirkungspflichten ergänzt werden darf. Auch kam die Pflicht zur Benennung eines Datenschutzbeauftragten durch kommunale Schiedsstellen zur Sprache. Der Umgang mit der Einführung elektronischer Akten sowie mit Auskunftsersuchen nach Arti-

kel 15 DS-GVO wurden umfassend diskutiert. Auf großes Interesse stieß auch die Erörterung, wie mit Auskunftsersuchen von Ermittlungsbehörden zu verfahren ist.

Die Landesbeauftragte schätzt das Engagement der Teilnehmerinnen und Teilnehmer des Jahrestreffens und betont ausdrücklich die Bedeutung der behördlichen Datenschutzbeauftragten in deren Dienststellen. Nur wenn sie frühzeitig in bevorstehende Projekte eingebunden werden, sind sie in der Lage, dem Entstehen datenschutzrechtlicher Probleme entgegenzuwirken und die Verantwortlichen effektiv zu unterstützen. Ihnen sollten deshalb nicht nur das nötige Vertrauen, sondern auch ein ausreichendes Zeitbudget für die Bewältigung ihrer Aufgaben zur Verfügung gestellt werden. Nicht zuletzt dient dies der Vermeidung von Datenschutzverstößen und damit möglicher Sanktionen. Behördliche Datenschutzbeauftragte stellen keine zusätzlichen Hürden für die Arbeit der Verwaltungen auf, sondern vermitteln, wie die in den jeweiligen Fachbereichen angestrebten Ziele mit den bestehenden gesetzlichen Vorgaben zum Schutz personenbezogener Daten in Einklang zu bringen sind. In diesem Sinne stellt die Zusammenarbeit zwischen den behördlichen Datenschutzbeauftragten und der Aufsichtsbehörde im Rahmen ihrer regelmäßigen Treffen einen wichtigen Beitrag zum Datenschutz in den brandenburgischen Kommunen dar.

V Zahlen und Fakten

1 Beschwerden

Im Berichtszeitraum gingen bei der Landesbeauftragten 878 Beschwerden ein. Davon umfasst sind alle Beschwerden von natürlichen Personen, die der Ansicht sind, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen das Datenschutzrecht verstößt. Keine Berücksichtigung fanden hierbei telefonische Beschwerden, die sich mündlich erledigen ließen. Vielfach wenden sich Betroffene aus Brandenburg auch dann an die Landesbeauftragte, wenn der für die Datenverarbeitung Verantwortliche seinen Sitz nicht in Brandenburg, sondern in einem anderen Bundesland hat. In diesen Fällen leiten wir die Eingabe an die zuständige Aufsichtsbehörde weiter und unterrichten den Beschwerdeführer über die Abgabe. Dies betraf 137 Beschwerden.

2 Beratungen

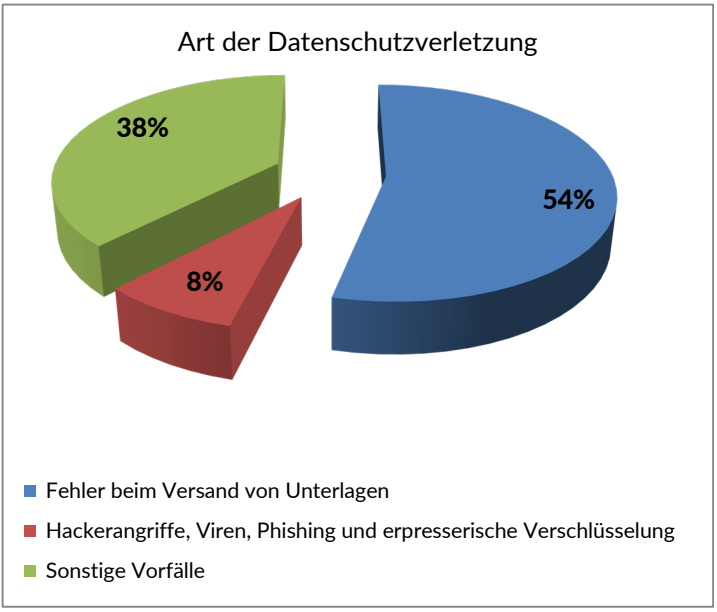
Neben der Bearbeitung von Beschwerden gehört auch die Beratung in Datenschutzfragen zu den Aufgaben der Landesbeauftragten. Sie hat betroffene Personen, Verantwortliche im öffentlichen und nicht öffentlichen Bereich sowie die Landesregierung bei Rechtssetzungsverfahren in insgesamt über 400 Fällen schriftlich beraten. Hinzu kommt eine Vielzahl von telefonischen Beratungen, die nicht in Akten erfasst werden.

3 Meldungen von Datenschutzverletzungen

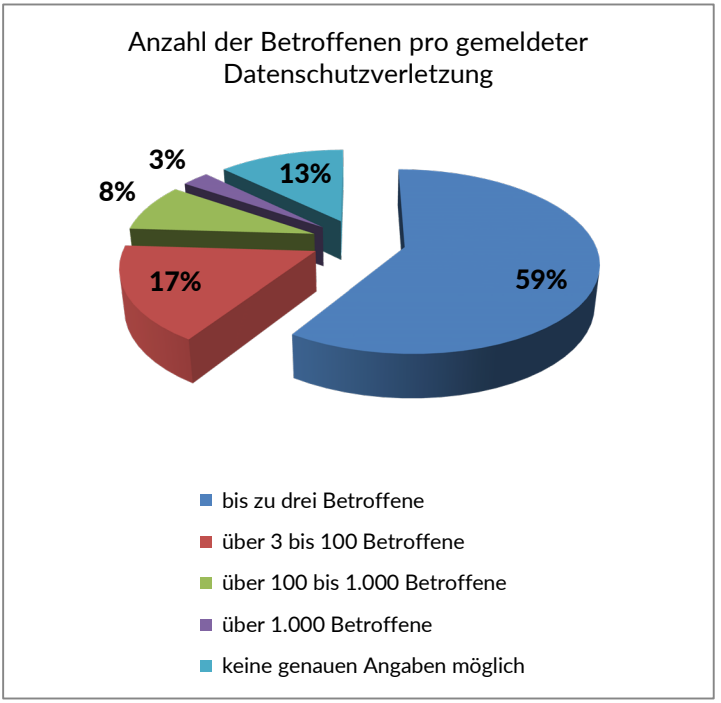
Verantwortliche sind nach Artikel 33 Datenschutz-Grundverordnung (DS-GVO) verpflichtet, der Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten zu melden. Davon ausgenommen sind lediglich Vorfälle, die voraussichtlich kein Risiko für die Betroffenen darstellen. Die Meldung hat unverzüglich und möglichst binnen 72 Stunden ab Kenntnis der Datenschutzverletzung zu erfolgen. Mit der Meldung ist der Vorfall zu beschreiben; ferner sind die Kategorien und die ungefähre Zahl der betroffenen Personen sowie die Kategorien und die ungefähre Zahl der betroffenen personenbezogenen Datensätze anzugeben. Die Meldung soll außerdem Ausführungen über die möglichen Folgen der Datenschutzverletzung für die Betroffenen sowie Angaben zu den ergriffenen oder beabsichtigten Maßnahmen zur Behebung der Datenschutzverletzung oder Abmilderung ihrer Auswirkungen enthalten. Hat der Datenschutzvor-

fall voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge, ist der Verantwortliche nach Artikel 34 DS-GVO verpflichtet, sie unverzüglich von der Verletzung zu unterrichten.

Im Berichtszeitraum erhielt die Landesbeauftragte 362 Meldungen im Sinne von Artikel 33 DS-GVO. Von Verantwortlichen aus dem öffentlichen Bereich gingen 177, von solchen aus dem nicht öffentlichen Bereich 185 Meldungen ein. Mehr als die Hälfte der Meldungen betraf Fälle, in denen Unterlagen an falsche, weil veraltete Adressen, an namensgleiche Personen oder ehemalige Ehepartnerinnen bzw. -partner versandt wurden, in denen aufgrund von Fehlkuvertierungen Unterlagen Dritter beigefügt waren oder in denen den Verantwortlichen Fehler beim E-Mail-Versand unterliefen. Hervorzuheben sind daneben die Fälle von Hackerangriffen, Virenbefall, Phishing und erpresserischer Verschlüsselung. Diese Datenschutzverletzungen beliefen sich auf 30 Fälle. In der überwiegenden Zahl der Fälle waren nur wenige Personen betroffen. Die Zahl der Meldungen von Vorfällen mit bis zu drei oder weniger betroffenen Personen lag bei 214. Dies korrespondiert mit der hohen Zahl von fehlgeleiteten Unterlagen, die in der Regel nur



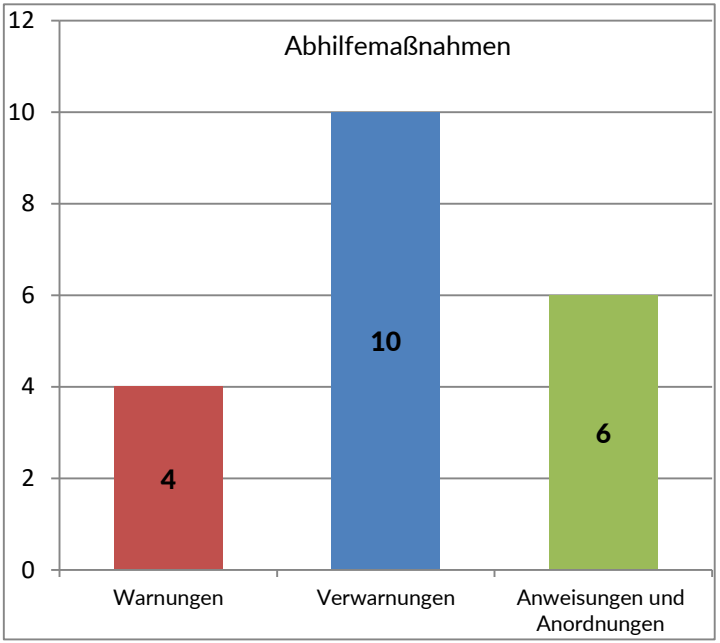
wenige Personen betrifft. Datenschutzvorfälle mit mehr als 1.000 Betroffenen wurden der Landesbeauftragten zehnmal gemeldet.



4 Abhilfemaßnahmen

4.1 Warnungen, Verwarnungen, Anweisungen und Anordnungen

Artikel 58 Absatz 2 Datenschutz-Grundverordnung (DS-GVO) stattet die Aufsichtsbehörden mit Befugnissen aus, die es ihnen erlauben, gegen Verantwortliche vorzugehen und sie zur Einhaltung der datenschutzrechtlichen Vorschriften anzuhalten. Die Landesbeauftragte machte von diesen Befugnissen (ohne Geldbußen) im Berichtszeitraum in 20 Fällen Gebrauch. Mit zehn Verwarnungen musste diese Abhilfemaßnahme am häufigsten ergriffen werden, gefolgt von sechs Anweisungen bzw. Anordnungen, mit denen Verantwortliche zu einem konkreten Tun oder Unterlassen aufgefordert werden. Beispiele für ergriffene Abhilfemaßnahmen schildern wir in diesem Bericht unter A I.



