Landesbeauftragte
für Datenschutz
und Akteneinsicht

Tätigkeitsbericht 2018
Datenschutz

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

Titelbild: © Kai_Vogel / www.pixabay.com

Tätigkeitsbericht Datenschutz

der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zum 31. Dezember 2018

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat nach Artikel 59 Datenschutz-Grundverordnung einen Jahresbericht über ihre Tätigkeit zu erstellen und dem Landtag sowie der Landesregierung zu übermitteln. Dieser Bericht schließt an den am 18. April 2018 vorgelegten Tätigkeitsbericht 2016/2017 an und deckt den Zeitraum vom 1. Januar bis zum 31. Dezember 2018 ab.

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

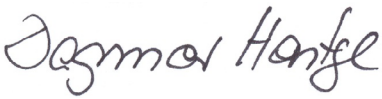
Vorwort

Liebe Leserinnen und Leser,

aufgrund der neuen Rechtslage umfassen meine Tätigkeitsberichte zum Datenschutz künftig nur noch ein Kalenderjahr. Über meine Aufgaben nach dem Akteneinsichts- und Informationszugangsgesetz werde ich wie gewohnt alle zwei Jahre informieren – künftig aber in Form eines eigenständigen Berichts.

Mein aktueller Tätigkeitsbericht zum Datenschutz erscheint nicht nur äußerlich in einem moderneren Gewand, sondern ist im Vergleich zu früheren Berichten auch wesentlich kürzer. Die Straffung ergibt sich nicht zuletzt aus der Verkürzung des Berichtszeitraums. Zudem unterscheidet sich die Gliederung seines Inhalts von der Aufteilung in früheren Berichten. Sie differenziert jetzt deutlicher zwischen Prüfungen, Beratungen und Sanktionen. Nach der Devise „weniger ist mehr“ fokussiert sich die Darstellung auf ausgewählte Fälle und Projekte. Neu ist ein Abschnitt, der die Tätigkeit meiner Behörde statistisch darstellt. Die Einführung der Datenschutz-Grundverordnung hat unsere Arbeit im zurückliegenden Jahr wesentlich geprägt; dies spiegelt sich in einem eigenen Schwerpunktkapitel wider. Selbstverständlich berichte ich auch über Fälle, die meine Mitarbeiterinnen und Mitarbeiter in den ersten fünf Monaten des Jahres auf der Grundlage des damals geltenden Datenschutzrechts bearbeitet haben.

Beim Lesen meines Tätigkeitsberichts werden Sie feststellen: 2018 war ein bewegtes Jahr für den Datenschutz. Ich hoffe, dass die neue Berichtsform dem gestiegenen Interesse am Datenschutz entgegenkommt und wünsche Ihnen eine interessante Lektüre.



Dagmar Hartge

Kapitel I
Schwerpunkte

I Schwerpunkte

1 Die Datenschutz-Grundverordnung – ein Update mit Startschwierigkeiten

Das Berichtsjahr brachte neue Herausforderungen mit sich – nicht nur für öffentliche und nicht öffentliche Stellen, die personenbezogene Daten verarbeiten (die sog. Verantwortlichen), sondern auch für die Landesbeauftragte:

Am 25. Mai 2018 begann eine neue Datenschutz-Ära. Von diesem Tag an wurde die Datenschutz-Grundverordnung (DS-GVO) nach einer zweijährigen Übergangszeit in allen Mitgliedstaaten der EU wirksam. Ab diesem Tag galt ein neues EU-weit einheitliches Datenschutzrecht. Ein wesentliches Ziel war, die grenzüberschreitend tätigen Unternehmen nunmehr in allen EU-Mitgliedstaaten den gleichen gesetzlichen Anforderungen an den Datenschutz zu unterwerfen. Bürgerinnen und Bürger können sich zukünftig bei Beschwerden über Unternehmen mit Sitz in einem anderen Mitgliedstaat an ihre lokale Aufsichtsbehörde wenden, Unternehmen haben nur mit einer Aufsichtsbehörde, und zwar der im Land ihrer Hauptniederlassung, zu tun (One-Stop-Shop). Damit ist sowohl dem Interesse der Bürgerinnen und Bürger in der EU an einem effektiven Datenschutz gedient als auch dem Interesse der Unternehmen an einheitlichen Wettbewerbsbedingungen und nur einem Ansprechpartner in Datenschutzfragen.

Zur Gewährleistung einer einheitlichen Anwendung der Datenschutz-Grundverordnung in allen Mitgliedstaaten wurde der Europäische Datenschutzausschuss (EDSA) geschaffen, in dem aus jedem Mitgliedstaat die Leitung einer Datenschutzaufsichtsbehörde vertreten ist. Gemeinsamer Vertreter für die deutschen Aufsichtsbehörden ist die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Zu den wesentlichen Aufgaben dieses Ausschusses gehört es, die einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen und bei unterschiedlichen Auffassungen unter den Aufsichtsbehörden der Mitgliedstaaten in Einzelfällen den Streit durch verbindliche Entscheidungen beizulegen. Ein wichtiges Instrument des EDSA ist die Erstellung verbindlicher Leitlinien (Guidelines) und Empfehlungen zur Datenschutz-Grundverordnung, die auch die Landesbeauftragte bei ihrer Arbeit zu beachten hat.

Im Vorgriff auf seine Konstituierung hatte das Vorläufergremium, die Artikel-29-Datenschutzgruppe, bereits erste Leitlinien erlassen, die später vom EDSA gebilligt wurden. Sie beantworten aber längst noch nicht alle Fragen, die sich bei der Anwendung des neuen Datenschutzrechts ergeben.

Im Zusammenhang mit Auslegungsfragen und Beratungsersuchen betonte die Landesbeauftragte immer wieder, dass ihre Auskünfte unter dem Vorbehalt zukünftiger Hinweise und Entscheidungen des EDSA stehen. Auch die von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder erarbeiteten 19 Kurzpapiere weisen ausdrücklich auf den Vorrang der Auslegung durch den EDSA hin. Diese Kurzpapiere wurden erstellt, nachdem klar war, dass der EDSA nicht in der Lage sein würde, kurzfristig Aussagen zu konkreten Auslegungsfragen zu treffen. Sie stießen auf großes Interesse.

Die Landesbeauftragte wurde mit Anfragen von Betroffenen und Verantwortlichen gleichermaßen überhäuft. Obwohl sich gerade für die Unternehmen mit Sitz in Deutschland die Änderungen gegenüber dem vorhergehenden Recht auf einige – wenn auch wichtige – Teilaspekte beschränkten, vermittelten die Verantwortlichen vielfach den Eindruck, der Datenschutz sei vollkommen neu erfunden worden, und die Kosten für die Umsetzung würden sie an den Rand des Ruins bringen. Wer jedoch schon nach altem Recht seine Hausaufgaben gemacht hatte, war durch die neu hinzukommenden Anforderungen keineswegs überlastet.

Die Arbeitsweise der Landesbeauftragten hat sich mit Wirksamwerden der Datenschutz-Grundverordnung erheblich verändert. Dies liegt nicht nur an den neuen inhaltlichen Vorschriften und dem stärkeren EU-Bezug. Auch wurde das behördliche Verfahren der Datenschutzaufsicht und -kontrolle im Vergleich zur vorherigen Rechtslage deutlich formalisiert. Die Landesbeauftragte muss ihre Entscheidungen nunmehr in förmlichen Verfahren nach dem Verwaltungsverfahrensgesetz treffen und sie in der Regel mit einem rechtsmittelfähigen Bescheid abschließen. Verantwortliche (öffentliche und nicht öffentliche Stellen) werden zuvor formell angehört, etwa bevor sie zur Auskunft verpflichtet werden oder ihnen eine Verwarnung oder Anweisung erteilt wird oder wenn gegen sie eine sonstige Abhilfemaßnahme im Sinne des Artikel 58 Absatz 2 DS-GVO erlassen wird. Auf der anderen Seite sind die Beschwerdeführerinnen und

Beschwerdeführer innerhalb von drei Monaten über den Stand des Verfahrens und nach dessen Abschluss über das Ergebnis ihrer Beschwerde zu unterrichten. Bei Nichtbeachtung der Frist oder wenn sie das Ergebnis für unzureichend erachten, haben sie das Recht der gerichtlichen Überprüfung.

Mit zunehmendem zeitlichen Abstand zum 25. Mai 2018 hat sich die anfängliche Aufregung weitgehend gelegt und auch die Unsicherheiten bei der Auslegung und Anwendung der Datenschutz-Grundverordnung konnten zu einem großen Teil behoben werden. Dennoch besteht weiterhin ein großer Abstimmungsbedarf mit und zwischen den Aufsichtsbehörden. Vor allem hat sich gezeigt, dass die Zusammenarbeit – gerade bei grenzüberschreitenden Fällen – komplex und langwierig ist. Gleiches gilt für die Erstellung von Leitlinien und Empfehlungen durch den Europäischen Datenschutzausschuss.

2 Beratungsbedarf zur Umsetzung der Datenschutz-Grundverordnung

2.1 Schulungsveranstaltungen der Landesbeauftragten

Mit der Datenschutz-Grundverordnung wurde der Datenschutz zwar nicht neu erfunden; seit Mai 2018 gelten jedoch einige wesentliche Änderungen. Diese haben unmittelbar Einfluss auf die Verarbeitung personenbezogener Daten bei öffentlichen und nicht öffentlichen Stellen des Landes Brandenburg. Bereits während der zweijährigen Übergangsphase war die Verunsicherung bei brandenburgischen Unternehmen und Verwaltungen über die neuen Anforderungen deutlich spürbar. Viele von ihnen haben die Landesbeauftragte daher gebeten, den Umsetzungsprozess zu unterstützen. Vor diesem Hintergrund planten wir frühzeitig eine Fortbildungsreihe.

Bedingt durch die hohe Nachfrage standen wir vor großen Herausforderungen, Veranstaltungspartnerinnen und -partner vor Ort zu finden, teilweise zu motivieren und zu koordinieren. In Kooperation mit Wirtschaftsverbänden, Industrie- und Handelskammern, Bildungs- und Sozialeinrichtungen, mit Ministerien, nachgeordneten Behörden sowie Landkreis- und andere Kommunalverwaltungen konnten wir von Januar bis Juni des Berichtszeitraums fast 40 Veranstaltungen mit insgesamt über 1900 Führungskräften und Datenschutzverantwortlichen durchführen.

Unser Ziel war es, den Teilnehmenden einen Gesamtüberblick über die ihnen teils unbekannte Materie zu vermitteln und einen möglichst einheitlichen Kenntnisstand auf der Führungskräfteebene zu erreichen. Auch wenn die Umsetzung der Verordnung grundsätzlich alle Beschäftigten betrifft, stehen Führungskräfte hierbei in einer besonderen Verantwortung. Dies gilt sowohl für die Leitung und Lenkung der Tätigkeiten in der jeweiligen Organisationseinheit als auch für die Initiierung, Steuerung und Kontrolle der Umsetzungsprozesse. Und letztendlich sind Führungskräfte immer auch Vorbild. Wie sich aus der regen Veranstaltungsteilnahme von Hauptverwaltungsbeamtinnen und -beamten sowie Leiterinnen und Leiter von Fachbereichen, Ämtern, Dezernaten, Schulen, Unternehmen u. a. schlussfolgern ließ, stieß diese Betrachtungsweise auf Zustimmung. Außerdem nahmen zahlreiche behördliche und betriebliche Datenschutzbeauftragte sowie interessierte Beschäftigte teil.

Schulungen sorgen für mehr Klarheit.

Das Datenschutzrecht besteht – im Gegensatz zu vielen anderen Rechtsgebieten – zu einem großen Teil aus technisch-organisatorischen Anforderungen. Dieses Zusammenspiel rechtlicher und technischer Aspekte sollte sich auch in unseren Fortbildungen widerspiegeln, weshalb wir in der Regel mit je einer Referentin bzw. einem Referenten aus dem Bereich Recht sowie aus dem Bereich Technik und Organisation durch die Schulung geführt haben. Die Teilnehmerinnen und Teilnehmer nahmen dabei die Gelegenheit wahr, uns in den zwei- bis dreistündigen Veranstaltungen Fragen aus der Praxis zu stellen und angeregt zu diskutieren. Dieser persönliche Kontakt war auch für uns eine willkommene Bereicherung, da wir so aus erster Hand die Probleme vor Ort und weiteren Beratungsbedarf bei der Gesetzesanwendung feststellen konnten.

Im Ergebnis ist die Resonanz auf das bereits 2017 initiierte Projekt durchweg positiv zu bewerten – trotz des einen oder anderen Kopfschüttlers über die neuen Anforderungen.

2.2 Anfragen aus der Wirtschaft

Uns erreichten im Berichtszeitraum auch aus dem nicht öffentlichen Bereich zahlreiche Anfragen zu datenschutzrechtlichen Fragestellungen und insbesondere zur Umsetzung der Anforderungen der

Datenschutz-Grundverordnung. Vor allem wandten sich kleine und mittlere Unternehmen an uns und suchten Orientierung. Neben allgemeinen Fragen zum Anwendungsbereich der Grundverordnung und zum Begriff des personenbezogenen Datums lagen die Schwerpunkte bei der Anfertigung von und dem Umgang mit Fotografien, bei der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten sowie bei der Abgrenzung von Sachverhalten, die als Auftragsverarbeitung besonderen Anforderungen unterliegen.

Auch war ein gestiegener Beratungsbedarf hinsichtlich der Umsetzung der Rechte der betroffenen Personen zu verzeichnen. Diesen steht etwa nach Artikel 15 Datenschutz-Grundverordnung ein Recht auf umfassende Auskunft über die sie betreffenden personenbezogenen Daten sowie über den Umgang mit ihnen zu. Die verantwortlichen Unternehmen haben der Antrag stellenden Person diese Angaben grundsätzlich unverzüglich zur Verfügung zu stellen. Sie müssen vor diesem Hintergrund Vorkehrungen treffen, um den Anträgen schnell und umfassend entsprechen zu können. Die Art und Weise sowie der Umfang der Auskunftserteilung war dabei gleichermaßen Gegenstand von Beratungsanfragen wie von Beschwerden. So forderten Unternehmen für die Identifizierung der Antrag stellenden Personen häufig vollständige und ungeschwärzte Ausweiskopien, obwohl dies in den konkreten Fällen nicht erforderlich war.

Daneben erreichten die Landesbeauftragte zahlreiche Anfragen zur Zulässigkeit von Werbemaßnahmen, insbesondere wenn Unternehmen diese per Post oder E-Mail versandten. In unseren Antworten zeigten wir zum einen die Grenzen der zulässigen Werbeansprache auf, betonten zum anderen aber auch, dass sie nicht in allen Fällen einer Einwilligung bedarf.

Erhebliche Unsicherheiten bestanden auch bei der Wahl der richtigen Rechtsgrundlage für einzelne Verarbeitungstätigkeiten. Oft wurde die Einwilligung der betroffenen Personen eingeholt, obwohl eine andere Rechtsgrundlage die Datenverarbeitung erlaubt hätte. Nach der Datenschutz-Grundverordnung ist eine solche auch gestattet, wenn sie z. B. für die Erfüllung eines Vertrags oder – sofern die Interessen und Grundrechte der betroffenen Person nicht überwiegen – zur Wahrnehmung eigener berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Eine Einwilligung kann jederzeit widerrufen werden. Im Fall eines Widerrufs wäre die

Verarbeitung der Daten der betroffenen Personen unverzüglich zu beenden.

Abgesehen von den rechtlichen Anforderungen stellten sich wiederholt Fragen zu den technischen und organisatorischen Maßnahmen, die der Verantwortliche treffen muss, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau für die Rechte und Freiheiten der betroffenen Personen gewährleisten zu können. Hier spielten insbesondere die Auswahl geeigneter und angemessener Maßnahmen, die Datenschutz-Folgenabschätzung sowie Datenschutz durch Technikgestaltung und datenschutzgerechte Voreinstellungen eine Rolle. Thematisiert wurde unter anderem die Notwendigkeit einer verschlüsselten Datenübertragung bei der Nutzung von Kontaktformularen auf Webseiten wie auch die Sicherstellung der Wiederherstellbarkeit der verarbeiteten personenbezogenen Daten. So wurden im Berichtszeitraum wiederholt Fälle bekannt, in denen die eingesetzten IT-Systeme mit Schadsoftware infiziert wurden, welche den Zugriff und die Nutzung des Systems durch Verschlüsselung der Daten verhinderten (sog. Ransomware). Die Entschlüsselung wurde dabei häufig von der Zahlung eines Lösegeldes abhängig gemacht. Soweit kein vollständiges und aktuelles Backup der betroffenen Systeme vorliegt, kann ein solcher Vorfall zum Verlust des gesamten Kundenbestandes führen. Schon vor diesem Hintergrund betonten wir die Notwendigkeit eines entsprechenden Datensicherungskonzepts sowie insbesondere der Sensibilisierung der Mitarbeiter hinsichtlich des Umgangs mit E-Mail bzw. Spam, da die Infektion nicht selten durch E-Mails verursacht worden ist.

Unternehmen mit großen Unsicherheiten

Im Rahmen unserer Beratungstätigkeit konnten wir in den meisten Fällen die, auch medial geförderte, Unsicherheit bei den Wirtschaftsunternehmen ausräumen. Verschiedenste Informationsangebote der Landesbeauftragten, aber auch der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, konnten den Unternehmen Wege für die rechtmäßige Umsetzung der neuen gesetzlichen Anforderungen aufzeigen. Nur exemplarisch seien hier die Kurzpapiere sowie mehrere Orientierungshilfen der Datenschutzkonferenz genannt, z. B. zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung und zur Einholung von Selbstauskünften bei Mietinteressenten.

2.3 Anfragen von Vereinen

Besonderer Beratungsbedarf war bei Vereinen zu verzeichnen. Insbesondere kleine und ehrenamtlich tätige Vereine wandten sich mit zahlreichen Fragen an uns. Die wesentlichen Antworten wollen wir im Folgenden darstellen.

Grundsätzlich gilt, dass ein Verein gemäß Artikel 6 Absatz 1 Buchstabe b Datenschutz-Grundverordnung (DS-GVO) solche Daten der Mitglieder verarbeiten darf, die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind. Die Vereinssatzung bestimmt – soweit sie keine überraschenden oder illegitimen Inhalte aufweist – die Vereinsziele, für die die Mitgliederdaten genutzt werden können. Die Verarbeitung personenbezogener Daten, die weder für die Begründung und Durchführung des Mitgliedschaftsverhältnisses noch für die Erreichung des Vereinszwecks erforderlich ist, darf nicht auf die genannte Erlaubnisnorm gestützt werden. Dies betrifft in der Regel z. B. den Versand von Newslettern.

Ein Verein darf jedoch Mitgliedsdaten auch auf Grundlage einer Einwilligungserklärung gemäß Artikel 7 DS-GVO verarbeiten. Eine Einwilligung ist insbesondere nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht und diese zuvor ausreichend und verständlich darüber informiert worden ist, welche Daten für welchen Zweck verarbeitet werden sollen. Der Verein muss im Zweifel nachweisen können, dass die betroffenen Personen wirksam in die Verarbeitung ihrer personenbezogenen Daten eingewilligt haben. Die Einwilligungslösung kann z. B. für den Versand von Newslettern genutzt werden.

Auch müssen Vereine einen Datenschutzbeauftragten benennen, wenn die gesetzlichen Voraussetzungen für diese Pflicht erfüllt sind. Das kann insbesondere dann der Fall sein, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Vereine müssen für regelmäßige Verarbeitungen personenbezogener Daten, wie z. B. die Mitgliederverwaltung und Beitragsabrechnung, ein Verzeichnis ihrer Verarbeitungstätigkeiten führen. Daneben sind Informations- und Auskunftspflichten zu erfüllen. Beispielsweise

haben Vereinsmitglieder einen Anspruch, bereits bei der Datenerhebung umfassend über die Verarbeitung ihrer Daten informiert zu werden.

Weitergehende Informationen zum Datenschutz im Verein sind in unserem Internetangebot abrufbar.