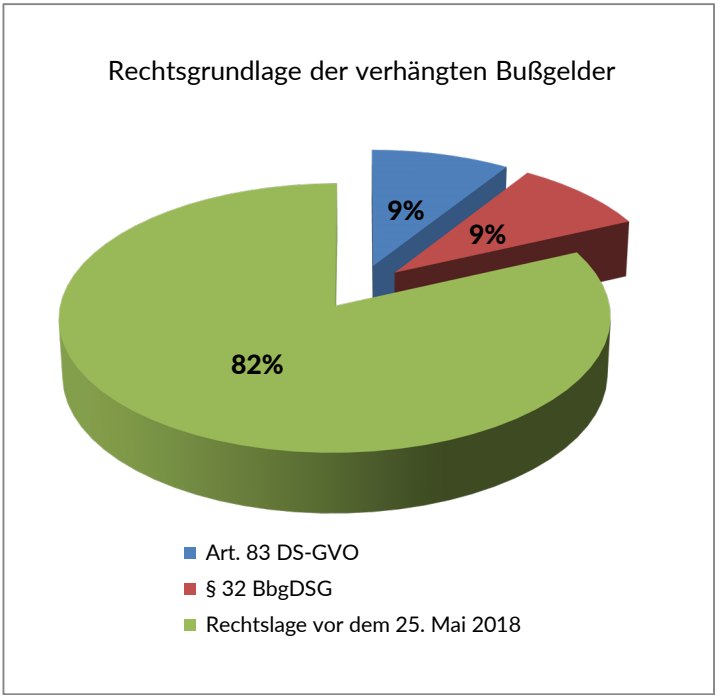
4.2 Geldbußen

Im Berichtsjahr wurden der Bußgeldstelle der Landesbeauftragten 47 Sachverhalte wegen Verstößen gegen datenschutzrechtliche Vorgaben zur Kenntnis gegeben, um die Einleitung eines Ordnungswidrigkeitenverfahrens zu prüfen. Dies bedeutete eine spürbare Steigerung zu den im vorherigen Berichtszeitraum eingegangenen Fällen, die sich in der Summe auf 24 beliefen. Ein erheblicher Anteil, nämlich 28 Fälle, wurde von den zuständigen Polizeibehörden oder Staatsanwaltschaften an die Bußgeldstelle weitergeleitet. Einen kleineren Anteil stellten insgesamt 14 Sachverhalte dar, die von aufsichtsbehördlich tätigen Mitarbeiterinnen und Mitarbeitern der Landesbeauftragten an die Bußgeldstelle abgegeben wurden. Die übrigen fünf Fälle setzten sich aus Abgaben unzuständiger Aufsichtsbehörden sowie Anzeigen von Bürgerinnen und Bürgern zusammen.

Von den 47 neu eingegangenen Sachverhalten sind mehr als die Hälfte nach der neuen Rechtslage zu bewerten. Dennoch erreichen uns auch weiterhin Fälle, in denen die relevante Handlung bereits vor dem Wirksamwerden der Datenschutz-Grundverordnung am 25. Mai 2018 abgeschlossen wurde. Diese sind weiterhin nach der

alten Rechtslage zu beurteilen. Da zusätzlich ein Rückstau an Altfällen zu verzeichnen ist, war die Bußgeldstelle auch im Berichtszeitraum schwerpunktmäßig mit der Bearbeitung von Bußgeldverfahren befasst, auf die die alte Rechtslage anwendbar ist.

Im Jahr 2019 hat die Bußgeldstelle 24 Verfahren abgeschlossen, die sich sowohl gegen nicht öffentliche Stellen als auch gegen Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen richteten. In 11 Fällen, also fast der Hälfte, verhängte die Landesbeauftragte wegen der festgestellten datenschutzrechtlichen Verstöße eine Geldbuße. Die Gesamtsumme der festgesetzten Bußgelder betrug 69.150 Euro. Der weit überwiegende Teil der Bußgeldverfahren war bereits im vorangegangenen Berichtszeitraum eröffnet worden und betraf Verstöße, die nach der alten Rechtslage zu bewerten waren. Lediglich in einem Fall war ein Ordnungswidrigkeitentatbestand des Artikels 83 DS-GVO erfüllt, da der Verstoß nach Wirksamwerden der Datenschutz-Grundverordnung begangen wurde. In einem weiteren Fall haben wir das Bußgeldverfahren nach § 32 des neuen Brandenburgischen Datenschutzgesetzes geführt.



Die andere Hälfte der geführten Verfahren – also jene Fälle, in denen wir kein Bußgeld verhängt haben – wurde auf verschiedenen Wegen beendet: Vier Verfahren hat die Bußgeldstelle aufgrund von Opportunitätserwägungen oder rechtlichen Hindernissen gar nicht erst eingeleitet. In drei Fällen wurde das Verfahren mangels hinreichenden Tatverdachts eingestellt. In zwei Fällen erhielten die Verantwortlichen eine ordnungswidrigkeitenrechtliche Verwarnung nach alter Rechtslage. In zwei weiteren Fällen gab die Bußgeldstelle mangels eigener Zuständigkeit in der Sache die Verfahren an die Datenschutzaufsichtsbehörde eines anderen Bundeslandes ab. Zwei Fälle wurden durch die Staatsanwaltschaft übernommen.

5 Europäische Verfahren

Die Datenschutz-Grundverordnung (DS-GVO) hat zu einer Intensivierung der Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden in Fällen grenzüberschreitender Datenverarbeitung geführt. Eine solche grenzüberschreitende Verarbeitung liegt unter anderem vor, wenn die Verarbeitung personenbezogener Daten durch den Verantwortlichen in mehreren Mitgliedstaaten erfolgt. Das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission bietet eine elektronische Plattform für den hierzu erforderlichen Austausch zwischen den Behörden. In den Kooperationsverfahren der Mitgliedstaaten hatte die Landesbeauftragte im Berichtszeitraum in 1249 Fällen zu prüfen, ob sie tätig werden muss:

748 Fälle wurden über das Binnenmarkt-Informationssystem von anderen Aufsichtsbehörden aufgrund von Beschwerden gemeldet. Hier prüften wir, ob die Landesbeauftragte federführende oder betroffene Aufsichtsbehörde ist und entsprechende Verfahrensschritte ergreifen muss. Die Federführung orientiert sich dabei an der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen in der Europäischen Union. Eine Betroffenheit ist demgegenüber dann gegeben, wenn die gemeldete Verarbeitungstätigkeit durch das Unternehmen erhebliche Auswirkungen auf Bürgerinnen und Bürger im Land Brandenburg haben könnte oder der Verantwortliche eine Niederlassung im Zuständigkeitsbereich der Landesbeauftragten hat.

Eine Federführung der Landesbeauftragten haben wir in einem Fall angenommen. Eine Betroffenheit der Landesbeauftragten bejahten wir in 27 Fällen. Bei den übrigen Sachverhalten haben wir nach Durchsicht 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 zu erwarten waren.

Sechs bei uns eingegangene Beschwerden gegen eine grenzüberschreitende Datenverarbeitung haben wir den übrigen europäischen Aufsichtsbehörden mit Hilfe des Binnenmarkt-Informationssystems zur Kenntnis gegeben. Sie haben damit die Gelegenheit, ebenfalls zu prüfen, ob sie in diesen Fällen federführende oder betroffene Aufsichtsbehörde sind.

In 501 Fällen beteiligten wir uns an Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII Datenschutz-Grundverordnung, die keine Individualbeschwerde zum Gegenstand hatten, etwa im Rahmen gegenseitiger Amtshilfe oder bei der Vorbereitung einer Stellungnahme des Europäischen Datenschutzausschusses. Davon gehen 20 auf die Initiative der Landesbeauftragten zurück.

Im Berichtszeitraum wurden europaweit 81 Kooperationsverfahren nach Artikel 60 DS-GVO durch einen Beschluss der jeweils zuständigen federführenden Aufsichtsbehörde abgeschlossen. Zehn dieser Beschlüsse beruhen auf Prüfungen anderer deutscher Aufsichtsbehörden, einer geht auf Brandenburg zurück.

6 Förmliche Begleitung bei Rechtsetzungsvorhaben

Gemäß § 18 Absatz 5 Satz 1 Brandenburgisches Datenschutzgesetz ist die Landesbeauftragte vor dem Erlass von Rechts- und Verwaltungsvorschriften zu hören. Auch die Datenschutz-Grundverordnung überträgt in Artikel 57 Absatz 1 Buchstabe c den Aufsichtsbehörden eine Beratungsfunktion bei legislativen Maßnahmen. Im Berichtszeitraum hat die Landesbeauftragte dementsprechend zu 20 Rechtsetzungsvorhaben Stellung genommen. Dies betraf sechs Gesetze des Landes Brandenburg, ein Gesetz des Landes Sachsen-Anhalt und 13 brandenburgische Rechtsverordnungen.

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

1 Vorbemerkung zur Änderung der Rechtslage

Die im deutschen Rechtssystem inzwischen etablierte Datenschutz-Grundverordnung findet bei straf- oder ordnungswidrigkeitenrechtlichen Verfahren sowie im Vollzugsbereich keine Anwendung. Für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, also im Bereich Justiz und Inneres, wurde bereits 2016 die sogenannte europäische JI-Richtlinie,[19] erlassen. Anders als die unmittelbar anwendbare Datenschutz-Grundverordnung muss die Richtlinie in nationales Recht umgesetzt werden. Dieser Umsetzungsprozess erfolgt teilweise im Bundesrecht aber auch in landesrechtlichen Gesetzen. Um einzelne Fachgesetze nicht mit einer Fülle von datenschutzrechtlichen Neuregelungen anzureichern, hat sich das Land Brandenburg entschlossen, die allgemeinen Inhalte der Richtlinie in einem gemeinsamen Gesetz für die Rechtsbereiche polizeiliches Handeln, Justizvollzug und Maßregelvollzug umzusetzen. Das Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz trat am 22. Juni 2019 in Kraft.[20]

2 Beanstandung wegen des fehlenden Rahmensicherheitskonzepts der Polizei

Die Polizei Brandenburg betreibt seit vielen Jahren eine große Zahl an Verfahren zur Verarbeitung personenbezogener Daten, z. B. das polizeiliche Vorgangsbearbeitungssystem ComVor, das Informations- und Auskunftsverfahren POLAS, das Einsatzleitsystem für Behörden und Organisationen mit Sicherheitsaufgaben ELBOS und das Kennzeichenerfassungssystem KESY.

Damit die Einzelnen durch die Verarbeitung personenbezogener Daten nicht in unzulässiger Weise in ihren Grundrechten beeinträch-

19 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU L 119/89).

20 siehe B 6

tigt werden, hat die Polizei Brandenburg bei Einführung und Betrieb dieser Verfahren datenschutzrechtliche Vorgaben einzuhalten. Dazu gehört es auch, dass ein aus einer Risikoanalyse entwickeltes IT-Sicherheitskonzept ergeben muss, dass die von dem Verfahren ausgehenden Gefahren für die Rechte und Freiheiten der Betroffenen durch geeignete technische und organisatorische Maßnahmen beherrscht werden können.

Die gesetzliche Verpflichtung zur Erstellung von Sicherheitskonzepten für die von ihnen betriebenen Verfahren ist den Verantwortlichen der Polizei Brandenburg seit Langem bekannt. Im Sinne einer systematischen und effizienten Herangehensweise hatte die Polizei vorgesehen, ein sogenanntes Rahmensicherheitskonzept für die polizeiliche IT-Infrastruktur mit allen angeschlossenen Systemen und Komponenten zu erstellen, in dem grundlegende, verfahrensunabhängige Sicherheitsmaßnahmen beschrieben und umgesetzt werden. Das Rahmensicherheitskonzept sollte damit die Basis für alle auf ihm aufbauenden Teilsicherheitskonzepte der einzelnen Fachverfahren bilden. Diese Vorgehensweise ist bei großen und komplexen Informationsverbünden üblich, entspricht dem Stand der Technik und wird von der Landesbeauftragten unterstützt.

IT-Sicherheit lange nicht nachgewiesen

Trotz unserer wiederholten Aufforderung hat die Polizei das Rahmensicherheitskonzept allerdings über Jahre hinweg nicht komplett vorgelegt. Bereits in unserem letzten Tätigkeitsbericht hatten wir deshalb kritisiert, dass es immer noch nicht fertiggestellt ist, und gefordert, diesen Mangel zu beseitigen.

Die Verantwortlichen stellten uns nacheinander mehrere Termine in Aussicht, ohne sie einzuhalten. Stattdessen wurde die Finalisierung des Konzeptes immer weiter verschoben. Wir mussten daher feststellen, dass es hinsichtlich der Erfüllung der gesetzlichen Anforderungen zur Gewährleistung des Datenschutzes und der Informationssicherheit bei der Verarbeitung personenbezogener Daten Betroffener mittels eines umfassenden und aktuellen Rahmensicherheitskonzeptes erhebliche Mängel gibt und dieser Missstand bereits seit vielen Jahren andauert. Die Landesbeauftragte hat daher gegenüber dem verantwortlichen Minister für Inneres und Kommunales die Verstöße gegen § 7 Abs. 3, § 10 und § 10a Brandenburgisches

Datenschutzgesetz in der am 24. Mai 2018 geltenden Fassung beanstandet und ihn aufgefordert, unverzüglich ein vollständiges Rahmensicherheitskonzept vorzulegen.

Der Minister legte in seiner Stellungnahme dar, dass er sich mit Nachdruck für die Fertigstellung der erforderlichen Dokumente einsetzen werde und versicherte, dass Datenschutz und Informationssicherheit höchste Priorität hätten. Einige Monate später wurden uns von der Polizei Brandenburg umfangreiche Unterlagen zum geforderten Sicherheitskonzept übergeben. Diese befinden sich zurzeit in der Prüfung. Eine endgültige datenschutzrechtliche Bewertung steht daher noch aus.

Auch nach der mit dem Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz bestehenden neuen Rechtslage sind die Verantwortlichen der Polizei verpflichtet, technische und organisatorische Maßnahmen zu bestimmen und umzusetzen, um die Risiken für die Rechte und Freiheiten der von polizeilicher Datenverarbeitung betroffenen Personen zu beherrschen. Wir werden die uns zur Verfügung stehenden Mittel nutzen, die Einhaltung dieser gesetzlichen Anforderungen zu kontrollieren und durchzusetzen.

3 Kennzeichenerfassungssystem KESY

Im Jahr 2019 stand das Verfahren der brandenburgischen Polizei zur automatischen Kennzeichenerfassung (KESY) im Fokus. Anlass war ein Ermittlungsfall der Strafverfolgungsbehörden, der auch in der Öffentlichkeit, dem zuständigen Ministerium des Innern und für Kommunales und in parlamentarischen Gremien zu einer intensiven Befassung mit dieser Maßnahme führte. Für uns ist dieses Verfahren relevant, weil das Kraftfahrzeugkennzeichen ein personenbezogenes Datum ist, dessen Verarbeitung einer Rechtsgrundlage bedarf.

Die Polizei in Brandenburg nutzt das Verfahren KESY seit dem Jahr 2010. Es wird sowohl zu gefahrenabwehrrechtlichen Fahndungszwecken gemäß § 36a Brandenburgisches Polizeigesetz als auch zur Strafverfolgung nach Vorschriften der Strafprozessordnung (StPO) eingesetzt. Das System umfasst mehrere stationäre Anlagen mit Kameras, die an definierten Standorten in Brandenburg digitalisierte Bilder von Kraftfahrzeugkennzeichen und die rückwärtige Ansicht des Fahrzeugs aufnehmen. Das Verfahren kann im sogenannten

Fahndungsmodus betrieben werden, bei dem erfasste Kennzeichen mit einem konkreten Fahndungsbestand abgeglichen, Nichttreffer automatisiert gelöscht und nur sogenannte „Treffer“ für die weitere Bearbeitung gespeichert werden. Im sogenannten Aufzeichnungsmodus werden dagegen alle Kennzeichen von Fahrzeugen, die eine Erfassungskamera passieren, eingelesen, aufgezeichnet und gespeichert. Diese Datenbestände sind, solange keine Löschung erfolgt, dauerhaft recherchierbar. Den Aufzeichnungsmodus nutzt die Polizei zu repressiven Zwecken, beispielsweise im Zuge von Ringalarmfahndungen (§ 111 StPO) oder bei längerfristigen Observationen unter Verwendung besonderer für Observationszwecke bestimmter technischer Mittel (§ 163f i. V. m. § 100h Absatz 1 Nummer 2 StPO). Die längerfristige Observation einer oder eines Beschuldigten darf nur durch ein Gericht bei tatsächlichen Anhaltspunkten für Straftaten von erheblicher Bedeutung für die Dauer von maximal drei Monaten angeordnet werden, kann allerdings, soweit die Voraussetzungen fortbestehen, wiederholt verlängert werden. Der Einsatz des technischen Mittels zur Durchführung der Observation wird in der Regel von der zuständigen Staatsanwaltschaft angeordnet. Die Brandenburgische Polizei nutzt die Kennzeichenfahndung sowohl für landeseigene Ermittlungsverfahren als auch in Amtshilfe bei Ersuchen von Ermittlungsbehörden anderer Bundesländer.

3.1 Stein des Anstoßes: Ermittlungen im Fall einer Vermissten

Die Polizei des Landes Berlin ermittelte im März 2019 wegen einer vermissten jungen Frau, als bekannt wurde, dass das Fahrzeug eines Tatverdächtigen auf dem Gebiet des Landes Brandenburg an zwei mehrere Wochen zurückliegenden Tagen erfasst und gespeichert wurde, obwohl das Kennzeichen zu diesem Zeitpunkt weder zur Gefahrenabwehr noch zur Strafverfolgung in einer Fahndungsdatei der brandenburgischen Polizei hinterlegt war. Es stellte sich heraus, dass zu diesem Zeitpunkt der Aufzeichnungsmodus des Kennzeichenerfassungssystems aufgrund eines nicht mit dem Vermisstenfall zusammenhängenden, bei der Staatsanwaltschaft Frankfurt (Oder) betriebenen Ermittlungsverfahrens wegen schwerer Bandenkriminalität aktiviert war. Für dieses Verfahren lagen mehrere, zeitlich aneinander anschließende gerichtliche Beschlüsse zur längerfristigen Observation vor. Darüber hinaus existierten auch staatsanwaltliche Anordnungen, besondere für Observationszwecke bestimmte technische Mittel zu nutzen. Diese wurden erstmals im September 2017 erlassen und waren ohne Unterbrechung immer wieder verlängert

worden. Da das Ermittlungsverfahren noch nicht beendet war, wurden Daten über insgesamt 19 Monate angesammelt und dabei auch das von der Berliner Polizei gesuchte Kennzeichen miterfasst. Die brandenburgische Polizei hatte auf Ersuchen der Berliner Kolleginnen und Kollegen danach recherchiert und die Daten übermittelt.

3.2 Beanstandung wegen des Verstoßes gegen die Unterstützungspflicht

Für uns war die mediale Berichterstattung Anlass, den Einsatz des Kennzeichenerfassungssystems umfassend zu prüfen. Dazu führten wir im Juli 2019 eine Vor-Ort-Kontrolle im Einsatz- und Lagezentrum der Polizei in Potsdam und bei einer Dienststelle des Landeskriminalamts durch. Unsere Absicht, auch die bei der Polizei vorliegenden gerichtlichen Beschlüsse und staatsanwaltlichen Anordnungen einzusehen, die den Einsatz von KESY in dem Frankfurter Verfahren legitimieren sollten, konnten wir nicht umsetzen. Die Polizei verweigerte uns die Vorlage der Dokumente unter Hinweis darauf, dass allein die sachleitende Staatsanwaltschaft Frankfurt (Oder) berechtigt sei, Entscheidungen über die Akteneinsicht in ein noch laufendes Verfahren zu gewähren und keine Einwilligungen dieser Staatsanwaltschaft vorlägen. Aus unserer Sicht ist diese Argumentation unhaltbar, denn die Polizei ist trotz der Befugnis der Staatsanwaltschaft, derartige Maßnahmen anzuordnen, datenschutzrechtlich für das von ihr betriebene Verfahren KESY verantwortlich. Die Polizei bestimmt ausschließlich über die Mittel der Verarbeitung personenbezogener Daten, da sie Kenntnis und Kontrolle über die stationären Standorte, den Betrieb, einzelne Abläufe wie die Auswertung der Daten als auch über technisch-organisatorische Aspekte des Verfahrens hat. Sie ist in der Verfahrensdokumentation folgerichtig als verantwortliche Organisationseinheit benannt. Als Verantwortlicher ist sie daher gemäß § 35 Absatz 1 und 2 Brandenburgisches Polizei,- Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) verpflichtet, die Datenschutzaufsicht bei der Erfüllung ihrer Aufgaben zu unterstützen und insbesondere Einsicht in alle Vorgänge und Aufzeichnungen zu gewähren. Da die Beschlüsse und Anordnungen sich in Fallakten der Polizei befanden, war uns Zugang dazu zu gewähren. Wegen der fortgesetzten Weigerung der Polizei haben wir daher gemäß § 36 Absatz 1 Nummer 2 BbgPJMDSG gegenüber dem Polizeipräsidenten eine Beanstandung wegen Verstoßes gegen die Unterstützungspflicht ausgesprochen. Die gerichtlichen Beschlüsse und die Anordnungen der Staatsanwaltschaft Frankfurt (Oder) wurden uns zu

einem späteren Zeitpunkt durch die Generalstaatsanwaltschaft zur Verfügung gestellt. Dadurch konnten wir den Verfahrensgang und die Formulierungen in den Anordnungen prüfen.