2.4 Anfragen aus dem Gesundheitsbereich

Kurz vor dem Wirksamwerden der Datenschutz-Grundverordnung begannen vor allem Arzt- und Zahnarztpraxen, uns Fragen zur Umsetzung des neuen Rechts zu stellen. Am Telefon oder per E-Mail erhielten wir einen Eindruck davon, welche bürokratischen Blüten die Sorge angesichts der neuen Verordnung treiben kann: So wurden z. B. Patientinnen und Patienten Unterschriften unter Einwilligungserklärungen für bereits gesetzlich erlaubte Datenverarbeitungen abverlangt. Manche Praxen ließen sich die Erfüllung ihrer neuen datenschutzrechtlichen Informationspflichten durch Unterschrift bestätigen. Gern waren auch beide Anliegen miteinander in einem einzigen Dokument vermischt. Uns wurden sogar Einzelfälle bekannt, in denen die Behandlung oder die Ausstellung eines Rezepts von der Leistung einer Unterschrift durch den Patienten oder die Patientin abhängig gemacht wurden. Vereinzelt stellten Praxen zusätzliches Personal ein, um die Ausgabe und das Einscannen der Formulare zu bewältigen. Ärztinnen und Ärzte sowie Zahnärztinnen und Zahnärzte fragten sich und uns, ob der namentliche Aufruf von Patientinnen und Patienten noch möglich sei. Zugleich sahen sich einige erstmals Löschungsanträgen zu ihren Dokumentationen lange vor Ablauf der im Bürgerlichen Gesetzbuch und dem Standesrecht vorgegebenen Standard-Aufbewahrungsfrist ausgesetzt und waren angesichts der Rechtsänderung unsicher, wie sie mit solchen Anträgen der Patientinnen und Patienten umgehen sollten. Letztere wiederum waren zunächst oft felsenfest davon überzeugt, nach neuem Recht eine umgehende Löschung fordern zu können.

Informationspflichten sachgerecht umsetzen

Wir wiesen regelmäßig darauf hin, dass die datenschutzrechtliche Informationspflicht ein aktives Angebot des Verantwortlichen gegenüber den betroffenen Personen verlangt. Ein Aushang, auf den die Patientinnen und Patienten selbst aufmerksam werden müssen, genügt insoweit nicht. Wir warben auch dafür, Faltblätter zum Mit-

nehmen für diejenigen vorzuhalten, die sich zum Behandlungstermin nicht mit der Thematik befassen möchten, grundsätzlich aber informiert sein wollen. Angesichts der großen Unsicherheit haben wir Hinweise zu dieser Fragestellung erarbeitet und im Internetangebot der Landesbeauftragten veröffentlicht.

Wichtig war uns auch klarzustellen, dass die betroffenen Personen nicht verpflichtet sind, auf das Informationsangebot einzugehen, bestätigende Unterschriften hierfür zu leisten oder Ähnliches. Die Ablehnung einer Behandlung kann nicht damit begründet werden, dass sich eine Patientin oder ein Patient weigert, der Praxis die Erfüllung ihrer Informationspflicht zu bestätigen. Vielmehr genügt als Nachweis dieser Pflicht eine interne Notiz des Verantwortlichen z. B. in der Patientenakte. Hierzu hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im Herbst 2018 auch einen entsprechenden Beschluss[1] gefasst und in ihrem Internetangebot publiziert.

Wir ermutigten die Praxen, wie bisher mit den namentlichen Aufrufen fortzufahren und nur mit Personen, die dieses ablehnen, Alternativen abzusprechen. Auch stellten wir klar, dass die Aufbewahrungsfristen für ärztliche Dokumentationen als Ausnahmen von der Löschungspflicht zu berücksichtigen sind.

Nachdem die Anfragen nach einigen Monaten deutlich abgenommen haben, hoffen wir, dass sich zwischenzeitlich Verfahrensweisen etabliert haben, die rechtskonform und für beide Seiten akzeptabel sind. Durch erste Stichprobenkontrollen von Informationsformularen versuchen wir, die Fortschritte in diesem Prozess zu überprüfen.

2.5 Anfragen aus den Kommunen

Ein wichtiger Fokus der Beratungsarbeit bei der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) lag auf den Gemeinden, Ämtern und Landkreisen. Die Landesbeauftragte lud deren Entscheidungsträgerinnen und Entscheidungsträger dazu ein, sich mit Fragen und Praxisfällen, aber auch mit Sorgen und Befürchtungen an

1 Beschluss: „Ablehnung der Behandlung durch Ärztinnen und Ärzte bei Weigerung der Patientin oder des Patienten, die Kenntnisnahme der Informationen nach Art. 13 DS-GVO durch Unterschrift zu bestätigen“ vom 5. September 2018.

unsere Dienststelle zu wenden. Manches konnte am Telefon geklärt werden, anderes bedurfte genauerer Prüfung und wurde schriftlich beantwortet.

Das Beratungsangebot wurde gut angenommen, auch wenn deutlich wurde, dass sich viele Kommunen erst kurz vor oder sogar erst nach Wirksamwerden der Datenschutz-Grundverordnung mit wichtigen Umsetzungsfragen zu beschäftigen begannen. Um den Stichtag am 25. Mai 2018 kam es daher zu einer Häufung von Anfragen, die die Dienststelle nur mit Mühe und Verzögerungen beantworten konnte. Als sich allmählich die Erkenntnis durchgesetzt hatte, dass die neuen Anforderungen für die Verantwortlichen durchaus zu bewältigen waren, stabilisierten sich die Eingangszahlen – jedoch auf hohem Niveau. Inzwischen nehmen die zahlreichen Meldungen von Datenpannen nach Artikel 33 DS-GVO einen gewichtigen Anteil am Gesamtaufwand ein.

Auch Kommunen müssen ihre Prozesse an die DS-GVO anpassen

Nicht alle Fragen konnten im Vorfeld umfassend beantwortet werden – oft konnte nur die Praxis die abstrakten Normen mit Leben erfüllen. Es zeigte sich jedoch mehr und mehr, dass sich die materiellen Voraussetzungen für Datenverarbeitungsmaßnahmen in den allermeisten Fällen nicht wesentlich geändert haben. Dies erscheint angesichts der Tatsache, dass Hauptzweck der Datenschutz-Grundverordnung die europaweite Vereinheitlichung von Datenschutzanforderungen im nicht öffentlichen Bereich war, folgerichtig. Trotzdem ergaben sich auch im materiellen Recht zahlreiche Fragestellungen, aus denen wir exemplarisch zwei vorstellen:

Ein Schwerpunkt waren die Informationspflichten gemäß Artikel 13 und 14 DS-GVO. Zwar enthielt bereits das Brandenburgische Datenschutzgesetz alter Fassung (BbgDSG a. F.) sog. Aufklärungspflichten, diesen wurde jedoch in der Praxis wenig Aufmerksamkeit geschenkt. Bei der Anpassung von Verarbeitungsprozessen an die DS-GVO konnte dieser Aspekt nun nicht mehr unberücksichtigt bleiben.

Fraglich war unter anderem, unter welchen Bedingungen personenbezogene Daten als nach Artikel 13 DS-GVO „bei der betroffenen Person“ erhoben gelten, inwieweit bei mehrstufigen Verarbeitungsvorgängen die betroffene Person mehrfach zu informieren ist sowie unter welchen Voraussetzungen die Ausnahmetatbestände gemäß

Artikel 13 Absatz 4 sowie Artikel 14 Absatz 5 DS-GVO greifen und eine Benachrichtigung entfallen kann.

Ein weiterer Schwerpunkt betraf die Frage, welche Stellen datenschutzrechtlich als öffentliche und welche als nicht öffentliche Stellen gelten. Unsicherheiten ergaben sich insbesondere im Hinblick auf kommunale Eigenbetriebe, die keine eigene Rechtspersönlichkeit haben. § 2 Absatz 3 Brandenburgisches Datenschutzgesetz sieht vor, dass öffentliche Stellen, soweit sie am Wettbewerb teilnehmen und personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten, wie nicht öffentliche Stellen zu behandeln sind.

Zu beantworten war unter anderem die Frage, wie Eigenbetriebe einzuordnen sind, wenn ihre Tätigkeit nicht der Teilnahme am Wettbewerb dient, sondern eine interne Dienstleistung für die kommunale Verwaltung darstellt. In entsprechenden, an uns herangetragenen Fällen haben wir uns für eine Zuordnung zum öffentlichen Bereich ausgesprochen.

Die erforderliche Abgrenzung ist jedoch einer ständigen Weiterentwicklung unterworfen und kann nur anhand des konkreten Einzelfalls und in enger Orientierung an den Wertungen des Kommunalrechts erfolgen.

2.6 Fotografien und Datenschutz

Schon in den Monaten vor Geltungsbeginn der Datenschutz-Grundverordnung ist bei den Aufsichtsbehörden für den Datenschutz die Anzahl an Nachfragen zur Zulässigkeit von Personenfotografien spürbar gestiegen. Die Landesbeauftragte hat in diesem Zeitraum eine zunehmend besorgte mediale Berichterstattung hinsichtlich der praktischen Konsequenzen der Datenschutz-Grundverordnung wahrgenommen. Zu Beginn wurde diese Debatte teilweise sehr pauschal und negativ geführt. Das überraschte uns, denn auch nach der früheren Rechtslage war für die Anfertigung und Verwendung von Personenfotografien grundsätzlich erforderlich, dass die oder der Abgebildete einwilligt oder eine andere Rechtsgrundlage es erlaubt. Der Materie wird aufgrund des neuen Sanktionsrahmens nunmehr jedoch größere Aufmerksamkeit geschenkt.

Die Anfertigung und Verwendung von Personenfotografien ist nicht nur im klassischen künstlerischen und journalistischen Bereich rele-

vant, sondern auch für die Auftragsfotografie, die Gestaltung von Webseiten, für Veranstaltungen und Blogs sowie in der Presse- und Öffentlichkeitsarbeit von privaten und öffentlichen Stellen. Je nach Motiv, Aufnahme- und Verwendungszusammenhang sowie dem jeweils verantwortlichen Verarbeiter, kann die rechtliche Bewertung unterschiedlich ausfallen. Besondere Schwierigkeiten bereitet dabei die nicht abschließend geklärte Frage, ob und in welchem Umfang das Kunsturhebergesetz, welches seit 1907 speziell die Verbreitung und öffentliche Zurschaustellung von Bildnissen regelt, noch Anwendung findet. Für viele Verantwortliche und Betroffene bringt dies Unklarheiten und Unsicherheiten mit sich. Wir haben uns in der ersten Jahreshälfte daher entschieden, eine Handreichung zu den rechtlichen Grundsätzen und den Besonderheiten in speziellen Verarbeitungssituationen zu veröffentlichen.

Die in der Folge zurückgegangene Anzahl an allgemeinen Beratungsanfragen wurde mittlerweile durch eine zunehmende Anzahl von Beschwerden zum Thema Fotografie abgelöst. Auch hier stoßen wir jedoch immer wieder auf Fälle, in denen der Konflikt durch die oben erwähnten Unsicherheiten ausgelöst wurde. Häufig konnten wir die betroffenen Personen durch individuelle Beratung zwar unterstützen. Eine klare gesetzliche Regelung, die die derzeit vorherrschenden Unklarheiten beseitigt, wäre zugunsten von Rechtssicherheit jedoch wünschenswert. Wir erklärten uns daher auch gern bereit, als Sachverständige in einer Anhörung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtags mitzuwirken. Der Initiative lag der Antrag „Rechtssicherheit beim Fotografieren in der Öffentlichkeit erhalten“ zu Grunde. Die von uns abgegebene Stellungnahme verdeutlicht den gesetzgeberischen Handlungsbedarf und unterstützt die Bemühungen, sich für klarstellende bereichsspezifische Regelungen einzusetzen.

Rechtssicherheit beim Umgang mit Fotografien erforderlich

2.7 Benennung von Datenschutzbeauftragten

Sehr viele Anfragen erreichten uns von verantwortlichen Stellen, ob sie verpflichtet sind, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen. Wir klärten darüber auf, dass sich diese Pflicht sowohl aus der Datenschutz-Grundverordnung (DS-GVO) als auch aus dem Bundesdatenschutzgesetz (BDSG) ergeben kann.

Nach Artikel 37 Absatz 1 Buchstabe c DS-GVO ist eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter beispielsweise dann zu benennen, wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DS-GVO besteht. Da dazu insbesondere Gesundheitsdaten zählen, war es nicht verwunderlich, dass uns zahlreiche Anfragen aus der Ärzteschaft und von Apotheken erreichten. Bei diesen kommt es entscheidend darauf an, ob die Verarbeitung von Patientendaten als umfangreich zu klassifizieren ist. Nach Erwägungsgrund 91 DS-GVO stellt eine Verarbeitung von Patientendaten durch ärztliche oder sonstige Angehörige eines Gesundheitsberufs regelmäßig keine solche umfangreiche Datenverarbeitung dar. Anders verhält es sich hingegen, wenn die Praxis eine hohe, über das für vergleichbare Praxen übliche Maß deutlich hinausgehende Menge an personenbezogenen Daten besonderer Kategorien verarbeitet. In diesem Zusammenhang verwiesen wir u. a. auch auf den Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, der ergänzende Hilfestellungen bei Abgrenzungsschwierigkeiten bietet.[2]

In Ergänzung der Datenschutz-Grundverordnung haben die EU-Mitgliedstaaten die Möglichkeit, weitere Verantwortliche zur Benennung einer oder eines Datenschutzbeauftragten zu verpflichten. Der deutsche Gesetzgeber hat diesen Regelungsspielraum genutzt. Gemäß § 38 BDSG hat der Verantwortliche u. a. auch dann eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Der Begriff „ständig“ ist dabei weit auszulegen. Lediglich dann, wenn bei einer beschäftigten Person die Datenverarbeitung einen völlig untergeordneten Anteil ihrer Tätigkeit einnimmt, ist diese Person bei der Zählung nicht zu berücksichtigen. Auch der Begriff „automatisierte Verarbeitung“ ist weit zu verstehen und erfasst jede Form der Verarbeitung mittels einer Datenverarbeitungsanlage, wie z. B. PC, Smartphone, Scanner. Ob diese Voraussetzungen erfüllt sind, wurden wir insbesondere von kleinen und mittelständischen Handwerksunternehmen gefragt. Neben unserer rechtlichen Einschätzung wiesen wir die Verantwortlichen insbesondere auf die entsprechen-

2 Beschluss: „Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. c Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs“ vom 25. bis 26. April 2018.

den Leitlinien des Europäischen Datenschutzausschusses[3] sowie auf das von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hierzu erarbeitete Kurzpapier[4] hin.

3 Umgang mit Datenschutzverletzungen und Meldepflicht nach Artikel 33 DS-GVO

Mit dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018 wurden die gesetzlichen Regelungen verschärft, wie Verantwortliche auf Verletzungen des Schutzes personenbezogener Daten zu reagieren haben. Zu nennen ist dabei insbesondere die Pflicht, die zuständige Datenschutzaufsichtsbehörde zu informieren, falls die Verletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Artikel 33 DS-GVO). Weiterhin hat der Verantwortliche auch die betroffenen Personen zu benachrichtigen, falls dieses Risiko voraussichtlich sogar hoch ist (Artikel 34 DS-GVO). Unabhängig von der Melde- bzw. Benachrichtigungspflicht muss der Verantwortliche die Datenschutzverletzung dokumentieren (Artikel 33 Absatz 5 DS-GVO). Nachdem über sieben Monate vergangen sind, ist es Zeit für ein erstes Resümee zu den Erfahrungen mit diesen Vorschriften.

Der europäische Gesetzgeber versteht unter einer „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die – ob unbeabsichtigt oder unrechtmäßig – zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder in sonstiger Weise verarbeitet wurden (Artikel 4 Nr. 12 DS-GVO). Liegt ein solcher Fall vor und besteht durch die Verletzung voraussichtlich ein Risiko für betroffene Personen, muss der Verantwortliche den Sachverhalt unverzüglich und möglichst binnen 72 Stunden, nachdem er ihm bekannt wurde, der zuständigen Aufsichtsbehörde melden. Verzögerungen sind zu begründen. Die Meldung muss nach den gesetzlichen Vorschriften mindestens

3 Arbeitspapier WP 243: „Leitlinien in Bezug auf Datenschutzbeauftragte (‚DSB')“.

4 Kurzpapier Nr. 12: „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“.

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,

- den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,

- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten sowie

- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

enthalten. Sie kann auch schrittweise erfolgen (je nach den Ergebnissen bei der Aufklärung des Vorfalls und dem Erkenntnisgewinn des Verantwortlichen). Auftragsverarbeiter müssen derartige Verletzungen unverzüglich dem jeweiligen Verantwortlichen melden. Zur Auslegung der Vorschriften hat der Europäische Datenschutzausschuss Leitlinien veröffentlicht.[5]

Bereits ein Blick auf die Statistik[6] zeigt, dass die Anzahl der Meldungen gem. Artikel 33 DS-GVO, die uns als zuständige Aufsichtsbehörde in den vergangenen Monaten erreichten, hoch ist. Im Vergleich zu den Vorjahren ist ein deutlicher Anstieg zu verzeichnen. Die Ursachen hierfür sind unterschiedlich: Zum Teil ergibt sich die Zunahme aus dem erweiterten Geltungsbereich der Regelung. Während die Meldepflicht nach dem alten Bundesdatenschutzgesetz nur Unternehmen und andere Verantwortliche aus dem nicht öffentlichen Bereich traf, gilt sie seit dem Wirksamwerden der Datenschutz-Grundverordnung auch für alle Behörden und sonstigen öffentlichen Stellen. Weiterhin war bislang eine Meldung nur dann

5 Arbeitspapier WP 250: „Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679".

6 siehe VII 3

erforderlich, wenn die Verletzung besonders sensitive Daten betraf (z. B. solche, die unter ein Berufsgeheimnis fallen oder Daten zu Bank- bzw. Kreditkartenkonten) und schwerwiegende Beeinträchtigungen für Betroffene drohten. Nach den neuen Vorschriften ist eine Meldung hingegen nur noch entbehrlich, wenn aus der Datenschutzverletzung kein Risiko für betroffene Personen resultiert – die Schwelle liegt also erheblich niedriger. Weiterhin haben vermutlich die allgemeine Sensibilisierung für Datenschutzfragen im Zuge der Berichterstattung der Medien zur Datenschutz-Grundverordnung sowie die Möglichkeiten der Sanktionierung von unterlassenen oder unvollständigen Meldungen durch die Aufsichtsbehörde zu dem geschilderten Anstieg geführt.

Die inhaltliche Bandbreite der Meldungen zu Datenschutzverletzungen, die uns erreichten, ist groß. Beispielhaft sollen nur einige Fälle benannt werden:

- Eine Kindertagesstätte meldete den Verlust einer Digitalkamera. Das darin genutzte Speichermedium enthielt zahlreiche Fotos von Kindern aus dem Kitaalltag.

- Eine Verwaltung gab an, dass ein Außendienstmitarbeiter Akten aus einem Vollstreckungsfall kurzzeitig auf dem Dach seines Dienst-PKW abgelegt hatte. Als er losfuhr, verteilten sich diese in der Umgebung. Der Verlust wurde erst nach Ankunft in der Dienststelle bemerkt.

- Mehrere Meldungen bezogen sich auf Fehler bei der Kuvertierung von Briefen. So wurden in einigen Fällen Gesundheits- oder Sozialdaten einzelner betroffener Personen an Dritte übermittelt. Gleiches war vereinzelt auch bei Lohn-, Gehalts- oder Bezügemitteilungen oder bei Gebührenbescheiden vorgefallen.

- Mehrfach meldeten Verantwortliche Fehlkonfigurationen ihrer Software, durch die personenbezogene Daten bzw. Dateien zeitweise für Unbefugte einsehbar waren. In zwei Fällen betraf dies Gesundheitsdaten bzw. Personalaktendaten von anderen Beschäftigten. Mängel in der Software könnten auch dafür verantwortlich sein, dass Kunden beim Online-Banking vereinzelt Kontoauszüge anderer Personen angezeigt wurden.

- In zwei Unternehmen gaben mehrere Beschäftigte als Reaktion auf Phishing-Mails Angreifern die Zugangsdaten zu ihren E-Mail-Konten bekannt. Beide Unternehmen konnten verifizieren, dass mit den erbeuteten Daten auf die E-Mail-Konten zugegriffen wurde.