3.3 Stellungnahme gegenüber dem Landesverfassungsgericht

Parallel nahmen wir die Gelegenheit wahr, gegenüber dem Verfassungsgericht des Landes Brandenburg eine Stellungnahme zu den datenschutzrechtlichen Fragen der Kennzeichenerfassung abzugeben. Dort war eine Verfassungsbeschwerde eines Beschwerdeführers anhängig, der mit seinem Fahrzeug regelmäßig einen Autobahnabschnitt in Brandenburg befährt und davon ausgeht, dass sein Kennzeichen mehrfach von der Polizei gespeichert wurde. Er sah darin einen Eingriff in sein Recht auf informationelle Selbstbestimmung und hatte vor dem Amtsgericht und nachfolgend im Beschwerdeverfahren vor dem Landgericht die Rechtmäßigkeit der strafprozessualen Anordnungen und deren Umsetzung überprüfen lassen wollen. Beide Gerichte lehnten seinen Antrag jedoch unter Hinweis auf die fehlende Antragsberechtigung ab, weshalb der Beschwerdeführer wegen Verletzung seines rechtlichen Gehörs vor das Verfassungsgericht zog. In unserer Stellungnahme legten wir auch unsere Rechtsauffassung zur flächendeckenden Erfassung von Kennzeichen durch die Polizei dar.

Als Ergebnis stellten wir fest, dass die herangezogene Befugnisnorm des § 100h Absatz 1 Satz 1 Nummer 2 StPO für den Einsatz der Kennzeichenerfassung im Aufzeichnungsmodus keine ausreichende Rechtsgrundlage darstellt. Bei der Ermächtigung zum Einsatz technischer Mittel für Observationen hatte der Bundesgesetzgeber ursprünglich an Mittel gedacht, die nicht zu Aufzeichnungen führen und Auswirkungen auf Dritte vermeiden, wie etwa Peilsender. Bei der fortlaufenden Daueraufzeichnung erfasst und speichert KESY jedoch eine unbegrenzte Anzahl von Fahrzeugen nicht beschuldigter Personen, die dadurch zu Zielpersonen werden, da jederzeit weitere Ermittlungshandlungen (wie zum Beispiel Halterabfragen oder spätere Datenabgleiche) daran anknüpfen können. Der Einsatz technischer Mittel gegen nicht beschuldigte Personen ist nur ausnahmsweise zulässig. Vor dem Hintergrund der angedachten technischen Mittel wurden an den Einsatz nur wenig beschränkende Voraussetzungen geknüpft. Dies lässt sich für die Kennzeichenerfassung nicht rechtfertigen, zumal ganz überwiegend gegenüber den betroffenen Personen (Halterin bzw. Halter oder Führerin bzw. Führer der aufge-

zeichneten Fahrzeuge) kein Verdacht besteht, dass sie in irgendeiner Verbindung zu den Beschuldigten des Ursprungsverfahrens stehen oder zu deren Auffinden führen. Im Jahr 2018 hat das Bundesverfassungsgericht festgestellt, dass bereits jede Kennzeichenkontrolle einen Eingriff in das Recht auf informationelle Selbstbestimmung aller in die Kontrolle einbezogenen Personen begründet, unabhängig davon, ob das Kennzeichen danach sofort gelöscht wird.[21] In unserem Prüffall sind wir unter Berücksichtigung der hohen Anzahl der gespeicherten Fahrzeuge von Unbeteiligten, der Laufzeit der Maßnahme von insgesamt 23 Monaten und dem Ermittlungsgegenstand (Eigentumsdelikte verübt durch eine Bande) zu dem Schluss gelangt, dass der Einsatz des KESY-Verfahrens im Aufzeichnungsmodus nicht verhältnismäßig war.

3.4 Beanstandung wegen datenschutzrechtlicher Verstöße und Warnung

Unabhängig von der Frage der Rechtsgrundlagen für den Betrieb des Kennzeichenerfassungssystems (KESY) im Aufzeichnungsmodus stellten wir bei unserer Prüfung vor Ort datenschutzrechtliche Verstöße fest.

In den Anordnungen der Staatsanwaltschaft Frankfurt (Oder) finden sich über viele Monate hinweg keine konkreten Anweisungen, KESY im Aufzeichnungsmodus als technisches Mittel einzusetzen. Vielmehr wurde lediglich die Rechtsnorm zitiert, ohne das Mittel konkret zu benennen. Die Polizei hat diesbezüglich auch nicht um eine Klarstellung ersucht, sondern das System eigenverantwortlich für die Observation im Aufzeichnungsmodus eingesetzt. Damit hat sie gegen das Gebot der Datensparsamkeit und das datenschutzrechtliche Erforderlichkeitsprinzip verstoßen. Als Verfahrensverantwortliche war die Polizei aus unserer Sicht darüber hinaus verpflichtet, die über Monate angesammelten Kennzeichendaten in angemessener Zeit und nach Absprache mit der Staatsanwaltschaft auch auf die Erforderlichkeit für ihre weitere Speicherung für das anhängige Ermittlungsverfahren zu überprüfen und nicht benötigte Daten zu löschen. Der gesamte Datenbestand wurde jedoch vorgehalten und sollte nach Auskunft der Polizei erst mit Abschluss des Verfahrens gelöscht werden, wenn die Staatsanwaltschaft eine entsprechende

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

Verfügung erlässt. Diese Praxis verstößt gegen das Gebot unverzüglicher Löschung nicht mehr erforderlicher Daten und ist unzulässig. Da die brandenburgische Polizei das Kennzeichenerfassungssystem im Aufzeichnungsmodus nicht nur für landeseigene Verfahren, sondern überwiegend in Amtshilfe für andere Staatsanwaltschaften in Amtshilfe betreibt, liegen häufig mehrere Anordnungen für den gleichen Zeitraum vor. Die über KESY akkumulierten Daten sind nicht nach den jeweiligen, sich teilweise überschneidenden Ermittlungsverfahren getrennt, was eine datenschutzgerechte Löschpraxis zusätzlich erschwert.

Schließlich stellten wir fest, dass die Polizei es versäumt hat, Zugriffsrechte auf das Verfahren nach strikten Erforderlichkeitskriterien zu begrenzen. Abgesehen von der Anzahl der Berechtigten konnten die Nutzungsberechtigten bis zu 28 Tage rückwirkend auf alle erhobenen Daten zugreifen.

Wir haben die in der Vergangenheit liegenden Verstöße der Polizei im Dezember 2019 gemäß § 36 Absatz 1 Nummer 2 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) beanstandet. Zugleich sprachen wir eine Warnung gemäß § 36 Absatz 1 Nummer 1 BbgPJMDSG über den datenschutzwidrigen Einsatz in der Zukunft aus, falls die Polizei beabsichtigt, die Datenverarbeitung so beizubehalten. Wir forderten, den bestehenden Datenbestand einer Überprüfung zu unterziehen und künftig nicht mehr erforderliche Kennzeichendaten zu löschen.

Das Polizeipräsidium hatte bereits vor unserer Beanstandung teilweise Abhilfe geschaffen, indem es durch eine interne Dienstanweisung festlegte, vor dem Einsatz von KESY darauf hinzuwirken, dass die Kennzeichenerfassung und der Betriebsmodus hinreichend konkret in der staatsanwaltlichen Anordnung benannt werden. Auch die Zahl der Zugriffsberechtigten wurde durch die Polizeiführung überprüft und bis Juni 2019 um mehr als die Hälfte reduziert. Diese Notmaßnahmen sind zu begrüßen, jedoch nicht ausreichend.

Wir haben deutlich gemacht, dass die Strafverfolgungsbehörden einen Eingriff in das informationelle Selbstbestimmungsrecht mit dieser Tragweite für nicht beschuldigte Verkehrsteilnehmende nicht auf die herangezogene Rechtsgrundlage § 100h StPO stützen können. Diese Position wird auch von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder geteilt, die

in ihrer Entschließung vom 6. November 2019 gefordert hat, die unterschiedslose Erfassung, Speicherung und Auswertung der Kennzeichendaten zu repressiven Zwecken zu unterlassen und rechtswidrig gespeicherte Daten zu löschen. Ob der Beschluss der Justizministerinnen und Justizminister der Länder auf ihrer Frühjahrskonferenz 2019 für eine ausdrückliche gesetzliche Regelung des Einsatzes von Kennzeichenlesesystemen tatsächlich zu einer Rechtsänderung und gegebenenfalls zu einer Neubewertung führen wird, bleibt abzuwarten.

Wir gehen jedoch davon aus, dass § 100h StPO in Brandenburg zunächst weiterhin für den repressiven Einsatz von KESY im Aufzeichnungsmodus herangezogen wird. Daher haben wir u. a. gefordert, dass zumindest die Form der Speicherung in einem einzigen Datenbestand überarbeitet werden muss, um unverzügliche Löschungen zu ermöglichen.

Bis zum Jahresschluss war nicht absehbar, ob die Polizeiführung nunmehr die datenschutzrechtliche Verantwortung für das Verfahren übernimmt. Eine Stellungnahme zu unserer Beanstandung und Warnung erwarten wir für den Jahresbeginn 2020.

4 Einsatz von Körperkameras

Im Rahmen einer Änderung des Brandenburgischen Polizeigesetzes (BbgPolG)[22] wurde im Berichtszeitraum eine Rechtsgrundlage für den Einsatz von Körperkameras (sogenannte Bodycams) zur Eigensicherung und Dokumentation geschaffen. Nach § 31a Absatz 2 BbgPolG kann die Polizei zur Erfüllung ihrer Aufgaben bei Personen- oder Fahrzeugkontrollen Bildaufnahmen, Bild- und Tonaufzeichnungen durch den Einsatz körpernah getragener technischer Mittel herstellen, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Beamtinnen und Beamten oder Dritten gegen eine Gefahr für Leib, Leben oder Freiheit erforderlich ist. Unzulässig ist eine solche Maßnahme u. a. in Wohn- und Nebenräumen, eingeschränkt zulässig in Arbeits-, Betriebs- und Geschäftsräumen sowie auf anderem befriedeten Besitztum.

22 Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 1. April 2019 (GVBl. I Nr. 3).

Bodycams können zunächst im Bereitschaftsmodus betrieben werden. Hierbei wird eine Bild- und Tonaufnahme als sogenannte Pre-Recording-Sequenz von 60 Sekunden Dauer im Kurzzeitspeicher der Kamera abgelegt und fortlaufend automatisch überschrieben. Versetzt die Beamtin oder der Beamte die Bodycam in den Aufzeichnungsmodus, wird die letzte Pre-Recording-Sequenz zusammen mit der fortlaufenden Bild- und Tonaufnahme dauerhaft gespeichert. Wird die Kamera ausgeschaltet, ohne dass der Aufzeichnungsmodus eingeschaltet war, ist die Pre-Recording-Sequenz aufgrund der Flüchtigkeit des Kurzzeitspeichers spurenlos gelöscht.

Die brandenburgische Polizei hat uns ihre Planungen zum Einsatz von Körperkameras vorgestellt. Beabsichtigt ist ein einjähriges Pilotprojekt in den Polizeiinspektionen Potsdam, Oranienburg und Cottbus, bei dem Bodycams im täglichen Streifendienst und von der Bereitschaftspolizei getestet werden. Dabei sollen 20 Kameras von vier verschiedenen Herstellern eingesetzt werden. Am Ende des Projektzeitraums ist eine standardisierte und vergleichende Auswertung unter Beteiligung der testenden Dienststellen und mit Hilfe der Expertise der Hochschule der Polizei Brandenburg vorgesehen.

Der Einsatz der Körperkameras wird vorrangig in Brennpunktbereichen erfolgen, entsprechend der gesetzlichen Regelungen jedoch nicht in Wohnräumen. Durch ein deutlich sichtbares Piktogramm bzw. einen Aufnäher mit dem Schriftzug „Video/Audio“ in einer Signalfarbe weist die Polizei deutlich auf die Kamera hin. Das Einschalten des Aufzeichnungsmodus wird zudem verbal angekündigt. Grundsätzlich sollen die Kameras abschreckend wirken, um Widerstands- und Gewalthandlungen vorzubeugen. Aufzeichnungen dürfen maximal 14 Tage gespeichert werden, außer in Fällen, in denen sie benötigt werden zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder für die Überprüfung der Rechtmäßigkeit von aufgezeichneten polizeilichen Maßnahmen, insbesondere wenn eine betroffene Person dies verlangt.

Wir haben darauf hingewiesen, dass die deeskalierende Wirkung von Körperkameras bisher nicht durch eine wissenschaftlich fundierte Evaluation belegt wurde. Aus unserer Sicht kann der durch die Video- bzw. Audioaufnahme eintretende Eingriff in das Recht auf informationelle Selbstbestimmung nur durch eine nachweislich erhöhte Sicherheit für Leib, Leben und Freiheit der Polizeibeamtinnen und -beamten oder Dritter gerechtfertigt sein. Wir haben deshalb un-

sere Zweifel an der Geeignetheit und Erforderlichkeit der Eingriffsbefugnis deutlich gemacht. Auf jeden Fall ist daher im Rahmen des Pilotbetriebs sicherzustellen, dass die Körperkameras entsprechend restriktiv eingesetzt und die Beamtinnen und Beamten angemessen für die Rechte der betroffenen Personen sensibilisiert werden. Die Polizei hat uns zugestimmt, dass der Einsatz von Bodycams nur bei Gefahr einer schweren Körperverletzung oder Lebensgefährdung in Betracht kommt. Sollen Aufnahmen für andere Zwecke als zur Eigensicherung und Dokumentation verwendet werden, läge eine Zweckänderung vor, über die die Behördenleitung nach Prüfung der Rechtsgrundlage zu entscheiden hätte.

Zudem ist der Polizei klar, dass sie sorgfältig geeignete technische und organisatorische Maßnahmen zu ergreifen hat, um die Vertraulichkeit und Integrität der Aufzeichnungen zu gewährleisten. Alle Kameras bieten zwar eine verschlüsselte Speicherung an – allerdings konnte die Polizei auf Nachfrage keine Aussagen zu den konkreten Verschlüsselungsverfahren treffen. Hier haben wir um nachträgliche Information gebeten. Wir haben außerdem auf die Notwendigkeit einer Datenschutz-Folgenabschätzung vor Projektbeginn und auf die zu erstellenden Fachkonzepte und Dokumentationen hingewiesen (z. B. Risikobewertung, IT-Sicherheitskonzept, Rechte-/Rollenkonzept, Löschkonzept, Verzeichnis der Verarbeitungstätigkeiten).

5 Beratung zur Änderung des Brandenburgischen Polizeigesetzes

Den Gesetzentwurf zur Änderung des Brandenburgischen Polizeigesetzes hat die Landesregierung im Oktober 2018 in den Landtag eingebracht.[23] Wir wurden vom Ministerium des Innern und für Kommunales bereits während des Entwurfsstadiums eingebunden und hatten im Januar 2019 nochmals die Gelegenheit, in einer Anhörung im Ausschuss für Inneres und Kommunales des Landtages Brandenburg unsere Stellungnahme zu erläutern.

Mit dem am 1. April 2019 verkündeten 12. Änderungsgesetz zum Polizeigesetz[24] wurden neue und teilweise erweiterte Eingriffsbefugnisse für die Polizei geschaffen. Neu eingefügt wurden die Mel-

23 Tätigkeitsbericht Datenschutz 2018, V 1.1.

24 Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes vom 1. April 2019 (GVBl I Nr. 3).

deauflage, Maßnahmen wie die erkennungsdienstliche Behandlung, die anlassbezogene Kennzeichenfahndung, Ausschreibung und verdeckte Registrierung jeweils zur Abwehr von Terrorgefahr, Aufenthaltsvorgaben und Kontaktverbote bis zu drei Monaten Dauer, der Gewahrsam zur Verhinderung einer Straftat und der Einsatz von Körperkameras im öffentlich zugänglichen Raum. Unsere Bedenken gegen den verdeckten Einsatz technischer Mittel zur Überwachung der Telekommunikation durch Eingriffe in informationstechnische Systeme (sogenannte Quellen-TKÜ) wurden vom beratenden Innenausschuss aufgegriffen und die Befugnis ersatzlos gestrichen.

Eine gravierende Änderung im Vergleich zur alten Rechtslage ist die Einführung eines von uns als nicht hinreichend konkret kritisierten „vorverlagerten Gefahrenbegriffs“ bei einigen Erhebungsbefugnissen zur Abwehr von Gefahren des Terrorismus. Aus unserer Sicht sind die festgelegten Eingriffsvoraussetzungen, die eine polizeiliche Einschätzung einer drohenden – im Gegensatz zu einer konkreten – Gefahrenlage und von möglicherweise strafrelevantem Verhalten erfordern, nicht ausreichend bestimmt. Die erwartete Begehung einer Straftat muss gemäß der neuen Vorschrift nur „ihrer Art nach konkretisiert“ sein und in einem „übersehbaren Zeitraum“ geschehen können. Bereits Verhaltensweisen, die eine „konkrete Wahrscheinlichkeit“ einer Rechtsgutschädigung begründen, sollen Eingriffe rechtfertigen können. Mit unserer Rechtsauffassung, dass das Abweichen von tradierten Gefahrenabwehrkategorien mit unbestimmten Rechtsbegriffen ohne nähere Konkretisierung in der Befugnisnorm nicht im Einklang mit sicherheits- und verfassungsrechtlichen Prinzipien steht, konnten wir uns jedoch nicht durchsetzen.

Für die beschlossene Einführung von Körperkameras zur Aufzeichnung von Bild und Ton zur Eigensicherung bei Personen- oder Fahrzeugkontrollen, die auch eine Pre-Recording-Funktion (Vorabaufzeichnung) umfasst, hätten wir uns zumindest eine Befristung und anschließende Evaluierung der Maßnahme hinsichtlich der behaupteten Abschreckungswirkungen gewünscht. Dies hat der Landtag jedoch nicht umgesetzt.

Im Vergleich zu den Änderungen der Polizeigesetze anderer Länder fällt die Erweiterung polizeilicher Befugnisse in Brandenburg noch moderat aus. Dennoch haben wir neben der konkreten Kritik an einzelnen Maßnahmen deutlich gemacht, dass uns die stetige Kumulation von Datenerhebungen durch neue Erlaubnisnormen und

herabgesenkte Eingriffsschwellen zunehmend Sorgen bereitet und die Polizei eine Gesamtschau der Eingriffsbefugnisse und der damit einhergehenden grundrechtlichen Belastungen der Bürgerinnen und Bürger vornehmen muss.

6 Beratung zur Umsetzung der Richtlinie (EU) 2016/680: Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz

Die EU-Richtlinie 2016/680 (sogenannte JI-Richtlinie) stellt das zweite Standbein der europäischen Datenschutzreform dar; sie ist für den Bereich der Datenverarbeitung von Sicherheitsbehörden und bei der Strafvollstreckung maßgeblich. Die Richtlinie war am 5. Mai 2016 in Kraft getreten und räumte den Mitgliedstaaten eine zweijährige Umsetzungsfrist bis zum 6. Mai 2018 ein. Da es in Brandenburg nicht gelang, die entsprechenden Landesvorschriften fristgerecht zu erlassen, beschloss der Landtag im April 2018 eine Übergangsregelung. Für die Datenverarbeitung der Polizei und Ordnungsbehörden, soweit sie Ordnungswidrigkeiten verfolgen, galt das Brandenburgische Datenschutzgesetz in seiner bisherigen Fassung fort, während in den übrigen, nicht der Datenschutz-Grundverordnung (DS-GVO) unterfallenden Anwendungsbereichen das novellierte Brandenburgische Datenschutzgesetz und die Datenschutz-Grundverordnung für entsprechend anwendbar erklärt wurden. Im Jahr 2019 wurden die Vorgaben der Richtlinie auf Landesebene durch das Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsgesetz (BbgPJMDSG)[25] umgesetzt. Es trat zum 22. Juni 2019 in Kraft.

Im Zuge der brandenburgischen Strategie, einen gemeinsamen Gesetzentwurf für die Bereiche Polizei, Justiz- und Maßregelvollzug mit den allgemeinen Inhalten der JI-Richtlinie vorzubereiten und nur einzelne, spezialgesetzliche Änderungen in den Fachgesetzen (Polizeigesetz, Strafvollzugs- und Maßregelvollzugsgesetz) einzufügen, war eine interministerielle Arbeitsgemeinschaft gegründet worden. In diese wurden wir im Herbst 2018 zunächst für eine Sitzung mit

25 Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 für die Verarbeitung personenbezogener Daten durch die Polizei sowie den Justiz- und Maßregelvollzug des Landes Brandenburg vom 19. Juni 2019 (GVBl. I 2019 Nr. 43).

einbezogen. Unsere beratende Mitarbeit in diesem Gremium fiel jedoch dem engen parlamentarischen Zeitrahmen zum Opfer. Die Ministerien wünschten unter allen Umständen eine Umsetzung der Richtlinie bis zum Ende der laufenden Legislaturperiode im Sommer 2019. Wir konnten diesen Prozess zwar mit einer ersten Stellungnahme begleiten, da wir vom Ministerium des Innern und für Kommunales frühzeitig beteiligt wurden. Angesichts des Zeitdrucks und kurzer Fristen war die gebotene tiefergehende Befassung mit dem Gesetzentwurf jedoch nicht möglich. Wir haben uns daher dafür ausgesprochen, das Vorhaben auf den Beginn der neuen Wahlperiode zu verschieben. Dem folgte die Landesregierung nicht. Der federführende Ausschuss für Inneres und Kommunales, an den der am 28. Februar 2019 ausgegebene Gesetzentwurf der Landesregierung zur Beratung überwiesen wurde, führte eine schriftliche Anhörung durch und ersuchte uns im April 2019 um eine Stellungnahme, deren wesentlichen Inhalt die Landesbeauftragte in einer nachfolgenden Ausschusssitzung nochmals erläutern konnte.