- Mehrere Unternehmen wurden Opfer von Hacking-Angriffen, da sie die verwendete Software nicht aktuell gehalten hatten. In einem Fall wurden beispielsweise nach dem erfolgreichen Angriff Kundendaten unbefugt kopiert. In einem anderen Fall wurden die Webseiten des Unternehmens so verändert, dass deren Besucher sich anschließend Schadsoftware auf den eigenen PC luden. Des Weiteren kam es hier zur Manipulation automatisch versandter Bestätigungsmails.

- Schon klassisch zu nennen sind Meldungen über den Befall von Rechnern mit Schadsoftware, die gespeicherte Daten verschlüsselt (Ransomware). Wenn eine aktuelle Sicherungskopie der Daten vorhanden ist, lassen diese sich nach der Bereinigung der Rechner wieder herstellen. In einem Unternehmen lag eine solche Kopie jedoch nicht vor – mehrere Tausend Datensätze sind vermutlich verloren.

Zum Teil gingen die Meldungen nach Artikel 33 DS-GVO in der vorgeschriebenen Frist und weitgehend vollständig bei uns ein. In einigen Fällen meldeten Verantwortliche zunächst nur das Vorkommnis und ergänzten konkrete Angaben später, z. B. zu den Datenkategorien, den betroffenen Personen, den Ursachen und möglichen Folgen der Verletzung. Zu einem nicht geringen Teil mussten wir allerdings auch Mängel feststellen. Diese betrafen insbesondere folgende Aspekte:

- Meldungen wurden komplett unterlassen. In mehreren Fällen erfuhren wir im Nachgang durch Beschwerden betroffener Personen davon, dass sie sich bereits an die Verantwortlichen gewandt und diese über die Datenschutzverletzung informiert hatten, eine Reaktion jedoch ausgeblieben war.

- Meldungen wurden verspätet eingereicht. Die Ursachen hierfür lagen zumeist in mangelnden organisatorischen Vorkehrungen bei den jeweiligen Unternehmen oder Behörden. Zum Teil wurde argumentiert, dass die Aufklärung noch nicht beendet wäre. Hierzu ist allerdings anzumerken, dass oftmals durch eine recht-

zeitige Einbindung der Aufsichtsbehörde gemeinsam über geeignete Maßnahmen entschieden werden kann, um die Folgen der Datenschutzverletzung zu beschränken.

- Mehrfach mussten wir durch aufwändige Nachfragen gewährleisten, dass uns alle gesetzlich vorgeschriebenen Inhalte einer Meldung mitgeteilt wurden. Zum Teil wurde z. B. versäumt, die Kategorien betroffener Personen, ihre Anzahl oder die Kategorien und Anzahl der betroffenen Datensätze zu benennen. Manche Verantwortliche verzichteten auch darauf, die von ihnen eingeleiteten Maßnahmen anzugeben. In einigen Fällen wurden unvollständige Erstmeldungen erst nach unserer ausdrücklichen Erinnerung und Mahnung ergänzt.

- Einige Unternehmen und Behörden schätzten das Risiko, zu dem die Datenschutzverletzung für betroffene Personen führen kann, falsch ein und kamen zu fehlerhaften Schlussfolgerungen bzgl. der Meldepflicht gegenüber der Aufsichtsbehörde bzw. der Benachrichtigungspflicht gegenüber Betroffenen. So stellt etwa der Verlust eines Datenträgers mit verschlüsselt gespeicherten personenbezogenen Daten aus unserer Sicht bereits eine meldepflichtige Datenschutzverletzung dar. In diesem Fall müssen allerdings nicht die betroffenen Personen benachrichtigt werden.

In Abhängigkeit vom konkreten Einzelfall werden wir in Zukunft verstärkt dazu übergehen, insbesondere offensichtliche Verstöße gegen die Melde- und Benachrichtigungspflichten nach Artikel 33 bzw. Artikel 34 DS-GVO zu sanktionieren. Alle Verantwortlichen sind deshalb aufgefordert zu überprüfen, ob sie hinreichende Vorkehrungen getroffen haben, um ihre gesetzlichen Pflichten zu erfüllen. Dies betrifft z. B. die Schaffung organisatorischer Regelungen, die Festlegungen von Zuständigkeiten oder Meldewegen, die Vorgabe von Kriterien zur Risikobewertung oder die allgemeine Sensibilisierung in Bezug auf das Erkennen von Datenschutzverletzungen. Wir werden auch vorrangig solche Stellen, die wiederholt Meldungen nach Artikel 33 DS-GVO abgeben mussten, hinsichtlich des Datenschutz- und Informationssicherheitsmanagements im Unternehmen bzw. in der Behörde prüfen.

4 Datenschutz im Bereich der Telemedien

Da die Verabschiedung der ePrivacy-Verordnung noch immer aussteht, ergab sich für die Datenschutzaufsichtsbehörden die Herausforderung, Fragen der Auslegung des Telemedienrechts im Licht der Datenschutz-Grundverordnung (DS-GVO) zu klären. Offen war insbesondere die Fortgeltung des Telemediengesetzes.

Zweck der ePrivacy-Verordnung soll es sein, die Vorschriften der Datenschutz-Grundverordnung um spezifisch telemedienrechtliche Normen zu ergänzen, um ein hohes Schutzniveau für betroffene Personen gerade auch gegenüber den großen Telemedienanbietern sicherzustellen und deren Praxis entgegenzuwirken, durch eine Verfolgung der Internetnutzung Einzelner möglichst umfassend personenbezogene Daten zu sammeln, zu Profilen zusammenzustellen und zu Werbezwecken zu nutzen.

Europäische Vorschriften ersetzen Telemediengesetz

Da bis heute unklar ist, ob und wann die ePrivacy-Verordnung erlassen wird, bekam die Frage des übergangsweise geltenden Rechts besondere Relevanz. In einer Positionsbestimmung vom 26. April 2018 stellte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fest, dass die Vorschriften des Telemediengesetzes (TMG) zu den Voraussetzungen der rechtmäßigen Datenverarbeitung bei Telemedien von denen der Datenschutz-Grundverordnung verdrängt werden. Insofern richten sich die Anforderungen für Telemedienanbieter bis auf Weiteres ausschließlich nach der Datenschutz-Grundverordnung.

Wegen der räumlichen Beschränkung der Aufsicht ist die Landesbeauftragte nur für solche Anbieter zuständig, die ihren Sitz in Brandenburg haben. Ein nach Fallzahlen besonders großer Datenverarbeiter ist die eBay GmbH, deren Aufsicht die Landesbeauftragte 2018 übernommen hat. Bei den sonstigen Betreiberinnen und Betreibern von Webseiten sowie den Nutzerinnen und Nutzern von Mediendiensten überwog der Beratungsbedarf die eigentliche Aufsichtstätigkeit bei Weitem. Aus Gründen der begrenzten Kapazität war unsere Behörde in vielen Fällen gezwungen, sich bei Auskünften auf ihre Kernaufgaben zu beschränken. So war es uns etwa – trotz einer anhaltend großen Nachfrage – nicht möglich, bei der Erstel-

lung von einzelnen Datenschutzerklärungen Formulierungshilfen anzubieten oder diese etwa im Einzelfall auf ihre Rechtmäßigkeit hin zu prüfen. Gegenüber den Verantwortlichen bemühten wir uns aber um eine Klärung der Betreiberpflichten, sodass sie selbst entscheiden konnten, welche Anpassungen für ihr individuelles Telemedium erforderlich und welche verzichtbar waren.

Die geänderten Pflichten bei der Anbieterkennzeichnung und der Datenschutzerklärung bildeten die Schwerpunkte unserer Beratung. Bisher hatten sich beide Pflichten aus dem Telemediengesetz ergeben. Der nunmehr einschlägige Art. 13 DS-GVO erweitert und konkretisiert die Informationspflicht. Problematisch war hier einerseits, dass einige Verantwortliche die Pflicht zur Erstellung einer Datenschutzerklärung irrtümlich für eine grundsätzliche Neuerung hielten. Schwierigkeiten bereitete darüber hinaus oft die fehlende Kenntnis der Rechtsgrundlagen für die eigenen Verarbeitungstätigkeiten.

Im Zusammenhang mit der erweiterten Informationspflicht waren im Vorfeld Befürchtungen aufgekommen, es werde nunmehr eine Welle von wettbewerbsrechtlichen Abmahnungen und aufsichtsbehördlichem Einschreiten einsetzen. Es wurde gemutmaßt, die Aufsichtsbehörde würde bereits kurz nach Einführung der Datenschutz-Grundverordnung hohe Sanktionen selbst für kleine Mängel an der Datenschutzerklärung verhängen. Demgegenüber haben wir unsere Rolle zunächst vor allem darin gesehen, den Webseitenbetreiberinnen und -betreibern ihre Pflichten bewusst zu machen, insbesondere, welche Daten auf ihrer Webseite durch sie selbst und durch Dritte erhoben und verarbeitet werden, sowie dass zu diesen Datenverarbeitungsvorgängen jeweils eine Rechtsgrundlage erforderlich ist. Nur soweit Verstöße gegen Regeln auch des vor dem 25. Mai 2018 geltenden Rechts im Raum standen, wurde bisher eine Sanktionierung in Betracht gezogen.

Schwieriger zu beantworten ist derzeit die Frage nach dem zulässigen Umfang des individualisierten Trackings von Nutzerinnen und Nutzern sowie der Speicherung personenbezogener Daten zum Schutz der Integrität des Telemediums. Zwar kann dieses nicht mehr auf den – nach Wirksamwerden der Datenschutz-Grundverordnung nicht mehr anwendbaren – § 15 Absatz 3 TMG gestützt werden, der die Anlage pseudonymisierter Profile zu Werbezwecken zuließ. Trotzdem können sich Webseitenbetreiberinnen und -betreibern zumindest an bisherigen Kriterien zur Erforderlichkeit orientieren,

soweit die Frage zu entscheiden ist, ob die Verarbeitung von Nutzungsdaten im Sinne von § 15 TMG auch gemäß Artikel 6 Absatz 1 Buchstabe f DS-GVO zulässig ist. Dies ist jedoch dann nicht der Fall, wenn die genutzten Daten personenbezogen bleiben, obwohl die Verarbeitung anonymisierter Daten den verfolgten Zweck gleichermaßen erfüllt.

Für den Betrieb des Telemediums dürfen Webseitenbetreiberinnen und -betreiber hingegen personenbezogene Daten über den Nutzungsvorgang hinaus speichern, soweit dies erforderlich ist, um sich gegen Angriffe auf ihr System zu verteidigen und zu schützen. Soweit die Speicherung sich im erforderlichen Rahmen hält, zum Zweck der Bewahrung der Funktionsfähigkeit der Webseite erfolgt, eine Woche nicht übersteigt und technisch-organisatorisch sichergestellt ist, dass die gespeicherten Daten nur zweckgebunden genutzt werden, ist die Speicherung insoweit zulässig. Das hat der Europäische Gerichtshof in seinem Urteil vom 19. Oktober 2016, Rechtssache C-582/14, entschieden.

Weitere Fragen vieler öffentlicher und nicht öffentlicher Stellen betrafen den Einsatz von Messengerdiensten. Die Landesbeauftragte hat immer darauf hingewiesen, dass nur solche Dienste für die Kommunikation genutzt werden dürfen, die die datenschutzrechtlichen Anforderungen vollständig erfüllen. Insbesondere müssen die technisch-organisatorischen Vorkehrungen dem Schutzbedarf der betreffenden personenbezogenen Daten angemessen sein. Diese Voraussetzung kann der Verantwortliche nicht dadurch unterlaufen, dass er das Einverständnis der jeweils betroffenen Person einholt. Auf erforderliche Maßnahmen zur Datensicherheit kann aus datenschutzrechtlicher Sicht nicht wirksam verzichtet werden.

Von der Nutzung von Messengerdiensten, bei deren Betrieb Meta- oder gar Inhaltsdaten außerhalb des Europäischen Wirtschaftsraums (hier insbesondere in die Vereinigten Staaten) oder an sonstige Dritte übermittelt werden, rät die Landesbeauftragte in allen Fällen ab. Die Nutzung eines solchen Mediums kann zu einer Beschränkung oder einem Verbot durch die Landesbeauftragte führen.

5 Übernahme der Zuständigkeit für eBay – neue Herausforderungen für die Landesbeauftragte

Veränderungen ergaben sich während des Berichtszeitraumes nicht nur durch die Datenschutz-Grundverordnung, sondern auch durch strukturelle Änderungen bei dem Unternehmen eBay und der dazugehörigen Handelsplattform im Internet. Betreiberin der Website und verantwortliche Vertragspartnerin der deutschen und europäischen eBay-Nutzerinnen und -nutzer (mit Ausnahme Großbritanniens) ist seit Mai 2018 die eBay GmbH mit Sitz im brandenburgischen Kleinmachnow. Während die Aufsichtszuständigkeit für die Plattform bisher bei der Nationalen Kommission für den Datenschutz (CNPD) in Luxemburg lag, ist auf Grundlage der Funktionszuweisungen innerhalb des eBay-Konzerns nunmehr die Landesbeauftragte umfassend für die datenschutzrechtliche Aufsicht zuständig.[7] Um einen möglichst fließenden Übergang zu gewährleisten, bat die Landesbeauftragte die bisher zuständige Behörde um die Weitergabe von Erfahrungen und die Übermittlung offener Beschwerden. Im Rahmen eines persönlichen Treffens kam die CNPD dieser Bitte nach.

3…2…1…meins – eBay in Kleinmachnow

Kurz nach dem Wechsel der Aufsichtszuständigkeit wurde die Datenschutz-Grundverordnung wirksam – wodurch auch die Anzahl von Beschwerden über die eBay GmbH erheblich zunahm. Inhaltlich wurde ein breites Spektrum an Sachverhalten vorgetragen. Die überwiegende Anzahl an Beschwerden bezog sich auf Betroffenenrechte, wie die Rechte auf Auskunft und Löschung. Teilweise wurden auch prozessuale Abläufe beim Unternehmen und technische Einstellungen auf der Internetplattform infrage gestellt. In der kurzen Zeit unserer Aufsichtstätigkeit konnten wir bereits in mehreren Fällen zur Aufklärung der Beschwerdehintergründe beitragen und das Funktionieren der Verfahren zur Gewährung von Betroffenenrechten prüfen. In anderen Fällen dauert die abschließende Klärung noch an, da die Sachverhalte zunächst unter Mitwirkung sowohl der eBay GmbH als auch der Beschwerdeführerinnen und Beschwerdeführer vollständig aufgeklärt werden müssen.

7 Zur Übernahme der Aufsichtstätigkeit über die eBay Kleinanzeigen GmbH siehe Tätigkeitsbericht 2016/2017, B 18.1.

Nach unserer bisher gewonnenen Erfahrung stellt die Umsetzung der Datenschutz-Grundverordnung die Unternehmen nicht nur vor rechtliche, sondern gerade auch vor praktische Herausforderungen. In diesem Zusammenhang waren mit der eBay GmbH einige technisch-organisatorische Grundsatzfragen zu klären. Im Ergebnis hat das Unternehmen zwischenzeitlich beispielsweise seinen Gesamtprozess zur Identitätsprüfung vor Gewährung einer Auskunft an betroffene Personen in mehrfacher Hinsicht überarbeitet. Auch das Verfahren der zeitlich nachfolgenden Übersendung der Auskunftsinhalte wurde verändert.

Nicht nur für die Verantwortlichen, sondern auch für die Kooperation der Aufsichtsbehörden haben sich mit Wirksamwerden der Datenschutz-Grundverordnung Veränderungen ergeben. Beispielweise wurden neue Instrumente zur Zusammenarbeit der Aufsichtsbehörden aller EU-Länder bei grenzüberschreitenden Sachverhalten geschaffen. Da die eBay GmbH nicht nur die deutschen Webseiten, sondern auch Plattformen in vielen Mitgliedsstaaten betreibt, stehen wir zukünftig vor der Herausforderung, federführend internationale Beschwerden zu prüfen und Lösungen mit den Aufsichtsbehörden aller betroffenen Länder abzustimmen.

6 Verfahren, für die eine Datenschutz-Folgenabschätzung durchzuführen ist

Auch wenn eine Datenverarbeitung rechtlich zulässig ist, können von ihr hohe Risiken für die Rechte und Freiheiten der betroffenen Personen ausgehen. Die Datenschutz-Grundverordnung (DS-GVO) verlangt deshalb in diesem Fall vom Verantwortlichen, eine Datenschutz-Folgenabschätzung durchzuführen. Darin sind insbesondere die Risiken der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen zu untersuchen und zu bewerten sowie Abhilfemaßnahmen zur Bewältigung dieser Risiken festzulegen. Die Datenschutz-Folgenabschätzung ist vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen, kann aber bei wesentlichen Änderungen oder neu auftretenden Bedrohungen auch für bereits bestehende Verfahren verpflichtend sein. Da sie einen intensiven Arbeits- und Abstimmungsprozess erfordert, muss rechtzeitig damit begonnen werden.

Ob eine Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko birgt und damit eine Datenschutz-Folgenabschät-

zung erforderlich ist, stellt der Verantwortliche durch Abschätzung der konkreten Risiken der geplanten Verarbeitungsvorgänge fest (Schwellwertanalyse). Zur Unterstützung kann er hierbei die Leitlinien des Europäischen Datenschutzausschusses anwenden.[8] Diese Leitlinien enthalten neun Kriterien zur Einordnung der Verarbeitungsvorgänge. Sofern zwei oder mehr Kriterien erfüllt sind, ist in der Regel von einem voraussichtlich hohen Risiko auszugehen. Unter Umständen kann ein solches jedoch auch schon dann bestehen, wenn nur ein Kriterium erfüllt ist.

Darüber hinaus hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder jeweils ein Kurzpapier zur Einschätzung des Risikos[9] sowie zur Durchführung einer Datenschutz-Folgenabschätzung[10] veröffentlicht.

Liste riskanter Verfahren bietet Orientierung

Weitere Hilfestellung können Listen gemäß Artikel 35 Absatz 4 DS-GVO liefern. Diese werden von den Datenschutzaufsichtsbehörden publiziert und enthalten Verfahren, für die eine Datenschutz-Folgenabschätzung verpflichtend durchzuführen ist (sog. Muss-Listen). Im Berichtszeitraum haben die unabhängigen Aufsichtsbehörden des Bundes und der Länder ihre Listen für Unternehmen und andere Verantwortliche insbesondere im nicht öffentlichen Bereich abgestimmt, vereinheitlicht und auf ihren jeweiligen Webseiten bekannt gemacht. Die gemeinsame Liste wurde dem Europäischen Datenschutzausschuss gemeldet, da sie dem Kohärenzverfahren gemäß Artikel 63 DS-GVO unterliegt.

Für Behörden und andere öffentliche Stellen im Land Brandenburg hat die Landesbeauftragte zusätzlich eine ergänzende Liste nach Artikel 35 Absatz 4 DS-GVO veröffentlicht. Diese enthält Verfahren der öffentlichen Verwaltung, von denen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen ausgeht und für die eine Datenschutz-Folgenabschätzung durchzuführen ist.

8 Arbeitspapier WP 248: „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt'".

9 Kurzpapier Nr. 18: „Risiko für die Rechte und Freiheiten natürlicher Personen".

10 Kurzpapier Nr. 5: „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO".

Öffentliche Stellen des Landes sind somit verpflichtet, die beiden genannten Listen in ihre Betrachtungen bei der Schwellwertanalyse einzubeziehen.

Der Verantwortliche hat in jedem Fall die Entscheidung über die Durchführung oder die Nichtdurchführung einer Datenschutz-Folgenabschätzung unter Angabe der maßgeblichen Gründe hierfür schriftlich zu dokumentieren. Kommt er zu dem Ergebnis, dass eine Datenschutz-Folgenabschätzung erforderlich ist, ergeben sich die weiteren Anforderungen aus Artikel 35 und 36 DS-GVO sowie aus den Erwägungsgründen 84 sowie 90 bis 93. Über die verwendete Methode zur Durchführung kann der Verantwortliche selbst entscheiden. Werden bestehende Methoden oder Standards eingesetzt, ist jedoch zu beachten, dass die Anforderungen der Datenschutz-Grundverordnung immer vorrangig zu behandeln sind. Eine Möglichkeit zur Durchführung einer Datenschutz-Folgenabschätzung ist die Anwendung des Standard-Datenschutzmodells,[11] das im Jahr 2018 von der Datenschutzkonferenz beschlossen und veröffentlicht wurde. Es befindet sich derzeit in der Erprobung.