Nur wenige unserer Empfehlungen wurden im Gesetz berücksichtigt. Neben begrifflichen Besonderheiten, die von der Terminologie der Richtlinie weiterhin abweichen und in einigen Fällen Verkürzungen darstellen, sehen wir u. a. folgende Regelungsaufträge nur unzureichend umgesetzt:

- Aus der JI-Richtlinie und den vorangestellten Erwägungsgründen geht hervor, dass so weit wie möglich zwischen den personenbezogenen Daten verschiedener betroffener Personengruppen, wie zum Beispiel der Verdächtigen, Verurteilten, Opfer, Zeuginnen und Zeugen, klar zu unterscheiden ist. Dieser Ansatz wurde nicht in das brandenburgische Gesetz übernommen.

- Polizeiliches Tätigwerden zur Gefahrenabwehr oder im Strafverfolgungsbereich umfasst häufig Maßnahmen zur Datenverarbeitung, denen die betroffene Person aufgrund einer rechtlichen Verpflichtung auch gegen ihren Willen nachkommen muss. Werden Daten durch die zuständigen Behörden aufgrund einer so legitimierten Anweisung oder Anordnung verarbeitet, sieht die JI-Richtlinie vor, dass diese Datenverarbeitung grundsätzlich nicht durch eine Einwilligung der betroffenen Person gerechtfertigt werden kann. Schließlich besteht in diesen Fällen keine Freiwilligkeit, die aber ein wesentliches Element der Einwilligung ist. Nur im Ausnahmefall sollen Betroffene der Datenverarbei-

tung für präventive oder repressive Zwecke zustimmen können, insbesondere wenn dies in einer Rechtsvorschrift vorgesehen ist. Die Formulierung in der umsetzenden Norm (§ 10 BbgPJMDSG) verkennt diese scharfe Trennung, indem sie lediglich die Option erläutert, dass eine Datenverarbeitung auf der Grundlage einer Einwilligung erfolgen kann und für diesen Fall Voraussetzungen festlegt, ohne klarzustellen, auf welche Situationen sich dies beschränkt.

- Ein weiterer Kritikpunkt betraf die Aufsichtsbefugnisse der oder des Landesbeauftragten, die durch das neue Gesetz verkürzt werden. Die JI-Richtlinie verpflichtet die EU-Mitgliedstaaten dazu, wirksame Untersuchungs- und Abhilfebefugnisse zu schaffen und benennt dabei beispielhaft verschiedene, alternativ anwendbare Maßnahmen bis hin zur vorübergehenden oder endgültigen Beschränkung oder einem Verbot der Datenverarbeitung. Da Maßnahmen von Ermittlungsbehörden teilweise erheblich in das Recht auf informationelle Selbstbestimmung eingreifen, haben wir uns dafür ausgesprochen, diesen Katalog auszuschöpfen und als Ultima Ratio auch ein Verbot der Datenverarbeitung zuzulassen. Die im Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz festgelegten Befugnisse sehen dagegen ein zweistufiges System vor, das eine Anweisung, Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken, von einer vorgeschalteten erfolglosen Beanstandung oder Warnung durch die Landesbeauftragte abhängig macht. Auf die Möglichkeit, eine Datenverarbeitung zu untersagen, verzichtet das neue Gesetz vollständig.

- Schließlich haben wir bemängelt, dass auch bei technisch-organisatorischen Maßnahmen, die der Verantwortliche zu treffen hat, Abweichungen von den Vorgaben der Richtlinie zu Inkonsistenzen, Ungenauigkeiten und teilweise auch Abschwächungen der datenschutzrechtlichen Anforderungen geführt haben. So halten wir es beispielsweise für unzureichend, Sicherheitsmaßnahmen einschränkend von den Kosten für die Umsetzung abhängig zu machen (§ 17 BbgPJMDSG) oder die gebotene Trennung von Daten nach Zwecken und betroffenen Personen unter den Vorbehalt zu stellen, dass dies möglich bzw. ohne unverhältnismäßigen Aufwand möglich ist (§ 20 BbgPJMDSG).

Wie sich das neue Gesetz in der Anwendungspraxis bewährt, bleibt abzuwarten. Angesichts der Missbrauchspotenziale, die im Regelungsbereich der JI-Richtlinie bei polizeilichen Datenbeständen bestehen, kann es erforderlich werden, Umsetzungsdefizite zu beseitigen und das Gesetz nachzubessern.

7 Zahlen und Fakten

Im Berichtszeitraum erreichten uns 27 Beschwerden gegen Datenverarbeitungsvorgänge aus dem Bereich der polizeilichen Tätigkeit und drei Beschwerden, die sich ausschließlich gegen solche der Staatsanwaltschaften im Land Brandenburg richteten. Immer wieder ging es dabei um Auskunftsersuchen betroffener Personen, die nicht oder nur zum Teil erfüllt wurden, aber auch um den Fehlversand von Dokumenten mit personenbezogenen Daten an Dritte oder Fragen der Rechtmäßigkeit für polizeiliche Übermittlungsbefugnisse an andere öffentliche Stellen. Etwa 20 Prozent der Fälle bezogen sich auf die potenzielle Erfassung und Speicherung der personenbezogenen Daten der Beschwerdeführerinnen und Beschwerdeführer durch das polizeiliche Kennzeichenerfassungssystem KESY. Darüber hinaus haben wir betroffene Personen auch außerhalb von Beschwerdefällen in erheblichem Umfang beraten. Die genaue Zahl lässt sich im Nachhinein nicht angeben, da dies nur zum Teil in Akten erfasst wurde.

In sechs Fällen haben wir die Landesregierung sowie Verantwortliche in größerem Umfang beraten, so zum Beispiel die Polizei Brandenburg hinsichtlich der datenschutzrechtlichen und technisch-organisatorischen Voraussetzungen für die geplante Einführung von Körperkameras. Ein weiteres Großprojekt unter Führung des Landeskriminalamtes, das wir im Berichtsjahr beratend begleitet haben und weiter begleiten werden, ist das Landesprojekt zur Umsetzung des im Aufbau befindlichen neuen Polizeilichen Informations- und Analyseverbunds (PIAV) und des einheitlichen Fallbearbeitungssystems (eFBS). In diesem Zusammenhang nahmen wir auch am Informationsaustausch mit Vertreterinnen und Vertretern der Datenschutzaufsichtsbehörden anderer Bundesländer und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit teil. Des Weiteren haben wir zusammen mit den Aufsichtsbehörden der anderen beteiligten Bundesländer umfangreiche Beratungen im Rahmen des Aufbaus des Gemeinsamen Kommunikations- und

Dienstleistungszentrums durchgeführt. Intensive Beratungen des Ministeriums des Innern und für Kommunales erfolgten für das 12. Änderungsgesetz zum Brandenburgischen Polizeigesetz und das Umsetzungsgesetz für die Richtlinie (EU) 2016/680 (JI-Richtlinie), das Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG).

Zu den beiden letztgenannten Gesetzesvorhaben war die Landesbeauftragte im Berichtszeitraum außerdem an den jeweiligen parlamentarischen Verfahren beteiligt und hat hierzu gegenüber dem zuständigen Ausschuss des Landtages Brandenburg Stellung genommen. Gegenüber dem Verfassungsgericht des Landes Brandenburg hat die Landesbeauftragte zudem im Rahmen eines Beschwerdeverfahrens eine Stellungnahme abgegeben.

Auffällig ist, dass uns im Berichtszeitraum kein einziger Verantwortlicher Datenschutzverletzungen im Geltungsbereich der JI-Richtlinie gemeldet hat. Die mit der Umsetzung der Richtlinie in § 29 BbgPJMDSG eingefügte Verpflichtung zu derartigen Meldungen trat allerdings erst am 22. Juni 2019 in Kraft und ist vermutlich noch nicht ausreichend bekannt.

Im Berichtszeitraum hat die Landesbeauftragte eine Beanstandung nach § 25 BbgDSG in der am 24. Mai 2018 geltenden Fassung, zwei Beanstandungen nach § 36 Absatz 1 Nummer 2 BbgPJMDSG und eine Warnung nach § 36 Absatz 1 Nummer 1 BbgPJMDSG ausgesprochen.

Teil C: Die Dienststelle

1 Öffentlichkeitsarbeit

Der Safer Internet Day ist ein von der Europäischen Union initiierter, jährlich veranstalteter weltweiter Aktionstag für mehr Sicherheit im Internet. Im Berichtsjahr fand er am 5. Februar unter dem Motto „Together for a better internet“ statt. Die Landesbeauftragte beteiligte sich daran gemeinsam mit dem Ministerium der Justiz und für Europa und Verbraucherschutz sowie mit der Verbraucherzentrale Brandenburg. Ihre Mitarbeiterinnen und Mitarbeiter informierten an diesem Tag in den Bahnhofspassagen des Potsdamer Hauptbahnhofs zum Thema „Im Netz? Mit Sicherheit!“. Schwerpunkt der Aktion war die Sicherheit von Smartphones. Passantinnen und Passanten erhielten einfach umzusetzende Hinweise, mit denen sich verhindern lässt, dass die eigenen Daten auf dem Smartphone in falsche Hände geraten.

Die Sicherheit von Smartphones war auch Thema eines Informationsstandes der Landesbeauftragten auf dem Tag der offenen Tür im Landtag Brandenburg am 6. April 2019. In einer spielerischen Umfrage haben wir Besucherinnen und Besucher unseres Standes gebeten, einige Fragen zur Nutzung des Smartphones zu beantworten. Uns interessierte, welche Sicherheitsmaßnahmen sie konkret umsetzen. Die unerwartet rege Beteiligung haben wir zum Anlass genommen, die Ergebnisse – selbstverständlich anonym – auszuwerten. Auch wenn die 215 Antworten sicher nicht repräsentativ sind: Um bei Verlust oder Diebstahl des Mobiltelefons einen Basisschutz vor unbefugtem Zugriff auf persönliche Daten zu gewährleisten, nutzten 83 % der Befragten eine Zugangssperre bei ihrem Smartphone. 74 % der Befragten gaben an, regelmäßig aktuelle Sicherheitsupdates zu installieren. Regelmäßige Daten-Backups setzten allerdings nur 42 % um. Eine mögliche Erklärung für die geringere Nutzungsrate – im Verhältnis zu den anderen erwähnten Methoden – könnte die komplexere technische Umsetzung sein. Eine Vielzahl der Teilnehmerinnen und Teilnehmer war sich der Risiken bewusst, die eine permanente und uneingeschränkte Nutzung von Ortungsdiensten wie GPS bedeuten kann. 59 % der Befragten achteten auf einen bewussten Umgang mit diesem Dienst und deaktivierten ihn, wenn sie ihn nicht benötigten. Etwas mehr als 50 % achteten nicht auf die Deaktivierung der WLAN-Schnittstelle ihres Mobilgerätes, wenn sie diese nicht benötigten. Insgesamt lässt sich das Bewusstsein der Befragten für die Sicherheit von Smartphones also durchaus positiv bewerten. Bei den Fragen zu Zugangssperren und Sicherheitsupda-

tes ist festzuhalten, dass die große Mehrheit Mindeststandards des Datenschutzes für Mobilgeräte nutzt. Die Antworten auf die anderen Fragen lassen durchaus den Schluss zu, dass ein großer Anteil der bei der Umfrage mitwirkenden Gäste des Tages der offenen Tür im Landtag sich mit diesen Themen zumindest auseinandersetzt.

Seit Jahren stellt die Landesbeauftragte in ihrem Internetangebot Musterschreiben für Selbstauskünfte zur Verfügung. Diese erleichtern es Betroffenen, bei verantwortlichen Stellen Informationen über die zur eigenen Person gespeicherten Daten zu erfragen, Berichtigungen zu erreichen, Widerspruch gegen die Datenverarbeitung einzulegen und unter Umständen die Löschung der personenbezogenen Daten zu erzwingen. Im Zuge des Wirksamwerdens der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 war eine Anpassung an die neue Rechtslage erforderlich geworden, sodass wir die Musterschreiben vorübergehend vom Netz nehmen mussten. Im Berichtsjahr konnten wir sie in gründlich überarbeiteter Form wieder bereitstellen. Mehrere Auskunftsanliegen, die zuvor in separaten Vordrucken berücksichtigt wurden, haben wir zusammengefasst, sodass die Zahl der Schreiben sich zugunsten der Übersichtlichkeit reduzierte.

Die Druckbroschüre des bereits im Jahr 2018 an die neue Rechtslage angepassten Brandenburgischen Datenschutzgesetzes haben wir, nachdem die erste Auflage vergriffen war, im Berichtsjahr nachdrucken lassen. Außerdem haben wir das Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz, das die Richtlinie EU 2016/680 umsetzt, als Broschüre herausgegeben. Das Gesetz war vom Landtag Brandenburg im Juni 2019 verabschiedet worden. Inhaltlich überarbeitet und neu aufgelegt haben wir im Berichtszeitraum das Faltblatt „Digitale Angriffe? Nicht bei mir!“. Die genannten Publikationen sind auf Wunsch in Papierform kostenlos erhältlich und stehen in unserem Internetangebot in elektronischer Form zur Verfügung.

Die intensive Abstimmung zwischen den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im Rahmen der Datenschutzkonferenz schlug sich auch in der Öffentlichkeitsarbeit nieder. So beteiligte sich die Landesbeauftragte – ebenso wie die übrigen Konferenzmitglieder – an der Ausrichtung einer zentralen Veranstaltung anlässlich des 13. Europäischen Datenschutztages am 28. Januar 2019 in Berlin. Sie stand ganz im Zeichen der jüngsten

Reform des Datenschutzrechts: „Europäischer Datenschutz: Chance oder Risiko? Acht Monate Datenschutz-Grundverordnung – Bilanz und Blick nach vorn“. Die Konferenzvorsitzende des Vorjahres – die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen – hat diese Veranstaltung organisiert. Etwa 230 Gäste aus Politik, Wirtschaft, Verwaltung sowie interessierte Bürgerinnen und Bürger nahmen daran teil.

Gemeinsam mit den übrigen unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat die Landesbeauftragte mehrere neue Papiere für die Praxis des Datenschutzes in unterschiedlichen Sachgebieten veröffentlicht. Dazu zählen die Orientierungshilfe für Anbieter von Telemedien, die Orientierungshilfe mit Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung sowie die Orientierungshilfe zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen. In drei Positionspapieren legt die Konferenz ihre Rechtsauffassung zur biometrischen Analyse, zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (mittels sog. Dashcams) sowie zur Nutzung von Kameradrohnen durch nicht öffentliche Stellen dar. Das Whitepaper „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“ dient der öffentlichen Konsultation. Veröffentlicht hat die Konferenz darüber hinaus ein Prüfschema zum Datenschutz bei Windows 10 sowie eine Beschreibung des Akkreditierungsprozesses für den Bereich „Datenschutz“ gemäß Artikel 42, 43 DS-GVO. Das Standard-Datenschutzmodell – eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele – liegt inzwischen in einer überarbeiteten Version 2.0 vor. Im Berichtszeitraum hat die Konferenz ein weiteres Kurzpapier erarbeitet, das die Einwilligung nach der Datenschutz-Grundverordnung behandelt. Bei den inzwischen 20 Kurzpapieren handelt es sich um Hilfestellungen für kleine und mittlere Unternehmen bei der Umsetzung der neuen Rechtslage. Die genannten Dokumente stehen in unserem Internetangebot in elektronischer Form zur Verfügung.

In gleicher Weise veröffentlicht die Landesbeauftragte auch die vom Europäischen Datenschutzausschuss herausgegebenen Leitlinien. Im Berichtsjahr waren dies die Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen gemäß der Verordnung (EU) 2016/679 sowie die Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten unter Artikel 6 Absatz 1 Buchstabe b DS-GVO im Zusammenhang mit der Bereitstellung von Online-Diensten für

betroffene Personen. Weitere Leitlinien des Ausschusses (z. B. zur Videoüberwachung und zum Recht auf Vergessenwerden) befinden sich gegenwärtig in der öffentlichen Konsultation. Alle Dokumente werden sukzessive in die deutsche Sprache übersetzt.

2 Pressearbeit

Aus Anlass des Safer Internet Days am 5. Februar 2019 informierten die Landesbeauftragte, das Ministerium der Justiz und für Europa und Verbraucherschutz und die Verbraucherzentrale Brandenburg in einer Presseinformation über ihre an diesem Tag gemeinsam durchgeführte Aktion „Sichern Sie Ihr Smartphone“. Mitarbeiterinnen und Mitarbeiter aller drei Einrichtungen gaben hierzu in den Bahnhofspassagen des Potsdamer Hauptbahnhofs praktische Hinweise.

Ende März informierten wir über ein Urteil des Bundesverwaltungsgerichts vom 27. März 2019 zur Videoüberwachung in einer brandenburgischen Zahnarztpraxis. Die Landesbeauftragte hatte der Zahnärztin aufgegeben, die Kamera so auszurichten, dass der für Patientinnen und Patienten und sonstige Besucherinnen und Besucher zugängliche Bereich nicht mehr erfasst wird. Die Rechtmäßigkeit dieser Anordnung hat das Bundesverwaltungsgericht in einem Revisionsverfahren bestätigt. Über den Einzelfall hinaus kam der Entscheidung eine grundsätzliche datenschutzrechtliche Bedeutung zu. Die Richterinnen und Richter bestätigten darin auch die zuvor teilweise bestrittene Rechtsauffassung der Datenschutzaufsichtsbehörden zum Vorrang des Unionsrechts vor dem Bundesdatenschutzgesetz auf dem Gebiet der Videoüberwachung durch Private.

Am 25. Mai 2019 zog die Landesbeauftragte anlässlich des ersten Jahrestages der Geltung der Datenschutz-Grundverordnung eine erste Bilanz. Als positiv bewertete sie die Stärkung des Datenschutzes als Bürgerrecht, ein deutlich gestiegenes Bewusstsein auf allen Ebenen und die internationale Signalwirkung. Allerdings wies sie auch kritisch auf den Nachholbedarf so mancher Verantwortlicher sowie auf den Zuwachs vielfältiger neuer Aufgaben ihrer eigenen Behörde bei knappen Ressourcen hin.

Im Vorfeld der Wahlen zum Landtag Brandenburg rief die Datenschutzbeauftragte die Parteien zu einem sorgsamen Umgang mit Wählerdaten auf. Auch hier gelten die Vorschriften der Datenschutz-

Grundverordnung. Dies betrifft beispielsweise den Umgang mit Auskünften aus dem Melderegister, den Versand von Wahlwerbung, den Haustürwahlkampf und den Einsatz sozialer Netzwerke. Wir boten in diesem Zusammenhang ausdrücklich unsere Beratung an.

Am 20. August 2019 machten wir die Beanstandung der Landesbeauftragten gegenüber dem Polizeipräsidium Brandenburg publik. Grund war dessen mangelnde Unterstützung im Rahmen einer datenschutzrechtlichen Prüfung des Systems zur automatisierten Kennzeichenfahndung (KESY) – das Polizeipräsidium hatte der Datenschutzaufsichtsbehörde die Einsicht in gerichtliche Beschlüsse bzw. staatsanwaltschaftliche Anordnungen verweigert. Die Frage der Zulässigkeit der automatisierten Kennzeichenfahndung auf brandenburgischen Autobahnen sowie die Prüftätigkeit der Landesbeauftragten waren im Berichtsjahr wochenlang intensiv in den Medien diskutiert worden.

Im Sommer häuften sich Hinweise auf Akten, die auf frei zugänglichen Flächen oder in ungenutzten Gebäuden herumlagen und teilweise sogar Sozialdaten enthielten. Dies nahmen wir am 11. September 2019 zum Anlass, über die entsprechenden Aufsichts- und Bußgeldverfahren unserer Behörde zur Ahndung dieser Datenschutzverstöße zu informieren. Außerdem rief die Landesbeauftragte in ihrer Presseinformation Unternehmen und Vereine auf, Datensicherheit sowohl bei der elektronischen Datenverarbeitung als auch beim Umgang mit Papierakten als Daueraufgabe wahrzunehmen.

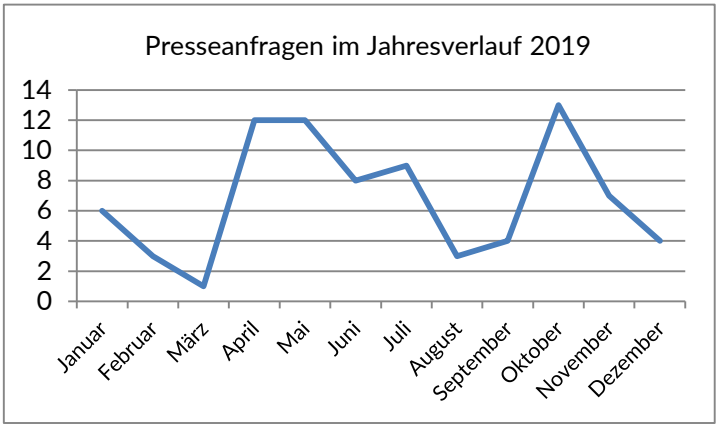
Ein Urteil des Europäischen Gerichtshofs vom 1. Oktober 2019 beantwortete die lange umstrittene Frage, wie Cookies datenschutzgerecht eingesetzt werden können. Aus diesem Anlass informierte die Landesbeauftragte am 7. Oktober 2019 über ihre Forderung an öffentliche Stellen, Unternehmen und Vereine in Brandenburg, die Cookie-Funktionen ihrer Webseiten zu überprüfen und verständliche Optionen für die erforderliche Einwilligung der Nutzerinnen und Nutzer anzubieten.

Aus Anlass zahlreicher Beschwerden über und Hinweise auf die unzulässige Einbindung von Analyse-Diensten auf Webseiten brandenburgischer Betreiberinnen und Betreiber wies die Landesbeauftragte im November 2019 darauf hin, dass diese eine wirksame Einwilligung der Besucherinnen und Besucher benötigen, wenn sie Dienste Dritter einbinden. Sie forderte die Verantwortlichen auf, ihre Web-

seiten auf die Zulässigkeit von Analyse-Tools und Tracking-Mechanismen zu überprüfen und kündigte im Falle der Beschwerden und Hinweise ihre aufsichtsrechtliche Prüfung an.