Der intensive Austausch mit anderen europäischen Datenschutzaufsichtsbehörden über eine gemeinsame Auffassung zu Anforderungen an die Muss-Listen für Datenschutz-Folgenabschätzungen und über die Bewertung der Listen aus anderen Mitgliedstaaten im Kohärenzverfahren war eine der ersten Gelegenheiten, das übergreifende Ziel der Datenschutz-Grundverordnung zur Vereinheitlichung der Datenschutzmaßstäbe in ganz Europa zu verwirklichen. Es zeigte sich, dass noch nicht eingespielte Kommunikationsflüsse und sehr kurze Fristen zur Abstimmung die Aufsichtsbehörden vor erhebliche Herausforderungen stellten. Hier gilt es, in zukünftigen vergleichbaren Verfahren die Effizienz zu steigern und Routine zu entwickeln.

7 Vorgaben zur Akkreditierung von Zertifizierungsstellen

Wie bereits in unserem letzten Tätigkeitsbericht[12] dargestellt, schafft die Datenschutz-Grundverordnung (DS-GVO) die Voraussetzungen für datenschutzspezifische Zertifizierungen, die dazu dienen, nach-

11 „Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele."

12 Tätigkeitsbericht 2016/2017, A 2.7

zuweisen, dass die Verordnung bei Verarbeitungen personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter eingehalten wird. Derartige Zertifizierungen sollen durch akkreditierte Zertifizierungsstellen erteilt werden. Im Berichtszeitraum stimmten die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Kriterien und Prozesse für Verfahren zur Akkreditierung von Zertifizierungsstellen ab. Die Deutsche Akkreditierungsstelle GmbH, die das Akkreditierungsverfahren koordiniert, ist in diesem Abstimmungsprozess eng eingebunden.

Insbesondere haben die Aufsichtsbehörden des Bundes und der Länder im Rahmen der Akkreditierung von Zertifizierungsstellen gem. Artikel 43 Absatz 3 DS-GVO die Aufgabe, die Vorgaben der internationalen Norm DIN EN ISO/IEC 17065 durch spezifische datenschutzrechtliche Vorgaben aus Artikel 42 und 43 DS-GVO zu ergänzen und zu konkretisieren. In diesem Zusammenhang wurde von einem Arbeitskreis, an dem auch unsere Dienststelle beteiligt ist, ein Regelpapier erarbeitet. Neben Geltungsdauer und Geltungsbereichen einer Akkreditierung gibt das Regelpapier u. a. vor, welche Mindestanforderungen für eine Zertifizierungsvereinbarung gelten müssen, wie die Unparteilichkeit der Zertifizierungsstelle sichergestellt werden kann, welche Ressourcen dort notwendig sind, welche Anforderungen an die beteiligten Prozesse (z. B. Antragstellung, Evaluierung, Zertifizierungsentscheidung, Zertifizierungsdokumentation, Überwachung und Zurückziehung von Zertifizierungen, Umgang mit Beschwerden und Einsprüchen) zu stellen sind und wie ein angemessenes Managementsystem etabliert werden kann.

Das Regelpapier berücksichtigt die Leitlinien des Europäischen Datenschutzausschusses zur Akkreditierung von Zertifizierungsstellen.[13] Es wurde von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vorläufig verabschiedet. Gem. Artikel 64 Absatz 1 Buchstabe c DS-GVO ist vorgesehen, dass der Europäische Datenschutzausschuss hierzu noch eine Stellungnahme abgibt. Im Anschluss wird das Papier durch unsere Behörde (wie auch durch die anderen Datenschutzaufsichtsbehörden in Deutschland) sowie durch die Deutsche Akkreditierungsstelle veröffentlicht.

13 Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679).

Auch die Zusammenarbeit der Aufsichtsbehörden untereinander sowie mit der Deutschen Akkreditierungsstelle in Akkreditierungsverfahren war zu regeln. Der Arbeitskreis hatte in diesem Zusammenhang u. a. die Aufgabe, eine entsprechende Vereinbarung zu formulieren, mit der Deutschen Akkreditierungsstelle abzustimmen und der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Beschlussfassung vorzulegen. Neben dem Austausch von Begutachtern und Mitgliedern des Akkreditierungsausschusses zwischen den Aufsichtsbehörden im Rahmen der Begutachtung von Zertifizierungsstellen wurden Regelungen getroffen, die die jeweiligen Zuständigkeiten und Aufgaben festlegen. Der nun vorliegende Vereinbarungsentwurf ist weitgehend fertiggestellt und wird demnächst der Konferenz zugeleitet.

Kapitel II Datenschutzverstöße: Maßnahmen und Sanktionen

II Datenschutzverstöße: Maßnahmen und Sanktionen

1 Beanstandung: Verfahren zur internetbasierten Kfz-Zulassung

In unserem letzten Tätigkeitsbericht hatten wir über ein landesweites Projekt zur Umsetzung der internetbasierten Kfz-Zulassung berichtet.[14] Entsprechend den rechtlichen Vorgaben der Fahrzeug-Zulassungsverordnung sind die für das Kfz-Zulassungswesen zuständigen Stellen in den Landkreisen und kreisfreien Städten seit Oktober 2017 verpflichtet, die Abmeldung und die Wiederzulassung von Kraftfahrzeugen auf denselben Halter auch über das Internet zu ermöglichen. Hierzu hatten sie gemeinsam mit dem Brandenburgischen IT-Dienstleister und mit unserer Beratung eine mandantenorientierte Lösung entwickelt, die sowohl eine elektronische Identifizierung der Antrag stellenden Person mittels elektronischem Personalausweis oder Aufenthaltstitel als auch das eigentliche Stellen des Antrags ermöglichte.

Die meisten Kfz-Zulassungsstellen des Landes beteiligten sich an diesem Projekt. Nur eine Minderheit wählte einen eigenen Weg und wollte eine Portallösung einsetzen, die ein anderer Dienstleister entwickelt hatte. Wir erkundigten uns bei diesen Zulassungsstellen noch vor dem Termin der verpflichtenden Inbetriebnahme des Verfahrens nach dem Stand der Implementierung. Insbesondere interessierten uns detaillierte Verfahrensbeschreibungen, Sicherheitskonzepte, Verträge zur Auftragsverarbeitung, die Bereitstellung von Informationen für Antrag stellende Personen sowie die datenschutzrechtlich erforderliche Freigabe des Verfahrens. Wir gingen davon aus, dass eine Produktivsetzung nur erfolgt, wenn alle Voraussetzungen erfüllt sind.

Bei unseren Recherchen auf dem zentralen Landesportal, in dem die Angebote aller brandenburgischen Zulassungsstellen zur internetbasierten Kfz-Zulassung verlinkt sind, stellten wir fest, dass auch die Lösungen derjenigen Kommunen erreichbar und produktiv waren, die sich nicht an der Landeslösung beteiligten. Allerdings konnte uns nur eine Zulassungsstelle – wenn auch erst auf wiederholte Nachfrage – die datenschutzrechtlich erforderlichen Unterlagen bereitstel-

14 Tätigkeitsbericht 2016/17, B 11.5

len. In einem anderen Fall informierte uns die verantwortliche Stelle – der Landkreis Oberspreewald-Lausitz – darüber, dass sie erst durch uns von der Inbetriebnahme des Verfahrens Kenntnis erlangt hatte. Offensichtlich hatte der dortige Dienstleister eigenmächtig gehandelt und die Freischaltung des Angebots dieser Zulassungsstelle ohne eine entsprechende Anweisung vorgenommen. Da auch die notwendige Verfahrens- und IT-Sicherheitsdokumentation nicht vorlag, sprach die Landesbeauftragte eine Beanstandung gegenüber dem Landkreis wegen mehrerer Verstöße gegen das damals geltende Brandenburgische Datenschutzgesetz aus.

Unabhängig von dieser Beanstandung mussten wir feststellen, dass bei der von der Landeslösung abweichenden Realisierung des Verfahrens personenbezogene Daten von Antrag stellenden Personen unzulässig verarbeitet wurden. Ursache hierfür war eine Vermischung von zwei datenschutzrechtlich unabhängig zu betrachtenden Verfahren – einerseits einem Online-Portal für die Bereitstellung und Verwaltung von Bürgerkonten und andererseits dem Online-Dienst für die Beantragung der Kfz-Abmeldung oder Wiederzulassung. Die konkrete Implementierung sah vor, dass Antragstellerinnen und Antragsteller sich vor dem elektronischen Identitätsnachweis für die internetbasierte Kfz-Zulassung mittels elektronischem Personalausweis oder Aufenthaltstitel zwangsweise auch für ein Bürgerkonto registrieren mussten. Dieser faktische Zwang zur Registrierung führte dazu, dass personenbezogene Daten verarbeitet wurden, die für das Verfahren der internetbasierten Kfz-Zulassung nicht erforderlich waren. Es gab für diese Datenverarbeitung auch weder eine gesetzliche Grundlage noch eine den gesetzlichen Vorgaben entsprechende Einwilligung der sich registrierenden Personen.

Verfahren online ohne Wissen des Verantwortlichen

Im Ergebnis unserer Feststellung nahmen die betroffenen Kfz-Zulassungsstellen das Verfahren zunächst außer Betrieb und gestalteten es um. Danach wird nun klar zwischen der Registrierung für ein Benutzerkonto und der Beantragung der Kfz-Abmeldung bzw. Wiederzulassung unterschieden. Insbesondere erfordert Letztere nicht das Anlegen eines dauerhaften Benutzerkontos.

Des Weiteren forderten wir die betroffenen Zulassungsstellen auf, diejenigen Bürgerinnen und Bürger, die sich bereits für ein Benutzerkonto registriert hatten, unter Verwendung der beim Registrierungsprozess angegebenen E-Mail-Adresse über die rechtswidrige Datenverarbeitung zu informieren und um eine nachträgliche Einwilligung zu ersuchen. Für den Fall, dass eine solche Einwilligung nicht erteilt wurde, waren die jeweiligen personenbezogenen Daten und das Benutzerkonto zu löschen.

Am Beispiel des Verfahrens zur internetbasierten Kfz-Zulassung zeigt sich, welche Schwierigkeiten bei der Digitalisierung von Verwaltungsdienstleistungen bestehen können. Zwar ist zu begrüßen, dass Verwaltungen die Herausforderungen im Rahmen des E-Governments und der entsprechenden Umgestaltung ihrer Prozesse annehmen. Allerdings sollten sie dabei verstärkt auf Kooperationen und gemeinsame Herangehensweisen setzen, um den Aufwand zu reduzieren und Fehler zu vermeiden. Dies ist gerade bei der Umsetzung des Online-Zugangsgesetzes und der geplanten Digitalisierung von mehreren Hundert Verwaltungsdienstleistungen in Deutschland bis Ende 2022 unabdingbar.

2 Beanstandung: Fachverfahren zum Verbraucherschutz

Bereits in unserem letzten Tätigkeitsbericht[15] informierten wir über unsere Prüfung eines landesweit genutzten Softwaresystems zur behördlichen Überwachung im Lebensmittel- und Veterinärbereich. Konkreter Anlass war damals das Auskunftsersuchen eines betroffenen Hobbynutztierhalters, der sich u. a. für die Löschfristen der über ihn gespeicherten Daten interessierte.

Das auch in anderen Bundesländern genutzte Verfahren wurde vor über 10 Jahren unter der Leitung des damals für Verbraucherschutz zuständigen Ministeriums eingeführt. Im Rahmen der Fachaufsicht wird seitdem auch über alle wesentlichen Aspekte des Verfahrenseinsatzes und der Weiterentwicklung entschieden. Die Administration erfolgt im nachgeordneten Landesamt, die Landkreise sind für die Pflege der Daten zuständig. Im Ergebnis unserer Kontrolle stellten wir wesentliche Mängel bei der Einhaltung der datenschutzrechtlichen Anforderungen fest. Insbesondere monierten wir die seit

15 Tätigkeitsbericht 2016/2017, B 7.4

über 10 Jahren fehlende Festlegung von Fristen für die Löschung personenbezogener Daten. Darüber hinaus waren die Angaben im Verfahrensverzeichnis während des gesamten Einsatzzeitraums nie aktualisiert und an neue technische Gegebenheiten angepasst worden. Weiterhin hatte das Verfahren nie die gesetzlich vorgeschriebene datenschutzrechtliche Freigabe erhalten.

Die gravierenden Verstöße gegen das damals geltende Brandenburgische Datenschutzgesetz teilten wir dem Ministerium der Justiz und für Europa und Verbraucherschutz mit. Insbesondere informierten wir die Leitungsebene hierüber. Damit verbunden war unsere Forderung, unverzüglich mit der Mängelbeseitigung zu beginnen. Da wir jedoch auch mehrere Monate später keine hinreichenden Aktivitäten des Ministeriums verzeichnen konnten, sprach die Landesbeauftragte eine Beanstandung aus.

Mit dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 und dem Inkrafttreten des novellierten Brandenburgischen Datenschutzgesetzes (BbgDSG) zum gleichen Zeitpunkt sind bei der Beseitigung der datenschutzrechtlichen Defizite im Fachverfahren nun die dortigen Regelungen zu beachten.

In seiner Antwort auf die Beanstandung teilte das Ministerium der Landesbeauftragten u. a. mit, dass im Rahmen einer Kooperation der Bundesländer eine Projektgruppe damit beauftragt wurde, ein Stufenkonzept zur Archivierung und Löschung der Daten in dem Fachverfahren zu erstellen. Diese Vorgaben sollten nach Beschlussfassung in der Länderarbeitsgemeinschaft in das Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO aufgenommen werden. Eine Erklärung der Freigabe gemäß § 4 BbgDSG sei erst nach dem Vorliegen des aktualisierten Verzeichnisses geplant und solle diesem beigefügt werden.

Bis zum Ende des Berichtszeitraums informierte uns das Ministerium weder über die Fortschritte noch lieferte es die geforderten Nachweise für einen datenschutzgerechten Betrieb des Fachverfahrens.

3 Beanstandung: Integrationsportal eines Jobcenters

Zur Unterstützung der beruflichen Eingliederung erwerbsfähiger Leistungsberechtigter betreibt das Jobcenter des Landkreises Havelland seit dem Jahr 2012 ein sog. Integrationsportal. Dafür übermittelt es schutzbedürftige Sozialdaten der Leistungsberechtigten regelmäßig an ein beauftragtes Unternehmen. Mit Hilfe eines speziellen Algorithmus werden dort potentiell passende Stellenangebote innerhalb des Netzwerks beteiligter Unternehmen gesucht und an das Jobcenter zurückgemeldet. Sofern die betroffene Person einwilligt, wird außerdem ein vorher erstelltes Bewerbungsprofil im Online-Portal veröffentlicht.

Da in dem Verfahren sensitive personenbezogene Daten verarbeitet werden, sehen die datenschutzrechtlichen Vorschriften besondere Vorkehrungen vor, um die Risiken für die Rechte und Freiheiten der Betroffenen Personen zu beherrschen. Insbesondere muss ein IT-Sicherheitskonzept vorliegen und eine Risikoanalyse vorgenommen werden, bevor das Verfahren eingeführt werden darf. Diese Pflicht erstreckt sich auch auf einen Dienstleister, falls ein solcher in die Verarbeitung einbezogen wird.

Datenschutz rechtzeitig berücksichtigen

Dementsprechend forderte der IT-Sicherheitsbeauftragte des Landkreises die nötigen Unterlagen von der beauftragten Firma an. Angesichts der daraufhin übergebenen Dokumente meldete er erhebliche Zweifel an, dass diese eine ausreichende Basis für eine Verfahrensfreigabe darstellen. Daher wandte er sich an die Landesbeauftragte mit der Bitte um eine Einschätzung. Wir informierten das Jobcenter, dass eine Verfahrensfreigabe auf Grundlage dieser Dokumentation wegen diverser Mängel unzulässig wäre.

Das Integrationsportal wurde dennoch eingeführt. Über mehrere Jahre hinweg hatte das Jobcenter in Schreiben und gemeinsamen Gesprächen immer wieder Nachbesserungen und eine Beseitigung der Lücken versprochen. Bei einer Prüfung Anfang 2018 wurde für uns jedoch ersichtlich, dass nach nunmehr sechs Jahren die geforderten Unterlagen noch immer nicht vorlagen. Stattdessen wurden uns Dokumente übergeben, die fast deckungsgleich waren mit jenen, die schon 2012 als unzureichend bemängelt wurden.

Daraufhin sprach die Landesbeauftragte eine Beanstandung aus. In einer Stellungnahme sollte das Jobcenter darlegen, wie die Mängel behoben werden. Mit der Stellungnahme übersandte es Unterlagen, die das beauftragte Unternehmen als Reaktion auf die Beanstandung zur Verfügung gestellt hatte und drückte die Hoffnung aus, dass die Bedenken damit ausgeräumt seien. Diese Unterlagen unterschieden sich allerdings weiterhin nicht wesentlich von jenen, die vorher beanstandet wurden.

Die Landesbeauftragte prüfte daher, die verantwortliche Stelle gemäß Artikel 58 Absatz 2 Buchstabe a Datenschutz-Grundverordnung anzuweisen, die vorgeschriebenen Nachweise zur Einhaltung der Datenschutzbestimmungen zu erstellen. Im Rahmen einer vorherigen Anhörung baten wir das Jobcenter um eine Stellungnahme. Als Reaktion wurde dort schließlich entschieden, den Vertrag mit dem Unternehmen zu kündigen und das Integrationsportal in dieser Form einzustellen. Ab Ende 2018 werden demnach keine Sozialdaten von Leistungsberechtigten mehr an die Firma übertragen.

Dieser Vorgang zeigt einmal mehr, wie wichtig es ist, Datenschutzbestimmungen schon vor Einführung eines neuen Verfahrens sehr genau zu prüfen sowie deren Einhaltung zu gewährleisten und zu dokumentieren. Dies gilt insbesondere bei der Verarbeitung von Sozialdaten und anderen Daten, durch deren unbefugte Kenntnisnahme, Manipulation oder Zerstörung ein hohes Risiko für die betroffenen Personen entstehen kann. Werden personenbezogene Daten im Auftrag durch Dritte verarbeitet, ist vor allem darauf zu achten, dass der Auftraggeber – hier das Jobcenter – voll verantwortlich für die Datenverarbeitung beim Auftragnehmer bleibt. Es ist daher unerlässlich, Datenschutzstandards vertraglich festzuschreiben und die entsprechenden Angaben des Unternehmens auch tatsächlich selbst zu überprüfen.

4 Warnung: Fehler vor der Wahl des Ausschusses ehrenamtlicher Richter

An jedem Sozialgericht wählen die dort berufenen ehrenamtlichen Richterinnen und Richter alle fünf Jahre einen sog. Ausschuss der ehrenamtlichen Richter. Für den Ausschuss können alle ehrenamtlichen Richterinnen und Richter kandidieren. Er wirkt an der Gerichtsverwaltung mit und ist beispielsweise zu hören vor Entscheidungen

über die Bildung von Spruchkammern, die Geschäftsverteilung und die Verteilung der ehrenamtlichen Richterinnen und Richter auf die Kammern. Die Kammern sind jeweils für bestimmte Fachgebiete zuständig (z. B. Angelegenheiten der Grundsicherung, Angelegenheiten des Vertragsarztrechts). Die ehrenamtlichen Richterinnen und Richter gehören – abhängig von den sie vorschlagenden Einrichtungen (z. B. aus dem Kreis der Versicherten oder dem Kreis der Arbeitgeberinnen und Arbeitgeber) – unterschiedlichen Gruppen an.

Bei uns beschwerte sich ein ehrenamtlicher Richter über die 2017 durchgeführte Wahl der Mitglieder des Ausschusses der ehrenamtlichen Richter am Sozialgericht Potsdam. Allen ehrenamtlichen Richterinnen und Richtern war ein Wählerverzeichnis übersandt worden, in dem sämtliche Wahlberechtigte am entsprechenden Sozialgericht in alphabetischer Reihenfolge aufgeführt waren mit Namen, vollständiger Wohnanschrift und der Angabe der Organisation, Behörde oder sonstigen Einrichtung, auf deren Vorschlag die Berufung als ehrenamtliche Richterin oder ehrenamtlicher Richter erfolgte. Der Beschwerdeführer bat uns zu prüfen, ob dies zulässig war.

Die Bildung des Ausschusses der ehrenamtlichen Richter ist dem Grunde nach in § 23 Sozialgerichtsgesetz (SGG) geregelt. Über die mit der Wahl im Zusammenhang stehende Datenverarbeitung enthält diese Vorschrift jedoch keine speziellen Bestimmungen. Die Zulässigkeit der Übermittlung der personenbezogenen Daten an die ehrenamtlichen Richterinnen und Richter richtet sich folglich nach allgemeinem Datenschutzrecht. Da das Wahlverfahren im Jahr 2017 stattfand, galt § 16 Brandenburgisches Datenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung. Wir hatten zu prüfen, ob die Übermittlung sämtlicher Daten an alle ehrenamtlichen Richterinnen und Richter für die rechtmäßige Durchführung der Wahl erforderlich war.

Das Sozialgericht sah die Übersendung des Wählerverzeichnisses als erforderlich an, um allen ehrenamtlichen Richterinnen und Richtern die Gelegenheit zu geben, die Richtigkeit des Wählerverzeichnisses zu prüfen und ggf. Widerspruch einzulegen. Das Gericht räumte lediglich ein, dass die Angabe der Wohnanschrift nicht erforderlich gewesen sein dürfte. Wir hielten eine Übersendung der Liste jedoch generell für unzulässig. Denn es genügt für ein transparentes Wahlverfahren, jeder ehrenamtlichen Richterin und jedem ehrenamtlichen Richter die sie oder ihn betreffenden Daten für die Prüfung

ihrer Richtigkeit mitzuteilen. Ergänzend kann das Wählerverzeichnis (ohne Angabe der Wohnanschrift) im Gericht zur Einsicht bereitgehalten werden, sodass eine Überprüfung aller Eintragungen möglich bleibt.

Das Gericht teilte uns außerdem mit, dass eine weitere Liste an alle ehrenamtlichen Richterinnen und Richter als Wahlvorschlag übersandt worden war. Sie enthielt dieselben Angaben wie das Wählerverzeichnis, ergänzt um den jeweiligen Beruf der ehrenamtlichen Richterin oder des ehrenamtlichen Richters. Das Sozialgericht ging davon aus, dass jede und jeder Wahlberechtigte aus jeder der beim Sozialgericht bestehenden sieben Gruppen von Richterinnen und Richtern zwei Kandidatinnen oder Kandidaten wählen kann.

Um die Wahl korrekt durchzuführen, hielten wir auch die Versendung dieser Liste an alle ehrenamtlichen Richterinnen und Richter für nicht erforderlich. Denn die Rechtslage hatte sich im Jahr 2012 geändert. Nach § 23 SGG steht es nicht mehr jeder und jedem Wahlberechtigten zu, Richterinnen und Richter aus sämtlichen am Sozialgericht vertretenen Richtergruppen zu wählen. Vielmehr kann seit dieser Rechtsänderung eine ehrenamtliche Richterin oder ein ehrenamtlicher Richter nur noch eine Kandidatin oder einen Kandidaten aus der Richtergruppe wählen, der sie oder er selbst angehört. Dementsprechend wäre es nur zulässig gewesen, für jede Richtergruppe einen separaten Wahlvorschlag zu erstellen und diesen auch nur den dieser Gruppe angehörenden ehrenamtlichen Richterinnen und Richtern zukommen zu lassen.

Da die alte Fassung des Brandenburgischen Datenschutzgesetzes zwischenzeitlich außer Kraft getreten war und somit eine Beanstandung nach altem Recht nicht mehr in Betracht kam, hielten wir es für angezeigt, gegenüber dem Sozialgericht eine Warnung nach Artikel 58 Absatz 2 Buchstabe a Datenschutz-Grundverordnung auszusprechen. Ziel der Warnung ist es, bei der nächsten turnusmäßigen Wahl des Ausschusses ein datenschutzkonformes Wahlverfahren zu gewährleisten. Eine solche Warnung war notwendig, da das Gericht uns lediglich zugesagt hatte, künftig auf die Angabe der genauen Wohnanschrift im Wählerverzeichnis verzichten zu wollen und stattdessen nur den Wohnort zu nennen. Unsere Empfehlung, von einer Versendung des gesamten Wählerverzeichnisses abzusehen, ignorierte das Gericht ebenso wie unseren Hinweis auf die geänderte Rechtslage, die eine Beschränkung bei den Wahlvor-

schlagslisten erfordert. Es ist also nicht ausgeschlossen, dass sich die festgestellten Verstöße gegen das Datenschutzrecht bei der nächsten Wahl des Ausschusses der ehrenamtlichen Richter wiederholen.

Die Warnung soll hier präventiv wirken und das Gericht vor einem vermeidbaren Verstoß gegen die Datenschutz-Grundverordnung sowie vor den sich daraus ergebenden Verletzungen der Rechte der betroffenen ehrenamtlichen Richterinnen und Richter und eventuellen Schadenersatzforderungen bewahren.

5 Verwarnung: E-Mail mit offenem Verteiler

Ein besonderes Ferienerlebnis sollte es werden: Reiten lernen, Natur erleben, Ausritte im Wald, das Pferd im Mittelpunkt. Die geplanten – und gebuchten – Reiterferien mussten jedoch ausfallen. Um Eltern und Kinder über die Stornierung zu informieren, verfasste der Veranstalter eine E-Mail, die die Adressdaten von insgesamt 23 Personen, davon 22 im CC-Feld (Carbon Copy) enthielt. Die jeweiligen E-Mail-Adressen waren so für alle Empfängerinnen und Empfänger sichtbar.

Eine Übermittlung personenbezogener Daten – und um solche handelt es sich grundsätzlich bei E-Mail-Adressen – ist nur zulässig, soweit das Gesetz dies erlaubt oder die betroffenen Personen eingewilligt haben. Eine wirksame Einwilligung lag in dem dargestellten Fall allerdings nicht vor. Auch auf eine gesetzliche Grundlage konnte der Veranstalter die Übermittlung nicht stützen. Für die Durchführung der jeweils abgeschlossenen Verträge war weder eine Offenbarung erforderlich noch bestand ein berechtigtes Interesse daran.

Im Rahmen des eingeleiteten datenschutzrechtlichen Aufsichtsverfahrens wurde dem Verantwortlichen die Möglichkeit der Stellungnahme eingeräumt. Er versicherte glaubhaft, dass es in dem konkreten Fall zu einem bedauerlichen Fehler gekommen ist und man üblicherweise das BCC-Feld (Blind Carbon Copy) verwendet. Aufgrund des festgestellten Verstoßes gegen den Grundsatz der Rechtmäßigkeit bei der Verarbeitung personenbezogener Daten haben wir gegenüber dem Reiseveranstalter eine Verwarnung gemäß Artikel 58 Absatz 2 Buchstabe b Datenschutz-Grundverordnung ausgesprochen. Da es sich um einen erstmaligen Verstoß handelte und sich der Verantwortliche kooperativ und einsichtig zeigte, sahen wir von weiteren Sanktionen ab.

6 Verwarnung: Veröffentlichung der Buchungen von Monteurszimmern im Internet

Uns erreichte eine Beschwerde, dass auf der Internetseite einer kleinen Immobilien- und Hausverwaltung Daten von Personen, die Monteurszimmer gebucht hätten, offen einsehbar seien. Die Datensätze umfassten unter anderem Vor- und Nachnamen von Kontaktpersonen, Bezeichnungen von Unternehmen und Telefonnummern.

Nachdem wir die Immobilienverwaltung zu diesem Vorwurf angehört hatten, entfernte sie die entsprechenden Daten sofort aus dem Internet und meldete uns eine Datenschutzverletzung nach Artikel 33 Datenschutz-Grundverordnung (DS-GVO). Sie gab an, dass die Daten versehentlich veröffentlicht worden sind. Eine Information der Betroffenen über den Vorfall erfolgte nicht, da kein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zu erwarten war. Des Weiteren teilte das Unternehmen mit, dass es nun über einen IT-Sicherheitsbeauftragten verfügt, um künftigen Datenschutzverletzungen vorzubeugen.

Unsere Prüfung des Sachverhalts ergab, dass die von der unrechtmäßigen Veröffentlichung betroffenen Datenkategorien grundsätzlich einem normalen Schutzbedarf unterliegen und der beruflichen Sphäre der Betroffenen zuzurechnen sind. 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. Zudem waren die ergriffenen Maßnahmen (z. B. die Bestellung eines IT-Sicherheitsbeauftragten) zur Vermeidung ähnlicher Vorfälle in der Zukunft angemessen. Von der Einleitung eines Bußgeldverfahrens haben wir daher abgesehen, jedoch eine Verwarnung nach Artikel 58 Absatz 2 Buchstabe b DS-GVO ausgesprochen.

7 Bericht der Bußgeldstelle

Auch in diesem Berichtszeitraum führten wir Ordnungswidrigkeitenverfahren wegen datenschutzrechtlicher Verstöße aus den verschiedensten Bereichen des gesellschaftlichen Lebens. Diese beziehen sich zumeist auf die alte Rechtslage, da die Ordnungswidrigkeiten vor dem 25. Mai 2018 begangen wurden. Exemplarisch seien hier

der unberechtigte Abruf von personenbezogenen Daten aus polizeilichen Datenbanken, die unzulässige Videoüberwachung des öffentlich zugänglichen Raumes durch Private und die Veröffentlichung personenbezogener Daten im Internet ohne Einwilligung der Betroffenen genannt. Geldbußen nach neuer Rechtslage hat die Landesbeauftragte bisher noch nicht verhängt.

Abrufe aus polizeilichen Datenbanken durch Polizeibedienstete sind nur dann erlaubt, wenn eine dienstliche Notwendigkeit dafür besteht. Jeder aus privaten Motiven veranlasste Einblick in die verschiedenen Datenbanksysteme der Polizei stellt eine Ordnungswidrigkeit dar, die wir sanktionieren können. So verhängten wir beispielsweise ein Bußgeld gegen einen Polizeibediensteten, der sich unbefugt Namen und Adresse eines Fahrzeughalters verschaffte. Dessen Sportwagen gefiel ihm anscheinend so gut, dass er ihm anschließend einen Besuch abstattete, um sein Interesse an einem Kauf des Wagens zu bekunden.

Verstöße mit Geldbußen geahndet

Um Autos ging es auch im nachfolgenden Fall. Ein Fahrzeughalter ließ zum Schutz seines Kraftfahrzeugs und um im Schadensfall Beweise zur Hand zu haben, während der Fahrt eine kleine Kamera (sog. Dashcam) mitlaufen, sodass andere Teilnehmerinnen und Teilnehmer des Straßenverkehrs ungewollt gefilmt wurden. Spätestens seit dem Urteil des Bundesgerichtshofs vom 15. Mai 2018 (VI ZR 233/17) steht fest, dass das anlasslose und permanente Aufzeichnen des Verkehrsgeschehens durch Dashcams massiv in die Persönlichkeitsrechte der von der Verarbeitung der Daten betroffener Personen eingreift und daher nicht mit den Regelungen des Bundesdatenschutzgesetzes vereinbar ist. Die Verhängung eines Bußgeldes war daher geboten.

In einem anderen Fall waren die Mitgliederlisten eines Vereins vermutlich aufgrund eines nicht funktionierenden Passwortschutzes im Internet über eine Suchmaschine auffindbar. So konnten Namen, Wohnanschriften, E-Mail-Adressen und Geburtsdaten der Vereinsmitglieder von jedermann eingesehen werden, ohne dass die betroffenen Personen zuvor in die Veröffentlichung ihrer Daten eingewilligt hatten oder die Veröffentlichung für den Vereinszweck erforderlich gewesen wäre. Auch wenn der Verein die Offenlegung nicht beabsichtigt hatte, sondern fahrlässig handelte, wurde der Verstoß von uns mit der Verhängung eines Bußgeldes sanktioniert. Denn jede

Stelle, ob öffentlich oder privat, die mit der Verarbeitung personenbezogener Daten betraut ist, muss durch Beachtung der erforderlichen Sorgfalt sicherstellen, dass die Daten vor der Kenntnisnahme Unbefugter geschützt sind. Sollten die veröffentlichten Daten in die falschen Hände gelangen, besteht beispielsweise die Gefahr von Identitätsdiebstahl oder Rufschädigung der betroffenen Personen.

Einige Streitigkeiten im Ordnungswidrigkeitenverfahren mussten im vergangenen Berichtszeitraum gerichtlich geklärt werden, da die Betroffenen Einspruch gegen unsere Bußgeldbescheide einlegten. Mit einer Ausnahme bestätigte das Gericht in allen Fällen, dass die Verhängung eines Bußgeldes geboten war. So konnte auch das Verfahren gegen eine Ärztin abgeschlossen werden. Sie wurde zur Zahlung einer Geldbuße verurteilt, weil sie Patientenunterlagen unsachgemäß im Hausmüll entsorgt hatte.

Kapitel III
Anlasslose Prüfungen

III Anlasslose Prüfungen

1 Prüfung der Verfahren ELBOS und WebView

Im Berichtszeitraum führten wir eine anlasslose Prüfung des polizeilichen Fachverfahrens „Einsatzleitsystem für Behörden und Organisationen mit Sicherheitsaufgaben (ELBOS)“ durch. Das Verfahren wird derzeit im Einsatz- und Lagezentrum sowie in den Dienststellen der Polizei des Landes Brandenburg eingesetzt. Es bestehen Schnittstellen u. a. zur Feuerwehr und zu den Rettungsstellen. Mit dem Fachverfahren ELBOS werden u. a. folgende Aufgaben erfüllt:

- Führung einer Übersicht der verfügbaren Einsatzmittel und deren Status,
- Übersicht über die laufenden und anstehenden Einsätze von Polizei und Rettungskräften,
- Recherche in abgeschlossenen Einsätzen,
- Unterstützung der Einsatzdokumentation und
- Unterstützung der Alarmierung.

Während der Prüfung stellten wir mehrere Verstöße gegen das Brandenburgische Datenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung (BbgDSG a. F.) fest. Insbesondere entsprachen das gemäß § 7 Absatz 3 BbgDSG a. F. erforderliche Sicherheitskonzept sowie die Umsetzung wichtiger technischer und organisatorischer Sicherheitsmaßnahmen gemäß § 10 Absatz 1 und 2 BbgDSG a. F. nicht den gesetzlichen Anforderungen.

Das uns vom Polizeipräsidium vorgelegte Sicherheitskonzept für das Verfahren ELBOS war unvollständig. So lagen beispielsweise erforderliche Teildokumente erst im Entwurf vor. Außerdem war eine Vielzahl von Maßnahmen des IT-Grundschutzes noch nicht bearbeitet. Ein Sicherheitskonzept ist jedoch nur dann vollständig, wenn ihm auch der Status der Umsetzung der technischen und organisatorischen Maßnahmen zu entnehmen ist. Für noch ausstehende Maßnahmen ist ein Realisierungsplan beizufügen, der konkrete Termine und die jeweils verantwortlichen Personen enthalten muss.

Das Sicherheitskonzept für das Verfahren ELBOS basiert auf dem Rahmen-Sicherheitskonzept der Polizei, in dem wesentliche Teile wie angeschlossene Systeme, Komponenten und die technische Infrastruktur sowie grundlegende, verfahrensunabhängige Sicherheitsmaßnahmen beschrieben werden. Dieses hat die Polizei jedoch noch immer nicht fertiggestellt. Wir haben erneut gefordert, den damit verbundenen und seit Jahren bestehenden Mangel zu beseitigen sowie das auf dem Rahmenkonzept aufbauende Sicherheitskonzept für ELBOS konsequent umzusetzen.

Mit dem Verfahren WebView kann auf einen Teil der in ELBOS gespeicherten Daten lesend zugegriffen werden. So können beispielsweise laufende Einsatzprotokolle mitgelesen oder in bereits beendeten und archivierten Einsätzen Recherchen durchgeführt werden. Das Rechte- und Rollenkonzept für das Verfahren wurde erst im März 2018 fertiggestellt, nachdem polizeiinterne Informationen an die Öffentlichkeit gelangt waren. Aus Medienberichten konnten wir damals entnehmen, dass zuvor ca. 5.400 Beamtinnen und Beamte der Polizei einen Zugang zu WebView hatten. Nachdem wir dies hinterfragten, entwickelte eine Arbeitsgruppe des Polizeipräsidiums das vorliegende Rechte- und Rollenkonzept und setzte es um. Nun hatten etwa 2.300 Bedienstete Zugriff auf das Verfahren WebView. Aus Sicht der Polizei wird der Zugriff zwingend zur Aufrechterhaltung des Dienstbetriebes benötigt und erfolgt grundsätzlich nur auf Antrag sowie nach Bestätigung durch die Dienstvorgesetzten.

Zugriffe auf polizeiliche Daten streng regeln

Wir haben das Polizeipräsidium aufgefordert, künftig sicherzustellen, dass Rechte- und Rollenkonzepte vor Freigabe eines Fachverfahrens erstellt und umgesetzt werden. Zugriffsrechte sind möglichst restriktiv zu vergeben.

Im Verlauf der Prüfung stellten wir weiterhin fest, dass in der zentralen ELBOS-Datenbank sensitive personenbezogene Daten unverschlüsselt gespeichert werden. Dies kritisierten wir, da so nicht auszuschließen ist, dass diese Daten durch Administratorinnen und Administratoren sowie Wartungspersonal unberechtigt eingesehen oder sogar modifiziert werden. Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes bei der Verarbeitung von personenbezogenen Daten abzuwenden.

Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden.

Ob eine Dienstanweisung zur Protokollierung der Zugriffe in ELBOS und WebView existiert, konnte während der Prüfung nicht abschließend geklärt werden. Im Nachgang teilte uns die Polizei mit, dass bei WebView die Einsatznummer, die IP-Adresse des zugreifenden Clients, der Benutzername und die Zeit des Zugriffs protokolliert werden.

Wir forderten das Polizeipräsidium auf, in einer Dienstanweisung konkret festzuschreiben, welche personenbezogenen Daten in ELBOS und WebView protokolliert werden, wer für welche Zwecke einen Zugriff auf diese Daten erhält und wann ihre Löschung erfolgt. Die entsprechenden Festlegungen sind anschließend in den Verfahren umzusetzen.

2 Prüfung von Kfz-Werkstätten

Unternehmen, die Kraftfahrzeuge herstellen, tendieren zu einer immer umfangreicheren Datenverarbeitung in ihren Produkten. Im gleichen Maße werden rein technische Daten und Daten mit Personenbezug im Rahmen eines Werkstattbesuchs verarbeitet. Im Berichtszeitraum haben die Datenschutzaufsichtsbehörden mehrerer Länder die Verarbeitung von Fahrzeugdaten durch die Autowerkstätten in ihrem Zuständigkeitsbereich auf datenschutzrechtliche Relevanz und Rechtmäßigkeit untersucht.

Unsere Prüffragen richteten sich an insgesamt zehn freie und herstellergebundene Werkstätten im Land Brandenburg. Gefragt wurde insbesondere, auf welcher rechtlichen Grundlage Daten aus dem Fahrzeug in den eigenen Systemen verarbeitet werden, zu welchen Zwecken ggf. eine Datenübermittlung an die Herstellerunternehmen durchgeführt wird und wie die Kundinnen und Kunden darüber informiert werden.