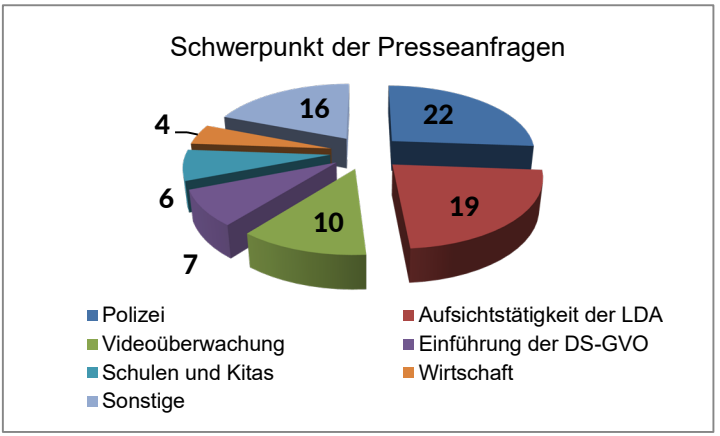
Bei den 84 im Jahresverlauf an die Landesbeauftragte gerichteten Presseanfragen lassen sich zwei deutliche Schwerpunkte ausmachen: Im April und Mai 2019 berichteten viele Medien über die Erfahrungen der Aufsichtsbehörden im ersten Jahr nach der Einführung der Datenschutz-Grundverordnung. In den an uns gerichteten Anfragen ging es neben einer Einschätzung dieser Erfahrungen vor allem um statistische Angaben zur Anzahl der Beschwerden, der verhängten Bußgelder, zu Sanktionen und Maßnahmen sowie zur Zahl der gemeldeten Datenschutzverstöße. Zwar hat der Neuigkeitswert der Datenschutzreform ganz offensichtlich nachgelassen – die Anfragen zur Einführung des neuen Datenschutzrechts nahmen erwartungsgemäß deutlich ab. Das Interesse an der Aufsichtstätigkeit der Landesbeauftragten war jedoch nur unwesentlich geringer als im Vorjahr.

Im Oktober 2019 war die datenschutzrechtliche Einschätzung der Landesbeauftragten zur Rechtsgrundlage für die automatisierte Kennzeichenfahndung im Zusammenhang mit einem entsprechenden Verfahren vor dem Landesverfassungsgericht Brandenburg am häufigsten gefragt. Auf diesem Thema lag eindeutig der inhaltliche



Schwerpunkt der Anfragen des Jahres 2019. Das Interesse an KESY erklärt zugleich den größten Teil der Anfragen, die uns im Wesentlichen seit dem Frühjahr 2019 zur Tätigkeit der Polizeibehörden erreichten.

Ein weiterer inhaltlicher Schwerpunkt der Presseanfragen lag auf dem Thema Videoüberwachung. Hier interessierten sich die Medien für ganz unterschiedliche Arten des Kameraeinsatzes – von der Webcam über die Übertragung von Gremiensitzungen, den Einsatz in einer Schule, Kamerafahrten für elektronische Kartendienste bis hin zur Verkehrsüberwachung. Die Fragen zur Videoüberwachung verteilten sich im Gegensatz zu den beiden anderen Schwerpunkten mehr oder weniger gleichmäßig über das Jahr.



Wie bereits im Vorjahr stellten wir fest, dass die meisten Anfragen – etwa 45 % – von Journalistinnen und Journalisten gestellt werden, die für Tageszeitungen recherchieren. Das Interesse von Fernsehen, Online-Medien sowie Nachrichtenagenturen beläuft sich jeweils auf etwas mehr als ein Zehntel der gesamten Pressekontakte. Weit über die Hälfte der Anfragen stammt von Medien aus der Region; etwas mehr als ein Drittel hat einen überregionalen Bezug und nur knapp fünf Prozent der Kontakte reichen über die Grenzen der Bundesrepublik Deutschland hinaus.

3 Personal und Organisation der Dienststelle

Im Berichtsjahr hat die Dienststelle insgesamt fast zwei Dutzend Stellenbesetzungsverfahren durchgeführt. Dies wurde deshalb erforderlich, weil mir der Landtag für den Doppelhaushalt 2019/2020 fünf neue Stellen bewilligt hat. Darüber hinaus waren sie veranlasst durch den Wechsel von Beschäftigten zu anderen Arbeitgeberinnen und Arbeitgebern oder Dienststellen im Land Brandenburg, die Vertretung von Elternzeiten, das Erreichen der gesetzlichen Altersgrenze sowie das Erringen eines Landtagsmandats.

Während die Stellenbesetzungen sowohl im juristischen als auch im Verwaltungs- und Sekretariatsbereich erfolgreich mit qualifizierten Mitarbeiterinnen und Mitarbeitern gelangen, war der Fachkräftemangel an Informatikerinnen und Informatikern deutlich zu spüren. Im Laufe des Berichtsjahres waren zeitweise nicht einmal die Hälfte der Stellen im Bereich Technik und Organisation besetzt. Dies erschwerte unsere Arbeit erheblich. Bis zum Ende des Berichtsjahres konnten zwei Informatiker eingestellt werden; drei Stellen bleiben allerdings noch vakant.

Im Tätigkeitsbericht 2018 hatte ich bereits darüber informiert, welche neuen inhaltlichen und organisatorischen Aufgaben meine Dienststelle im Zuge der intensivierten Zusammenarbeit der europäischen Aufsichtsbehörden seit Mai 2018 zu bearbeiten hat. Nicht nur Beschwerden zu grenzüberschreitenden Datenverarbeitungsprozessen erfordern eine enge Abstimmung zwischen den betroffenen europäischen Aufsichtsbehörden. Auch davon losgelöst stimmen sich die europäischen Datenschutzaufsichtsbehörden zunehmend intensiv ab, um das Recht einheitlich anzuwenden. Bereits nach einigen Monaten der europaweiten Kooperation hat sich herausgestellt, dass die Befassung mit grenzüberschreitenden Sachverhalten sowie die erforderlichen Abstimmungsverfahren im Rahmen der bisherigen Organisation in meiner Dienststelle außerordentlich aufwändig waren. Dies liegt nicht zuletzt daran, dass die europäische Kooperation in englischer Sprache geführt wird und der Nutzung eines spezifischen Informationssystems bedarf.

Um die Prozesse effektiver zu gestalten, habe ich die europäischen Aufgaben zu Beginn des Berichtsjahres in einer eigenständigen Organisationseinheit (Europa-IMI-Stelle) gebündelt. Hierfür wurde u. a.

ein eigenes Postfach eingerichtet, über das meine Dienststelle auch für Kolleginnen und Kollegen aus anderen Mitgliedstaaten erreichbar ist und die Kommunikation zu europäischen Kooperationsverfahren zentral verwaltet wird. Betreut wird die Europa-IMI-Stelle von drei Referentinnen und Referenten, die hierfür teilweise von anderen Aufgaben entlastet wurden und Unterstützung durch das Sekretariat erhalten.

Die Pläne, meine Dienststelle von Kleinmachnow in die Landeshauptstadt Potsdam zu verlegen, zerschlugen sich im Berichtsjahr leider erneut. Der bestehenden Raumnot am aktuellen Dienstsitz konnte nur noch durch die Aufgabe zahlreicher Funktionsräume und die Teilung eines Beratungsraums in zwei zusätzliche Büros begegnet werden. Sämtliche Notlösungen sind inzwischen ausgeschöpft. Darüber hinaus ist die fehlende Barrierefreiheit nach wie vor ein Problem – auch für Bürgerinnen und Bürger, die die Dienststelle besuchen. Da die derzeitige räumliche Situation für die Beschäftigten zunehmend belastend ist und die Aufgabenerfüllung erschwert, werde ich mich weiter aktiv bemühen, die Unterbringung der Dienststelle in der Landeshauptstadt Potsdam zu realisieren. Hierbei hoffe ich auf die Unterstützung des Landtages und der Landesregierung.

4 Neue Aufgaben der Landesbeauftragten in den Datenschutzgremien

4.1 Vorsitz in einem nationalen Arbeitskreis

Auf Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder habe ich den Vorsitz des Arbeitskreises Verwaltung von meinem sächsischen Kollegen übernommen. Gleichzeitig wurden die Themenfelder, die der Arbeitskreis bearbeitet, erheblich ausgeweitet. Vor dem Hintergrund der geplanten umfassenden Digitalisierung der Verwaltung – auch im Kontext der Umsetzung des Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen – sind bundesweit tiefgreifende Änderungen in der deutschen Verwaltungslandschaft zu erwarten, die auch eine aktive Begleitung und Mitwirkung der Datenschutzaufsichtsbehörden erfordern. Mit der Leitung des Arbeitskreises unterstützt meine Dienststelle diese Prozesse künftig aktiv.

Die Konferenz hat mehrere Arbeitskreise eingerichtet. Sie arbeiten ihr zu, indem sie gemeinsame Positionen auf Arbeitsebene abstim-

men und Entscheidungen vorbereiten. Diese Arbeitskreise decken verschiedene fachliche Fragestellungen zu rechtlichen und technisch-organisatorischen Aspekten des Datenschutzes ab. Üblicherweise führt jeweils ein Konferenzmitglied den Vorsitz eines Arbeitskreises. Ihm kommt neben der organisatorischen Vorbereitung der in den meisten Fällen halbjährlichen Sitzungen auch die Federführung für die inhaltlichen Arbeiten des Gremiums sowie die Koordination der Zusammenarbeit der teilnehmenden Datenschutzaufsichtsbehörden zu.

4.2 Ländervertretung in einer europäischen Arbeitsgruppe

Im Berichtszeitraum habe ich die Vertretung der unabhängigen Datenschutzaufsichtsbehörden der Länder in der Compliance, E-Government und Health Expert Subgroup des Europäischen Datenschutzausschusses übernommen. Diese Subgroup ist bereits ausweislich ihrer Bezeichnung für ein umfangreiches Fachgebiet zuständig. Als eine von mehreren Arbeitsgruppen unterstützt sie den Europäischen Datenschutzausschuss bei seiner europaweiten Aufgabe, eine einheitliche Anwendung der Datenschutzvorschriften zu fördern.

Meine Dienststelle hat damit künftig die Aufgabe, die Zusammenarbeit der unabhängigen Datenschutzaufsichtsbehörden der Länder innerhalb der Subgroup zu koordinieren sowie deren Positionen zu Stellungnahmen, Leitlinien, Empfehlungen sowie weiteren Entscheidungen des Europäischen Datenschutzausschusses inhaltlich abzustimmen. Neben den Ländern ist auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in der Subgroup vertreten, mit dem ich intensiv kooperiere. Üblicherweise finden die europäischen Gremiensitzungen in Brüssel statt und werden in englischer Sprache absolviert. Dies bringt im Gegensatz zur Teilnahme an nationalen Gremiensitzungen einen erhöhten Aufwand für Dienstreisen und fremdsprachliche Vorbereitung umfangreicher Unterlagen mit sich.

Kontakt

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

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

WWW.LDA.BRANDENBURG.DE