Die Ergebnisse unserer Prüfung spiegeln die unterschiedliche Ausrichtung der Werkstätten hinsichtlich des Umfangs und der Zwecke der Datenverarbeitung wider. Während die kleineren selbstständigen Werkstätten grundsätzlich nur die für die Reparatur- oder

Wartungsarbeiten notwendigen Daten verarbeiten, übermitteln die größeren Unternehmen und insbesondere die Vertragswerkstätten auch Daten an die Fahrzeughersteller. Als Zwecke für diese Datenübermittlung wurden überwiegend angegeben:

- Prüfung einer Erstattung durch den Automobilhersteller in Garantie-, Gewährleistungs- oder Kulanzfällen,

- Fragen zur Durchführung einer konkreten Reparatur (technische Hotline, Fahrzeugdiagnose, Telediagnose),

- Produktüberwachung und -beobachtung, Produkthaftung und eventuelle Rückrufaktionen („sicherheitsrelevante Daten“),

- Produkt- und Qualitätsverbesserungen, Produktfortentwicklungen (Informationen zum Verschleiß, Diagnose- und Reparaturprotokolle),

- zentrale Führung einer elektronischen Wartungs- und Reparaturhistorie beim Hersteller; digitaler Servicenachweis,

- Marketingaktionen, Kundenzufriedenheitsbefragungen u. Ä. durch den Automobilhersteller und

- Vergütungs- und Bonusprogramme des Automobilherstellers für Werkstätten.

Obwohl ein Werkstattvertrag als datenschutzrechtliche Grundlage gemäß Artikel 6 Absatz 1 Buchstabe b Datenschutz-Grundverordnung (DS-GVO) für die Verarbeitung der für Reparatur, Wartung bzw. Service zwingend erforderlichen Fahrzeugdaten vorhanden ist, gaben manche Werkstätten zusätzlich eine Einwilligung als Rechtsgrundlage an. In diesen Fällen ist deren Einholung schlicht nicht erforderlich. Sie ist auch datenschutzrechtlich bedenklich, da im Fall ihres Widerrufs die Datenverarbeitung zur Erfüllung des Vertrags weiterhin zulässig wäre, bei der Kundin oder dem Kunden aber der Eindruck entstehen kann, ihre oder seine Daten würden nicht weiter verarbeitet.

Neben dem Vorliegen einer Rechtsgrundlage für die Datenverarbeitung sind die Kundinnen und Kunden gemäß Artikel 12 ff DS-GVO in präziser, transparenter, verständlicher und leicht zugänglicher Weise

über die Verarbeitung ihrer personenbezogenen Daten zu informieren. Ihnen sind unter anderem Name und Kontaktdaten des Verantwortlichen und evtl. seiner oder seines Datenschutzbeauftragten mitzuteilen, außerdem der Zweck der Verarbeitung und ihre Rechtsgrundlage, die Empfängerinnen bzw. Empfänger sowie deren Kategorien und die Dauer der Speicherung. Zudem sind die Betroffenen auf ihre Rechte hinzuweisen.

Die geprüften Werkstätten gaben an, dass sie ihrer Informationspflicht dadurch nachkommen, dass die Kundinnen und Kunden entweder in der Betriebsanleitung des Fahrzeugs, in der Einwilligungserklärung oder durch die Servicemitarbeiterinnen und -mitarbeiter aufgeklärt werden.

Wird ein Werkstattauftrag erteilt, genügen die Informationen in der Betriebsanleitung des Herstellers in der Regel nicht den Anforderungen des Artikels 13 DS-GVO. Die Werkstatt muss selbst über die entsprechenden Inhalte informieren. Hier wurde empfohlen, beispielsweise dem Werkstattvertrag ein Informationsblatt gemäß Artikel 12 und 13 DS-GVO beizulegen oder die Informationen auf der Rückseite des Vertrags aufzudrucken.

Zwar schreibt die Datenschutz-Grundverordnung für die Erteilung der Information keine Schrift- oder Textform vor, sodass die Auskünfte durch die Servicemitarbeiterinnen und -mitarbeiter ausreichen könnten. Allerdings muss der Verantwortliche gemäß Artikel 5 Absatz 2 DS-GVO nachweisen können, dass er informiert hat. Kann er dies im Falle des Bestreitens durch die Kundin oder den Kunden nicht, gelten die Informationen als nicht erteilt. Auch aus diesem Grund wurde den Werkstätten empfohlen, die Informationen schriftlich zur Verfügung zu stellen.

Werden die personenbezogenen Daten zu einem anderen Zweck als für die Erfüllung des Werkstattvertrages – bspw. für Marketingaktivitäten der Werkstatt – erhoben und verarbeitet und sind die in Artikel 13 DS-GVO aufgelisteten Informationen in der hierfür erforderlichen Einwilligungserklärung enthalten, entfällt eine gesonderte Information.

Die geprüften Werkstätten wurden auf die o. g. datenschutzrechtlichen Vorgaben hingewiesen und aufgefordert, sie zu beachten.

3 Prüfung des Klinischen Krebsregisters

Mit den Kolleginnen und Kollegen der Berliner Beauftragten für Datenschutz und Informationsfreiheit führten wir im Berichtszeitraum eine Prüfung des gemeinsamen Klinischen Krebsregisters (KKR) der Länder Brandenburg und Berlin durch. Dieses ist in der Rechtsform einer gemeinnützigen Gesellschaft mit beschränkter Haftung organisiert. Die Prüfung erfolgte ausschließlich in der Berliner Registerstelle, die auch Teile der Landesauswertestelle und Teile der Koordinierungsstelle beinhaltet. Im Vordergrund unserer Prüfung standen die technischen und organisatorischen Maßnahmen wie die physische Sicherheit der Registerstelle, die Revisionssicherheit sowie das Vorhandensein von Berechtigungskonzepten. Dabei handelt es sich um Maßnahmen, die wesentlich dazu dienen, ein dem hohen Schutzbedarf angemessenes Sicherheitsniveau gewährleisten zu können.

Weiterhin sahen wir uns auch die Implementierung der im Gesetz zu dem Staatsvertrag zwischen dem Land Berlin und dem Land Brandenburg über die Einrichtung und den Betrieb eines klinischen Krebsregisters nach § 65c des Fünften Buches Sozialgesetzbuch (KKR-StV) beschriebenen Verarbeitungsprozesse vor Ort an und analysierten diese. Unser besonderes Augenmerk galt dabei

- den Verfahrensschritten zur Bearbeitung einer Meldung im Versorgungsbereich einschließlich ihrer pseudonymisierten Übergabe an den Registerbereich und die Übermittlung an das Gemeinsame Krebsregister,

- dem Vorgehen bei Nachfragen an Meldende,

- dem Abgleich der eingehenden Meldungen mit der Widerspruchsdatenbank,

- dem Nachvollziehen der Verfahrensschritte zur Löschung von Datensätzen Verstorbener einschließlich einer Überprüfung, ob Altfälle entsprechend der Regelung im Staatsvertrag gelöscht wurden und

- dem Umgang mit Papierdokumenten (Aufbewahrung, Verarbeitung, Vernichtung).

Die Kontrolle ergab, dass die physische Sicherheit der Räumlichkeiten grundsätzlich gegeben ist. Auch der Umgang mit den Papierdokumenten ist ausreichend geregelt; von der Einhaltung der Festlegungen konnten wir uns überzeugen. So werden konsequent Aktenvernichter der Sicherheitsstufe P-6 gemäß DIN 66399 sowie Stahlschränke zum Verschließen von Papierunterlagen eingesetzt.

Die Meldungen großer Berliner Krankenhäuser an die Registerstelle werden vornehmlich elektronisch und verschlüsselt auf Datenträgern durchgeführt. Die Meldungen kleinerer Krankenhäuser und niedergelassener Ärztinnen und Ärzte gehen meist postalisch ein. Hier stellte sich heraus, dass diese Stellen vielfach von der Ausnahmeregelung des Artikels 13 Absatz 2 Satz 4 KKR-StV Gebrauch machten, wonach ärztliche Befundberichte statt der vom KKR bereitgestellten Meldeformulare verwendet werden können. Die Einsichtnahme in einige der im KKR verarbeiteten Befundberichte zeigte, dass bei deren Übersendung nicht durchgängig eine Beschränkung auf die für die klinische Krebsregistrierung erforderlichen Daten gemäß Artikel 13 Absatz 2 Satz 5 KKR-StV erfolgte. Darüber hinaus werden diese Meldungen – entgegen den Regelungen des Staatsvertrags – durch die Posteingangsbearbeiterinnen und -bearbeiter komplett eingescannt und dauerhaft elektronisch gespeichert. Dies ist ein Umstand, auf dessen Beseitigung wir drängen werden.

Die Registerstelle Berlin verfügt noch immer nicht über ein umfassendes Löschkonzept. Uns wurde zugesichert, dass dieses bis Mitte 2019 erstellt und umgesetzt wird. Ein Revisionskonzept gibt es, allerdings mussten wir feststellen, dass in den Protokolldateien auch medizinische Daten gespeichert wurden. Auf eine inhaltliche Anpassung der Protokolldateien haben wir deshalb hingewiesen. Weiterhin wurden wir informiert, dass eine smartcardbasierte Zwei-Faktor-Authentifizierung der Nutzerinnen und Nutzer eingeführt werden soll. Auch dieses Projekt werden wir begleiten.

Kapitel IV
Ausgewählte Fälle

IV Ausgewählte Fälle

1 Facebook Fanpages – wer ist verantwortlich?

Am 5. Juni 2018 entschied der Europäische Gerichtshof in der Rechtssache C-210/16, dass Fanpagebetreiberinnen und -betreiber für die auf ihrer Seite stattfindenden Datenverarbeitungen eine Mitverantwortung tragen. Ausgangspunkt war ein Rechtsstreit zwischen der Wirtschaftsakademie Schleswig-Holstein und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), der seit 2011 besteht. Das Unternehmen war der Ansicht, es dürfe Facebook Fanpages betreiben, ohne sich um die Einhaltung datenschutzrechtlicher Anforderungen kümmern zu müssen, obwohl bei der Nutzung der Fanpage – u. a. mit Hilfe von Tracking Cookies – umfangreiche Verhaltens- und Interessenprofile der Besucherinnen und Besucher angelegt werden, von denen die Fanpagebetreiberinnen oder -betreiber profitieren können. Dem folgte der Europäische Gerichtshof nicht.

Facebook räumt den Stellen, die Fanpages betreiben, die Möglichkeit ein, Statistiken und sonstige aufbereitete Daten über die Personen, die ihre Fanpages besuchen, einzusehen und zu nutzen. Sie sind demzufolge an der Entscheidung über die Zwecke und Mittel der Verarbeitung beteiligt und somit Verantwortliche im Sinne des Artikels 4 Nummer 7 der inzwischen in Kraft getretenen Datenschutz-Grundverordnung (DS-GVO). Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom Gericht festgestellte Mitverantwortung der Seitenbetreiberinnen und -betreiber erstreckt sich auch auf das aktuell geltende Recht. Somit liegt eine gemeinsame Verantwortlichkeit nach Artikel 26 DS-GVO vor.

Aus der Entscheidung folgt, dass Fanpagebetreiberinnen und -betreiber für Verstöße von Facebook gegen die Datenschutz-Grundverordnung mitverantwortlich sein können. Außerdem sind Vereinbarungen gemäß Artikel 26 Absatz 1 Satz 2 DS-GVO zu schließen, die in transparenter Form regeln, welche Seite für die Erfüllung welcher Betroffenenrechte (u. a. Auskunfts- und Löschungsrechte) ver-

antwortlich ist und wer von ihnen welche anderen Pflichten eines Verantwortlichen wahrnimmt.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) wies in ihrem Beschluss vom 5. September 2018 nicht nur auf die Notwendigkeit hin, eine solche Vereinbarung zu schließen, sondern forderte die Betreiberinnen und Betreiber von Fanpages auch dazu auf, die Rechtmäßigkeit der beim Betrieb der Fanpageseite nachweisbaren Verarbeitungsvorgänge anhand der Datenschutz-Grundverordnung darzulegen. Dies betraf etwa die Speicherfristen für Cookies, die Bildung von Profilen und die Speicherung von Daten der Nutzerinnen und Nutzer, die kein Facebook-Konto haben. Es ist bislang nicht ersichtlich, inwieweit eine derartige Rechtfertigung nach der geltenden Rechtslage möglich ist.

Facebook Fanpages nur in gemeinsamer Verantwortung

Unter den gegenwärtigen Bedingungen ist der Betrieb von Fanpages durch öffentliche oder nicht öffentliche Stellen dann rechtswidrig, wenn die Verantwortlichen nicht nachweisen können, dass die Anforderungen der Datenschutz-Grundverordnung im vollen Umfang erfüllt werden.

Nach der Entscheidung des Europäischen Gerichtshofs hat Facebook ein sogenanntes Addendum (Zusatzvereinbarung) veröffentlicht, mit dem die Anforderungen des Artikels 26 DS-GVO erfüllt werden sollen. Sein Ziel ist es, Fanpagebetreiberinnen und -betreiber von ihrer datenschutzrechtlichen Verantwortung so weit wie möglich zu entlasten, indem Facebook diese weitgehend übernimmt. Das Addendum ist jedoch nicht geeignet, einen rechtmäßigen Betrieb von Fanpages sicherzustellen. Es fehlt weiterhin an einer hinreichenden Aufklärung über die tatsächlich stattfindende Datenverarbeitung, ohne die Fanpagebetreiberinnen und –betreiber ihre Verantwortlichkeit nicht wahrnehmen können.

Im Ergebnis sollte jeder Verantwortliche prüfen, ob er seine Facebook Fanpage weiter betreiben kann.

2 Ehemalige Mitarbeiterin bei Facebook an den Pranger gestellt

Eine Arbeitgeberin publizierte auf dem öffentlichen Profil ihrer ehemaligen Mitarbeiterin bei Facebook, dass diese mehrere Tausend Euro Steuerschulden habe und daher ihr Lohn gepfändet werden müsse. Das Profil enthielt den Vor- und Nachnamen sowie Fotos der ehemaligen Mitarbeiterin, sodass diese eindeutig identifiziert werden konnte.

Nach § 43 Absatz 2 Nummer 1 des zum damaligen Tatzeitpunkt anwendbaren Bundesdatenschutzgesetzes handelte ordnungswidrig, wer vorsätzlich unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, verarbeitet. Von dem Begriff des Verarbeitens ist die Übermittlung der Daten an Dritte, also eine Offenlegung an sämtliche Personen, die das Facebookprofil besuchen können, erfasst. Für die Offenlegung der Steuerschulden und der Lohnpfändung auf der Facebookseite hatte die Arbeitgeberin keine Befugnis, da ihre ehemalige Mitarbeiterin weder darin eingewilligt hatte noch eine andere gesetzliche Rechtsgrundlage für diese Aktion vorlag. Personenbezogene Daten, die für die Durchführung eines Beschäftigungsverhältnisses erforderlich sind, wie die Tatsache, dass der Lohn gepfändet wurde, dürfen nur unter sehr engen Voraussetzungen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden. Durch die Offenbarung dieser sensitiven Daten in einem sozialen Netzwerk können der betroffenen Person massive wirtschaftliche Nachteile entstehen, da die Gefahr besteht, dass sich mögliche Vertragspartner abwenden. Auch im sozialen Leben kann das Ansehen der betroffenen Person stark beschädigt werden.

Die Arbeitgeberin hätte sich aufgrund ihrer beruflichen Stellung über die Folgen bewusst sein und das Veröffentlichen der personenbezogenen Daten unterlassen müssen. Die Landesbeauftragte verhängte daher ein Bußgeld in vierstelliger Höhe.

3 Nutzung von WhatsApp durch Behörden und Unternehmen

Auch im vergangenen Jahr erkundigten sich verschiedene Behörden und Unternehmen bei uns, ob sie den Dienst WhatsApp für ihre jeweiligen Zwecke datenschutzgerecht einsetzen können. Zum Teil

erhielten wir auch Beschwerden betroffener Personen, die die Verarbeitung ihrer Daten mittels dieses Dienstes rügten.

WhatsApp ist ein Instant-Messaging-Dienst des Unternehmens WhatsApp Inc. mit Sitz in Kalifornien (USA). Nutzerinnen und Nutzer können über diesen Dienst nicht nur Textnachrichten, sondern auch Bilder, Videos, Sprachdateien und andere Dokumente austauschen. Seit 2014 gehört WhatsApp zum Unternehmen Facebook Inc. Personen, die den Dienst nutzen möchten, müssen sich mit ihrer Mobilfunknummer registrieren. WhatsApp liest daraufhin regelmäßig das Telefonbuch der Nutzerinnen und Nutzer aus und speichert dessen Inhalt (mindestens die Namen und Telefonnummern der Kontakte) auf den eigenen Servern. Der Abgleich der Kontaktdaten dient in erster Linie dazu, den Nutzerinnen und Nutzern mitzuteilen, wer ebenfalls bei diesem Dienst angemeldet ist. Der vollständige Zugriff auf das Telefonbuch erfolgt zunächst unabhängig davon, ob der jeweilige Kontakt selbst WhatsApp verwendet oder nicht.

Sobald also jemand WhatsApp auf dem Mobiltelefon nutzt, werden damit immer auch Daten Dritter aus der Liste aller Kontakte an das US-Unternehmen preisgegeben. Das Auslesen und Übertragen des Telefonbuchs an WhatsApp stellt eine Übermittlung von Daten dar. Regelmäßig dürfte hierfür keine Einwilligung aller betroffenen Personen vorliegen, sodass es bei behördlicher oder geschäftlicher Nutzung keine Rechtsgrundlage für die Verarbeitung gibt. Zugleich handelt es sich hier um eine Zweckänderung, da die Daten ursprünglich nicht zum Zwecke der Übermittlung an WhatsApp erhoben wurden. Auch die Zulässigkeit dieser Zweckänderung ist zweifelhaft. Wollte sich eine Anwenderin oder ein Anwender datenschutzgerecht verhalten, wäre sie oder er dazu verpflichtet, einem Löschanspruch betroffener Personen nachzukommen. Die Erfüllung dieses Anspruchs ist insbesondere im Hinblick auf die Durchsetzung gegenüber WhatsApp äußerst fraglich.

Mit Wirksamwerden der Datenschutz-Grundverordnung hat WhatsApp seine Nutzungsbedingungen und Datenschutzrichtlinien geändert. Wer den Dienst weiter nutzen möchte, muss diesen Änderungen zustimmen. Die Bedingungen und Richtlinien beinhalten auch das „Teilen“ von Informationen mit Facebook – es steht somit eine Datenübermittlung von WhatsApp an die Konzernmutter Facebook im Raum. Zweck dieser Übermittlung soll z. B. die kontinuierliche Verbesserung des Dienstes sowie die Gewährleistung des Schutzes

und der Sicherheit der Nutzenden, aber auch das Einblenden personalisierter Werbung sein. Nach eigenen Angaben werden die Telefonnummer, Gerätekennung, Betriebssysteminformation, App-Version, Plattforminformation, Ländervorwahl der Mobilnummer, Netzwerkcode und Nutzungsinformationen (letzte Nutzung, Anmeldung, Art und Häufigkeit der Nutzung von Features) an Facebook übertragen. Auch hier bestehen erhebliche Bedenken hinsichtlich der Wirksamkeit der Einwilligung in die Weitergabe der Daten.

Da eine datenschutzkonforme Nutzung des WhatsApp-Dienstes aus unserer Sicht derzeit nicht möglich ist, halten wir dessen Verwendung durch öffentliche sowie nicht öffentliche Stellen grundsätzlich für unzulässig. Beispielhaft werden im Folgenden drei Fälle beschrieben, mit denen wir uns im Berichtsjahr befasst haben:

Dauerbrenner WhatsApp

So wurde uns angezeigt, dass eine Apotheke WhatsApp zur Kommunikation im Unternehmensverbund sowie mit den Kundinnen und Kunden nutze. Nach Anhörung und Beratung der Geschäftsführung stellte diese die aktive Nutzung und Bewerbung des Messenger-Dienstes für den gesamten Unternehmensverbund ein. Die Umstellung der Kommunikation mit den Kundinnen und Kunden erfolgte kurze Zeit später, da diese vorab informiert werden mussten und die zum Teil lebenswichtige medikamentöse Versorgung umzuorganisieren war.

Auch im kommunalen Umfeld gab es Bestrebungen, WhatsApp zu nutzen. Ein Jugendamt hielt WhatsApp für die mittlerweile einzige Möglichkeit der Kontaktaufnahme mit den betroffenen Jugendlichen. In einer anderen Verwaltung war geplant, die Kommunikation zwischen Beschäftigten im Außendienst (z. B. des Ordnungsamtes) per WhatsApp zu ermöglichen, etwa um schnell Informationen auszutauschen oder Unterstützung herbeizurufen.

Im Fall eines Kindergartens hielten wir es für unzulässig, dass deren Leiterin die bei ihr lediglich für Notfälle hinterlegten Telefonnummern der Eltern ohne deren Einwilligung im Rahmen einer WhatsApp-Gruppe an alle Eltern weitergegeben hat, um zweckwidrig über kitainterne personelle Angelegenheiten ihrer Erzieherinnen zu informieren. Hierfür hätte es allerdings auch auf analogem Wege bereits keine Rechtsgrundlage gegeben.

Zwar mag das Ansinnen öffentlicher Stellen nachvollziehbar sein, auch moderne Kommunikationsmittel zu nutzen. Allerdings stehen einer Verwendung des Dienstes WhatsApp rechtliche Vorgaben aus der Datenschutz-Grundverordnung und dem Brandenburgischen Datenschutzgesetz sowie zum Teil spezialgesetzliche Regelungen entgegen. Grundsätzlich empfehlen wir stattdessen, Kommunikationskanäle zu nutzen, die unter Kontrolle und Administration der Verwaltung stehen und eine sichere, vertrauliche Kommunikation gewährleisten. Für die Kommunikation zwischen Außendienstmitarbeiterinnen und -mitarbeitern wären bspw. auch ein E-Mail-Austausch über gesicherte Verbindungen und der Einsatz von Push-Diensten möglich. Auch im Falle des Jugendamtes, das zusätzlich Sozialdaten verarbeitet, sollte auf den Einsatz von WhatsApp verzichtet werden, da neben der fehlenden administrativen Kontrolle durch die Verwaltung auch keine Rechtsgrundlage für die Datenübermittlung in die USA in den Sozialgesetzbüchern erkennbar ist.

4 Digitaler Sprachassistent Alexa in einer Praxis für Physiotherapie?

Im Berichtszeitraum erreichte uns ein Hinweis, dass in einer Physiotherapie-Praxis in mindestens einem Behandlungsraum der digitale Sprachassistent Alexa genutzt werde.

Alexa ist ein sprachgesteuerter, internetbasierter Dienst des US-Unternehmens Amazon, der als persönlicher Assistent nach der Aktivierung mit einem Signalwort Befehle entgegennimmt und Aktivitäten ausführt, etwa Informationen ausgibt, Musik abspielt, Termine und Kontakte verwaltet, Bestellungen aufgibt u. a. m. Nutzerinnen und Nutzer interagieren mit dem Dienst mit Hilfe spezieller Geräte (wie Amazon Echo oder Echo Dot), die über Mikrofone und Lautsprecher verfügen. Die Mikrofone lauschen im Bereitschaftsmodus auf das Signalwort und übertragen dann die gesprochenen Befehle zu zentralen Amazon-Servern, wo sie verarbeitet werden.

Den Einsatz dieses Sprachassistenten stufen wir als datenschutzrechtlich problematisch ein. So können die Sprachaufzeichnung und die Befehlsverarbeitung evtl. auch unbeabsichtigt gestartet werden, wenn nicht das Signalwort selbst, sondern ein phonetisch ähnliches Wort im Gespräch verwendet und durch den Dienst erkannt wird (Signalwort: „Alexa“, im Gespräch verwendet: „Alexander“ oder „Alexandra“).

Des Weiteren kann nicht ausgeschlossen werden, dass im aktivierten Zustand Hintergrundgespräche unbeteiligter Personen unberechtigterweise mit aufgezeichnet werden. Entscheidend hierfür sind die örtlichen Gegebenheiten, die den möglichen Erfassungsbereich der akustischen Aktivierung und Aufzeichnung bestimmen. Außerdem sind die Mechanismen zur Verschlüsselung der Datenströme vom Amazon Echo System zu den zentralen Servern, die auch im Bereitschaftsmodus und bei ausgeschaltetem Mikrofon registrierbar sind, nicht offengelegt und damit nicht überprüfbar.

Das System zeigte darüber hinaus auch andere Schwächen. So wurde 2017 eine Sicherheitslücke entdeckt, durch die die Kontrolle über ein Amazon Echo Gerät übernommen werden konnte. Hierfür wurden in der Nähe des Geräts akustische Signale ausgesandt, die im für Menschen nicht wahrnehmbaren Frequenzbereich lagen. Das Spracherkennungssystem konnte derartige Signale jedoch erfassen und die zugehörigen Befehle verarbeiten. Weiterhin bestehen Risiken durch die Speicherung der Sprachbefehle bei Amazon. So wurde gegen Ende des Berichtszeitraums publik, dass das Unternehmen einem Kunden auf dessen Auskunftsbegehren nach der Datenschutz-Grundverordnung hin die Sprachnachrichten eines Anderen zugesandt hatte.

Die Nutzung eines digitalen Sprachassistenten in einer Umgebung, in der auch vertrauliche Daten in Gesprächen ausgetauscht werden (wie z. B. in Behandlungsräumen) kann zu Risiken für die Rechte und Freiheiten der Betroffenen führen. Nachdem uns die Geschäftsleitung der in Rede stehenden Physiotherapie-Praxis glaubhaft mitteilte, keine digitalen Sprachassistenten einzusetzen, sahen wir davon ab, in der Angelegenheit weiter tätig zu werden.

5 Einsatz von Skype durch eine Hebamme

Eine brandenburgische Hebamme, die Beratungsleistungen über den Instant-Messaging- und Videokonferenzdienst Skype anbietet, wandte sich an uns. Sie beabsichtigte, ihr Angebot datenschutzkonform auszugestalten und bat um Auskunft, welche Vorgaben sie gemäß der Datenschutz-Grundverordnung einhalten müsse. Zur Bewertung übergab sie uns auch den Entwurf einer Datenschutzerklärung.

Nach eingehender Prüfung des Sachverhalts stellten wir fest, dass gegen eine Nutzung des Skype-Dienstes in diesem Fall erhebliche rechtliche Bedenken bestehen. In der beschriebenen Beratungsumgebung werden sensitive Gesundheitsdaten verarbeitet, wobei ein besonderes Risiko im Hinblick auf die Rechte und Freiheiten der betroffenen Personen entstehen kann. Darüber hinaus ist nicht sichergestellt, dass umfassend geeignete technische und organisatorische Maßnahmen ergriffen wurden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Skype ist ein internetbasierter Dienst, der u. a. für Videokonferenzen, Nachrichtenübertragung, Telefonie und Dateiaustausch genutzt wird. Anbieter ist seit einigen Jahren das Unternehmen Microsoft. Der Dienst speichert gemäß seinen Nutzungsbedingungen Inhalte von Gesprächen zumindest kurzfristig auf einem zentralen Server. Zudem enthält der Servicevertrag die Aussage, dass Microsoft, soweit dies für die Bereitstellung des Dienstes, den Schutz des Nutzers oder des Dienstes oder die Produkt- und Dienstverbesserung notwendig sei, eine weltweite und gebührenfreie Lizenz für geistiges Eigentum zur Inhaltsnutzung erhalte. Damit dürfte die Berechtigung von Microsoft verbunden sein, die Inhalte eines Gesprächs, das über Skype geführt wird, unter bestimmten Voraussetzungen zu speichern, zu übertragen, zu kopieren oder weiterzugeben. Die Vertraulichkeit einer online angebotenen Beratung ist damit nicht mehr sichergestellt.

Weiterhin erfolgen die Kommunikation sowie die Steuerung der Datenflüsse intransparent mit Hilfe eines proprietären Kommunikationssystems über Microsoft-Rechenzentren. Die Sicherheitsfunktionen sind damit nicht überprüfbar. Da auch die Schlüssel zur Verschlüsselung bei Microsoft liegen, ist nicht ausgeschlossen, dass das Unternehmen selbst oder Dritte unberechtigt auf die Übertragungsinhalte zugreifen können.

Der Hebamme haben wir dringend empfohlen, von der Nutzung des Dienstes Skype Abstand zu nehmen.

6 Verwendung von Fotos ehemaliger Beschäftigter auf der Unternehmens-Webseite

Das Ansehen eines Unternehmens wird nicht nur durch dessen Produkte, sondern vor allem auch durch dessen Außendarstellung maßgeblich beeinflusst. Für die persönliche und langfristige Kundenbeziehung setzen zahlreiche Unternehmen daher auf Fotos ihrer Mitarbeiterinnen und Mitarbeiter insbesondere für den eigenen Internetauftritt, um die Menschen hinter dem Unternehmen zu betonen.

Uns erreichte in diesem Zusammenhang die Beschwerde eines ehemaligen Mitarbeiters eines produzierenden Betriebes. Auch noch nachdem das Beschäftigungsverhältnis beendet worden war, hielt das verantwortliche Unternehmen Fotos der betroffenen Person auf der Webseite vor und verwendete diese zu Zwecken der Werbung.

Das Recht am eigenen Bild ist als grundrechtlich verankertes Rechtsgut besonders geschützt. Es darf daher nicht ohne Weiteres übergangen werden, selbst wenn der Arbeitgeber ein berechtigtes Interesse an der Verwendung des Fotos aus wirtschaftlichen Gründen hat. Darüber hinaus regelt § 26 Absatz 1 Bundesdatenschutzgesetz, dass personenbezogene Daten von Beschäftigten nur dann ohne Einwilligung der betroffenen Person verarbeitet werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder Beendigung erforderlich ist. Eine Einwilligung lag zum Zeitpunkt der Beschwerde nicht vor und die Bereitstellung der Fotos für eine breite Öffentlichkeit ließ sich aufgrund des Beschäftigungsverhältnisses nicht rechtfertigen, zumal dieses bereits beendet war. Da eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten nicht bestand, hat die betroffene Person gemäß Artikel 17 Absatz 1 Datenschutz-Grundverordnung ein Recht auf unverzügliche Löschung.

Wir haben den Verantwortlichen daher aufgefordert, die entsprechenden Fotos von der Webseite zu entfernen, um den Rechten des Beschwerdeführers zu entsprechen. Dies wurde auch unmittelbar umgesetzt.

7 Wer war zu schnell mit dem Dienstwagen unterwegs?

Zur Verfolgung von Geschwindigkeitsübertretungen werden in der Regel „Blitzerfotos“ genutzt, die das Kfz-Kennzeichen und die Person hinter dem Lenkrad zeigen. Soll ein Verwarn- oder Bußgeld verhängt werden, muss die konkrete Person, die das Fahrzeug geführt hat, ermittelt werden. Ist das Fahrzeug ein Dienstwagen und somit auf eine Behörde oder ein Unternehmen zugelassen, wirft dies regelmäßig die datenschutzrechtliche Frage auf, ob die Fahrzeughalterin oder der Fahrzeughalter die Daten der Fahrerin oder des Fahrers an die Verfolgungsbehörde übermitteln darf. Seit Geltung der Datenschutz-Grundverordnung (DS-GVO) erhielten wir mehrfach Anfragen, ob die Übermittlung des Namens an die Verfolgungsbehörde nach neuem Recht noch zulässig ist und ob die Arbeitgeberin oder der Arbeitgeber zur Übermittlung entsprechender Daten verpflichtet ist.

7.1 Übermittlungsbefugnis

Die Information, wer von den Beschäftigten einer Behörde oder eines Unternehmens den Dienstwagen zu einem bestimmten Zeitpunkt gefahren hat, ist ein personenbezogenes Datum im Sinne des Artikels 4 Nummer 1 DS-GVO. Dieses darf nur bei Vorliegen einer Einwilligung der betroffenen Person oder aufgrund einer sonstigen Rechtsgrundlage verarbeitet werden. Der Begriff der Verarbeitung umfasst auch die Offenlegung der Daten durch Übermittlung an Dritte.

Artikel 6 Absatz 1 Buchstabe c DS-GVO gestattet die Verarbeitung personenbezogener Daten, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der ein Verantwortlicher – also z. B. ein als Fahrzeughalter ermitteltes Unternehmen – unterliegt.

Das Straßenverkehrsrecht legt nahezu alle aus der Zulassung und dem Betrieb eines Fahrzeugs folgenden Pflichten ausdrücklich der Halterin oder dem Halter auf. Es ist daher grundsätzlich ihre oder seine Sache, auch ohne Vorlage eines Fotos Angaben zu der Person

zu machen, die im fraglichen Zeitpunkt das Fahrzeug geführt hat.[16] Der Gesetzgeber hat die Herausgabe der Daten der oder des Fahrzeugführenden nach unseren Erkenntnissen zwar nicht ausdrücklich als Pflicht der Halterin oder des Halters normiert. Die aus der Haltereigenschaft abzuleitende Verpflichtung halten wir jedoch für ausreichend und auch für erforderlich, wenn anderenfalls die Feststellung der oder des für den Geschwindigkeitsverstoß Verantwortlichen vor Eintritt der Verfolgungsverjährung unmöglich würde.

Darüber hinaus wird ein Unternehmen als Halter bzw. die das Unternehmen vertretende Person in diesem Fall von der Verfolgungsbehörde als Zeugin angehört. Sie ist – vorbehaltlich eines Zeugnisverweigerungsrechts gemäß §§ 52, 53 Strafprozessordnung (StPO) – verpflichtet, auszusagen und auf Befragung wahrheitsgemäße Angaben über die fahrzeugführende Person zu machen (§ 48 Absatz 1 und § 57 Absatz 1 StPO i. V. m. § 46 Gesetz über Ordnungswidrigkeiten [OWiG]). Bei der Zeugnispflicht handelt es sich schon nach allgemeiner Rechtstradition um eine staatsbürgerliche Pflicht[17], die zudem in § 48 Absatz 1 und § 161a Absatz 1 Satz 1 StPO ausdrücklich bestimmt ist. Diese Pflicht besteht nicht nur gegenüber dem Gericht und der Staatsanwaltschaft, sondern aufgrund einer Verweisungsklausel im Ordnungswidrigkeitenrecht auch gegenüber der Verwaltungsbehörde, die im Bußgeldverfahren dieselben Rechte und Pflichten wie die Staatsanwaltschaft hat (§ 161a StPO i. V. m. § 46 Absatz 2 OWiG).

Die Halter- und Zeugnispflicht sind rechtliche Verpflichtungen des Verantwortlichen im Sinne des Art. 6 Abs. 1 Buchstabe c DS-GVO. Wenn andere Ermittlungsbemühungen der Behörden nicht erfolgversprechend sind und kein Ermittlungsdefizit vorliegt, ist die Benennung der Person, die das Fahrzeug zum fraglichen Zeitpunkt geführt hat, auch als erforderlich anzusehen. Damit unterliegt die Halterin oder der Halter auch nach den Vorschriften der Datenschutz-Grundverordnung keinen datenschutzrechtlichen Übermittlungsbeschränkungen und darf die Angaben zur Fahrerin oder zum Fahrer an die Verfolgungsbehörde weitergeben.

16 Beschluss des Oberverwaltungsgerichts Nordrhein-Westfalen vom 29. April 2003, 8 A 3435/01.

17 Beschluss des Bundesverfassungsgerichts vom 8. Januar 1996, 2 BvR 2715/95.

7.2 Zweckänderung im Beschäftigungsverhältnis

Ein weiterer datenschutzrechtlicher Aspekt in diesem Zusammenhang ist die Frage, ob die Arbeitgeberin oder der Arbeitgeber mit der Übermittlung des Namens der beschäftigten Person, die das Fahrzeug geführt hat, an die Bußgeldstelle den Grundsatz der Zweckbindung im Beschäftigungsverhältnis verletzt. Denn für Beschäftigte gilt, dass ihre personenbezogenen Daten grundsätzlich nur für die Begründung, Durchführung, Beendigung und Abwicklung des Beschäftigungsverhältnisses oder mit Einwilligung der Beschäftigten verarbeitet werden dürfen (vgl. § 26 Bundesdatenschutzgesetz für nicht öffentliche Stellen und § 26 Brandenburgisches Datenschutzgesetz für öffentliche Stellen). In zwei Fällen wurde die Landesbeauftragte um ihre Einschätzung gebeten, ob Arbeitgeberinnen und Arbeitgeber durch diese Zweckbindungsvorschrift daran gehindert sind, personenbezogene Daten ihrer Beschäftigten an Bußgeldbehörden herauszugeben:

Im ersten Fall trat eine kreisfreie Stadt an uns heran, deren Bußgeldstelle wegen eines Verkehrsverstoßes gegen den Fahrer ermittelte. Halter des in den Vorfall verwickelten Fahrzeugs sei eine juristische Person, es läge nahe, dass der Fahrer, dessen „Blitzerfoto“ vorlag, Angestellter dieses Unternehmens sei. Die Geschäftsführung des Unternehmens sei um Mitteilung der erforderlichen personenbezogenen Daten des Fahrers gebeten worden. Das Unternehmen habe jedoch die Herausgabe der Daten verweigert. Zur Begründung habe es angegeben, seit Einführung der Datenschutz-Grundverordnung bedürfe es hierfür der Einwilligung der betroffenen Person, die aber nicht vorläge. Die Stadt bat um Auskunft, ob das Unternehmen an der Weitergabe der Daten tatsächlich gehindert sei.

Gemäß Artikel 6 Absatz 4 DS-GVO ist eine zweckändernde Datenverarbeitung zulässig, wenn sie auf eine Rechtsvorschrift der Union oder der Mitgliedstaaten gestützt werden kann, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 DS-GVO genannten Ziele darstellt. Eine solche Rechtsgrundlage ist § 161a StPO i. V. m. § 46 OWiG (vgl. dazu die Ausführungen oben). Sie erlaubt nicht nur die Übermittlung, ihr ist auch die Erlaubnis zur Zweckänderung immanent. Einer ausdrücklichen Ermächtigung zur Zweckänderung bedarf es nicht.

Diese Rechtsgrundlage genügt auch den Vorgaben von Artikel 23 Absatz 1 DS-GVO: Buchstabe d dieser Vorschrift nennt die Ermittlung, Aufdeckung und Verfolgung von Straftaten als einen tauglichen Zweck. Da in den Rechtsordnungen vieler Mitgliedsstaaten nicht zwischen Straftaten und Ordnungswidrigkeiten unterschieden wird, kann davon ausgegangen werden, dass auch Ordnungswidrigkeiten unter diese Vorschrift fallen. Da Betroffene sich weiterhin nicht selbst belasten müssen, ist, wie in Artikel 23 Absatz 1 DS-GVO gefordert, auch der Wesensgehalt der Grundrechte und -freiheiten in verhältnismäßiger Weise gewahrt. Somit ist die Zweckänderung vorliegend grundsätzlich zulässig und stünde einer Übermittlung der erforderlichen Daten nicht im Weg.

Im zweiten Fall bat ein Landkreis um Auskunft, ob er als öffentliche Stelle datenschutzrechtlich daran gehindert sei, einer Bußgeldstelle die zur Verfolgung eines bußgeldbewehrten Verkehrsverstoßes erforderlichen Daten eines Mitarbeiters zu übermitteln. Die Landesbeauftragte verneinte diese Frage.

Der auf Artikel 6 Absatz 1 Buchstabe e DS-GVO basierende § 5 Absatz 1 Brandenburgisches Datenschutzgesetz (BbgDSG) bestimmt, dass die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig ist, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist. Die Aufgabe besteht hier in der Kooperation mit den ermittelnden Behörden gemäß § 163 Absatz 1 Satz 2 StPO. Auch die erforderliche Zweckänderung lässt sich im Ergebnis rechtfertigen. Rechtsgrundlage ist § 6 Absatz 1 Nummer 3 BbgDSG. Danach ist die zweckändernde Verarbeitung zulässig, wenn sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint.

Zu bedenken ist hier zwar, dass die Anhaltspunkte nicht im Rahmen der eigenen Aufgabenerfüllung aufgetreten sind, sodass es sich nicht um eine Unterrichtung im Sinne einer Mitteilung eines Sachverhalts an einen bisher unkundigen Dritten handelt. Wir gehen aber davon aus, dass auch solche Fälle unter den Unterrichtungsbegriff fallen können, wenn – und sei es auf Nachfrage – für die empfangende Stelle neue Tatsachen offengelegt werden.

Die Verfolgungsbehörden sollten nach alledem im Interesse eines reibungslosen Verfahrens der übermittelnden Stelle die Rechtsnormen darlegen, aus denen sich eine Verpflichtung zur Datenübermittlung ergibt. Der Umstand, dass für die Erfüllung einer solchen Verpflichtung eine Übermittlung von Daten erforderlich ist, die zum Zweck der Abwicklung von Beschäftigungsverhältnissen gespeichert worden sind, steht der Auskunft jedenfalls in Fällen, in denen der Vorwurf einen Bezug zum Arbeitsverhältnis hat, regelmäßig nicht im Weg.

8 Fälle zur Videoüberwachung

8.1 Versteckte Kameras im Jagdpachtbezirk

Ein Jäger fragte uns, ob es zulässig sei, im Wald eine verdeckte Videoüberwachung zu betreiben. Zur Begründung führte er an, dass wildernde Personen in seinem Pirschbezirk ihr Unwesen trieben. Zudem würde ein für den öffentlichen Verkehr gesperrter Zufahrtsweg zum Wald von Passantinnen und Passanten als Durchfahrtsstraße missbraucht und vermehrt Müll im Wald abgeladen. Auch gebe es Hinweise, dass im Wald illegale Schießübungen stattfänden.

Datenverarbeitungen, wozu auch die Anfertigung von Videosequenzen mittels einer Videokamera gehört, sind nur zulässig, wenn die betroffenen Personen eingewilligt haben oder eine andere gesetzliche Erlaubnisnorm erfüllt ist. Da die Einholung von Einwilligungserklärungen des unbeschränkten Kreises der Waldbesucherinnen und Waldbesucher ausgeschlossen war, kam hier nur Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) in Betracht. Danach ist eine Verarbeitung personenbezogener Daten zulässig, soweit dies zur Wahrung berechtigter Interessen des Verantwortlichen oder Dritter erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, überwiegen.

Da es sich um allgemein zugänglichen Wald im öffentlichen Eigentum handelte, lagen die vom Jäger verfolgten Zwecke der Strafverfolgung und der Gefahrenabwehr nicht im originär eigenen Interesse. Datenverarbeitungen für diese Zwecke obliegen ausschließlich den hierfür zuständigen Behörden und sind nur aufgrund strenger, bereichsspezifischer Regelungen gestattet. Der beabsichtigte Betrieb

der Videoüberwachung für Zwecke der Polizei oder Ordnungsbehörden wäre deshalb unzulässig.

Als eigenes Interesse des Jägers erkannten wir hingegen den Schutz vor Jagdwilderei in seinem Pirschbezirk an. Sein berechtigtes Interesse als Jagdausübungsberechtigter ergab sich aus der Aufgabe einer effektiven Wildsorge und Wildbewirtschaftung, die auf das Jagdgesetz für das Land Brandenburg gestützt werden konnte.

Dieses Interesse war den Interessen, Grundrechten und Grundfreiheiten der Betroffenen, insbesondere dem Recht auf Schutz ihrer personenbezogenen Daten, gegenüberzustellen. Personen, die von der Videoüberwachung betroffen wären, halten sich im Wald zumeist zur Erholung und Freizeitgestaltung auf. Dies wird auch durch § 15 Landeswaldgesetz geregelt, wonach das Betreten des Waldes zum Zweck der Erholung grundsätzlich jedermann gestattet ist. Diese Interessen sind als besonders schützenswert anzusehen.

Hinzu kommt, dass Kinder, die beim Spielen im Wald ebenfalls von den Videokameras erfasst würden, nach Artikel 6 Absatz 1 DS-GVO besonderen Schutz genießen. Ihre Interessen sind in der Interessenabwägung nach dem gesetzgeberischen Willen besonders zu gewichten. Als weiteren Aspekt berücksichtigten wir, dass eine Vielzahl an Personen anlasslos als Unbeteiligte erfasst werden könnte. Als wichtiger Gesichtspunkt sind in der Interessenabwägung zudem die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen. Diese erwarten beim Betreten des Waldes keinesfalls, von Videokameras aufgezeichnet zu werden.

Im Ergebnis überwogen in Waldbereichen, die für Erholungszwecke der Allgemeinheit gewidmet sind, die schutzwürdigen Interessen der betroffenen Waldbesucherinnen und Waldbesucher das Interesse des Jägers an der Wildsorge und Wildbewirtschaftung, weswegen die geplante Videoüberwachung in diesem Bereich unzulässig wäre.

Darüber hinaus wäre ein verdeckter Einsatz von Videoüberwachungsanlagen in diesem Fall mit dem Transparenzgedanken der Datenschutz-Grundverordnung unvereinbar.

8.2 Videoüberwachung einer Garagenanlage

Aufgrund einer Beschwerde wurden wir auf ein Garagengelände aufmerksam, das mit Videokameras überwacht wurde. Betreiber der Garagenanlage und der Kameras war ein Verein. Als Zweck der Videoüberwachung gab dieser an, mögliche Straftaten beweisen zu können. Da der Verein zahlreiche Einbrüche, Sachbeschädigungen und Diebstähle – darunter einen besonders schweren Fall – auf dem Gelände uns gegenüber darlegen konnte, erkannten wir ein berechtigtes Interesse an dem Betrieb der Videokameras an. In der vorzunehmenden Interessenabwägung berücksichtigten wir, dass das Garagengelände vollständig umzäunt und nur von einem abschließend definierten Personenkreis betreten werden konnte.

Eine Videobeobachtung in Echtzeit erachteten wir dennoch als unzulässig. Denn um Täternachweise bei Vorfällen zu erhalten, war es nicht erforderlich, dass die Nutzerinnen und Nutzer der Garagen den ganzen Tag live am Monitor beobachtet werden. Demgegenüber hielten wir eine Speicherung der Videobilder angesichts der Interessen der betroffenen Personen für zulässig, allerdings nur in den Abendstunden und in der Nacht, weil in dieser Zeit die Begehung von Straftaten wahrscheinlicher war.

Um die Videoüberwachungsanlage rechtskonform betreiben zu können, müssen auch die gesetzlichen Vorschriften zu den technisch-organisatorischen Anforderungen erfüllt sein. Wir forderten den Betreiber daher u. a. auf, sicherzustellen, dass die erfolgten Zugriffe auf das Bildmaterial protokolliert und nicht mehr erforderliche Aufnahmen regelmäßig gelöscht werden. Außerdem sollte er entsprechende Nachweise und Dokumentationen vorlegen. Dem wollte der Betreiber jedoch nicht nachkommen; er entschied sich deshalb, die Videoüberwachung einzustellen und sicherte uns den Abbau der Kameras zu.

Kapitel V
Ausgewählte Beratungen

V Ausgewählte Beratungen

1 Stellungnahmen gegenüber Landtag und Landesregierung

1.1 Brandenburgisches Polizeigesetz

Wie fast alle Bundesländer strebt auch Brandenburg eine Neufassung des Polizeigesetzes an – nach Angaben der Landesregierung als Reaktion auf terroristische Bedrohungen. Sie beteiligte uns bereits im Jahr 2017 an einem ersten Referentenentwurf und im Juli 2018 an einem überarbeiteten Gesetzentwurf zur Änderung des Brandenburgischen Polizeigesetzes. Zu beiden Entwürfen nahmen wir gegenüber dem Ministerium des Innern und für Kommunales umfassend Stellung.

Der Gesetzentwurf zeichnete sich durch eine deutliche Ausweitung bestehender und Schaffung neuer polizeilicher Eingriffsbefugnisse aus. Mit Sorge betrachten wir, dass das grundrechtlich verbürgte informationelle Selbstbestimmungsrecht mit jedem Änderungsgesetz weiter unter Druck gerät, indem immer weiter reichende polizeiliche Datenverarbeitungsbefugnisse, die kumulativ zu betrachten sind, geschaffen werden. Das Bundesverfassungsgericht hat insoweit eine Gesamtschau aller Eingriffe in das Persönlichkeitsrecht angemahnt. Dies ist angesichts der immer größeren Datenmengen, die erhoben und ausgewertet werden dürfen, und der Ausweitung heimlicher Ermittlungsbefugnisse, auch dringend geboten.

Das Kernstück des Entwurfs war ein neu eingefügter Abschnitt 1a, der besondere Befugnisse zur Abwehr von Gefahren des Terrorismus festlegt. Er umfasste einerseits schon zu Zwecken der allgemeinen Gefahrenabwehr etablierte Befugnisse wie erkennungsdienstliche Maßnahmen, polizeiliche Ausschreibungen, Aufenthaltsverbote oder die anlassbezogene Kennzeichenfahndung. Andererseits sah er bisher nicht im Polizeigesetz enthaltene Maßnahmen wie Kontaktverbote und die elektronische Aufenthaltsüberwachung vor. Die nicht auf den ersten Blick erkennbare Besonderheit bestand darin, dass es damit zulässig wäre, diese Eingriffe ganz überwiegend bereits im Vorfeld einer konkreten Rechtsgutgefährdung einzusetzen, nämlich dann, wenn

- bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Rechtsgutschädigung begehen wird oder

- das individuelle Verhalten die konkrete Wahrscheinlichkeit einer Rechtsgutsschädigung in übersehbarem Zeitraum begründet.

Diese Formulierung, die aus der Begründung des Urteils des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz als äußerste Grenze für eine Überwachungsmaßnahme übernommen wurde und als gesetzliche Eingriffsvoraussetzung für eine Vielzahl von polizeilichen Maßnahmen dienen soll, haben wir als nicht ausreichend normenklar kritisiert. Die mit der Unschärfe des beschriebenen Kausalverlaufs und der zeitlichen Vorverlagerung verbundene Ausdehnung des polizeilichen Fokus auf möglicherweise betroffene Unbeteiligte war für uns nicht hinnehmbar. Das Einschreiten der Polizei wäre für den Einzelnen aufgrund der nicht ausdefinierten Begriffe nicht mehr vorhersehbar. Auch für die praktische Anwendung durch die Sicherheitsbehörden wäre sie ungeeignet. Sie ließe sich mit den herkömmlichen Gefahrenbegriffsbestimmungen nicht vereinbaren, sodass die Ausfüllung dieses „vorverlagerten Gefahrenbegriffs“ zunächst ausschließlich von der subjektiven Einschätzung der ausführenden Beamtinnen und Beamten abhängig wäre. Wir haben daher gefordert, die Eingriffsvoraussetzungen mit ausreichend bestimmten und nachprüfbaren Kriterien auszufüllen.

Bereits im Vorfeld einer Gefahr sollte der Polizei mit dem Gesetzentwurf auch ein heimlicher Zugriff auf informationstechnische Systeme ermöglicht werden, um nach relevanten Informationen suchen, die Daten erheben und sie auswerten zu können – die sog. Online-Durchsuchung. Um dies zu ermöglichen, plante die Landesregierung das Aufbringen entsprechender staatlich entwickelter Infiltrierungssoftware und ggf. dafür erforderliche Maßnahmen zum Auffinden des Endgeräts sowie das Eindringen in Wohnräume zu erlauben. Gestattet werden sollte auch das Infiltrieren eines informationstechnischen Systems zum Ausleiten der laufenden Telekommunikation, wenn diese über das Internet (Voice over IP) mit Computern oder sonstigen elektronische Endgeräten verschlüsselt erfolgt – die sog. Quellen-TKÜ. Das Abhören an der Quelle, also bevor die Kommunikation mittels inzwischen verbreiteter kryptischer Verfahren nicht

mehr auslesbar wird, sollte die bestehenden Überwachungsbefugnisse der Polizei ergänzen.

Hinsichtlich beider Befugnisse haben wir erhebliche Zweifel geäußert, ob sie mit bestehenden technischen Verfahren verfassungskonform durchführbar sind. Die Schwere des Eingriffs in die Rechte Betroffener ergibt sich dadurch, dass die Sicherheitsbehörden aus einem informationstechnischen System, sobald es einmal infiltriert ist, weit mehr als die erwünschte laufende Telekommunikation und die gesuchten Daten entnehmen können. Vielfach sind dort eine unermessliche Anzahl persönlichkeitsrelevanter Informationen zu dem Betroffenen – bis hin zum absolut geschützten Kernbereich persönlicher Lebensführung – gespeichert, die bei einem Zugriff Einblick in wesentliche Teile der Lebensgestaltung sowie die Bildung von Persönlichkeitsprofilen erlauben.

Technischer Kern des Eingriffs wäre die erfolgreiche Manipulation des Rechners oder des mobilen Endgerätes. Dies gelingt meist nur unter Ausnutzung von Schwachstellen in den jeweiligen Systemen. Aus unserer Sicht ist es datenschutzrechtlich nicht zu rechtfertigen und rechtspolitisch fragwürdig, dass eine Sicherheitsbehörde des Staates aus Ermittlungsinteressen den Hersteller nicht auf bekannt gewordene Schwachstellen hinweist, sondern diese für polizeiliche Zwecke ausnutzt. Dies sollte auch im Hinblick darauf, dass Kriminelle diese Schwachstellen ebenfalls ausnutzen können, unbedingt vermieden werden. Wir bezweifelten zudem, dass fehlerhafte Funktionen der aufgebrachten Software oder eine missbräuchliche Nutzung der Daten durch Schadsoftware Dritter ausgeschlossen und eine nachteilige Veränderung des informationstechnischen Systems mit hinreichender Sicherheit verhindert werden kann. Der Gesetzentwurf gab zudem keine Hinweise darauf, wie eine Schadsoftware wieder entfernt werden könnte oder wie sich manipulierte Eingriffe auf die Gerichtsfestigkeit von Beweisen auswirken würden.

Als unverhältnismäßig haben wir die Einführung der elektronischen Aufenthaltsüberwachung zur Gefahrenabwehr mittels eines getragenen Senders – die sog. elektronische Fußfessel – kritisiert, noch dazu unter Anknüpfung an den vorverlagerten Gefahrenbegriff. Die Maßnahme, die bisher nur im Rahmen der Führungsaufsicht für Straftäterinnen und Straftäter in geringer Zahl erprobt wurde, sollte nicht ohne fundierte wissenschaftliche Auswertung ihrer Wirksamkeit auf einen neuen Personenkreis übertragen werden. Von der Geeig-

netheit der Maßnahme war der Gesetzgeber jedoch ohne weiteren Nachweis ausgegangen. Aufenthaltsdaten, die bis zu einem Zeitraum von drei Monaten erhoben werden dürfen, erlauben weitreichende Einblicke in das Privatleben der Trägerin oder des Trägers und stellen – auch wenn es sich um eine offen durchgeführte Maßnahme handelt – einen erheblichen Eingriff in das Persönlichkeitsrecht der oder des Betroffenen dar.

Wir haben uns zudem gegen eine grundsätzliche Ausweitung der Speicherfristen bei Bildaufnahmen an öffentlich zugänglichen Straßen und Plätzen von 48 Stunden auf zwei Wochen ausgesprochen. Zum einen, weil ihre Wirksamkeit angesichts der gegenwärtig videoüberwachten Bereiche in Brandenburg nicht erkennbar ist, und zum anderen, weil sie einer vorsorglichen Datenerhebung gleichkommt, die Unverdächtige unnötig lange erfasst. Sofern der Weg einer Täterin oder eines Täters vor einer gravierenden Tat oder danach auf der Flucht tatsächlich für präventive Zwecke ermittelt werden soll, regten wir eher an, anlassbezogene Verlängerungen der Speicherfrist im Einzelfall in Betracht zu ziehen.

Neue polizeiliche Befugnisse überaus kritisch

Kritisch sahen wir auch die im Gesetzentwurf enthaltene Befugnis, Polizeibeamtinnen und Polizeibeamten bei Personenkontrollen im öffentlichen Raum am Körper getragene Kameras – sog. Body-Cams– zwecks Bild- und Tonaufzeichnung zur Eigensicherung zu erlauben. Die Datenerhebung sollte durch die die Kamera tragende Person manuell aktiviert werden. Obwohl eine vergleichbare Befugnis beschränkt auf Datenerhebungen in Fahrzeugen der Polizei bereits seit Längerem besteht, enthielt die Gesetzesbegründung keine Hinweise auf tatsächliche Erfahrungen hinsichtlich der Wirksamkeit dieser Maßnahme. Die erweiterte Befugnis wurde zwar mit positiven Erfahrungen aus Pilotprojekten anderer Länderpolizeien im städtischen Raum pauschal als geeignet und erforderlich zur Deeskalation und Vermeidung von Angriffen angesehen. Wir vertraten den Standpunkt, dass die tatsächlichen Abschreckungseffekte einer Körperkamera in einer nach wissenschaftlichen Kriterien ausgerichteten Analyse geklärt werden sollten, bevor Bild- und Tonaufzeichnungen von Personen angefertigt werden dürfen. Insbesondere war nicht nachvollziehbar, wieso eine 60 Sekunden umfassende Vorabaufzeichnung (prerecording), die ein noch nicht gefährdendes Geschehen bei einer Kontrolle aufzeichnet und die Daten ständig

überschreibt, für den Zweck der Eigensicherung geeignet und erforderlich sein soll. Da Bild- und Tonaufzeichnungen im öffentlichen, grundsätzlich überwachungsfreien Raum einen nicht unerheblichen Eingriff in die Rechte betroffener Personen und ggf. auch unbeteiligter Dritter darstellen, haben wir empfohlen, diese Eingriffsbefugnis allenfalls befristet aufzunehmen und nach spätestens zwei Jahren zu evaluieren.

Der schließlich am 30. Oktober 2018 in den Landtag eingebrachte Regierungsentwurf (Zwölftes Gesetz zur Änderung des Brandenburgischen Polizeigesetzes, Landtags-Drucksache 6/9821) verzichtet auf die Eingriffsbefugnisse der elektronischen Aufenthaltsüberwachung zur Gefahrenabwehr und die Online-Durchsuchung. Der Eingriff in informationstechnische Systeme zum Zweck der Telekommunikationsüberwachung wurde jedoch beibehalten und darüber hinaus auch im Vorfeld einer konkreten Gefahr zugelassen. Die übrigen neuen oder erweiterten Eingriffsbefugnisse, zu denen wir uns kritisch geäußert hatten, blieben bis auf eine geringfügige Reduzierung einiger Speicherfristen unverändert. Auch der Empfehlung einer nur befristeten Aufnahme von Bild- und Tonaufzeichnungen zur Eigensicherung folgte die Landesregierung nicht. Es bleibt abzuwarten, ob und, wenn ja, welche Änderungen der Gesetzentwurf im Verlauf des parlamentarischen Verfahrens erfahren wird.

1.2 Brandenburgisches E-Government-Gesetz

Bereits mehrfach hatten wir in der Vergangenheit darauf hingewiesen, dass in der Verwaltung des Landes Brandenburg gesetzliche Vorgaben und strategische Entscheidungen zum E-Government, also zur Durchführung und Unterstützung des Regierungs- und Verwaltungshandelns mittels Informations- und Kommunikationstechnik, fehlen.[18] Auch der Landtag Brandenburg regte wiederholt entsprechende Aktivitäten an.[19] Mit Beschluss vom 15. November 2017 forderte er die Landesregierung auf, bis zum April 2018 den Entwurf eines Brandenburgischen E-Government-Gesetzes vorzulegen.[20]

18 siehe z. B. Tätigkeitsbericht 2014/2015, B 8.1, Tätigkeitsbericht 2012/2013, B 7.1

19 siehe z. B. Landtags-Drucksache 6/4528-B, 6/5185-B bzw. 6/5383-B

20 siehe Landtags-Drucksache 6/7616-B

Das federführende Ministerium des Innern und für Kommunales erarbeitete daraufhin einen Referentenentwurf des Gesetzes und leitete die inhaltliche Abstimmung in der Landesverwaltung und mit den kommunalen Spitzenverbänden ein. Auch unsere Behörde hatte frühzeitig Gelegenheit, hierzu Stellung zu nehmen. Unsere Hinweise und Anregungen wurden zumindest teilweise in das Dokument übernommen. Nachdem der Gesetzentwurf durch die Landesregierung in das Parlament eingebracht wurde[21] und das dortige Verfahren durchlaufen hatte, stimmten die Abgeordneten dem Gesetz im November 2018 endgültig zu.[22]

Grundsätzlich sehen wir die erfolgte Schaffung gesetzlicher Vorgaben zum E-Government positiv. So regelt die Vorschrift etwa, dass jede brandenburgische Behörde einen elektronischen Zugang für Bürgerinnen und Bürger bzw. für Unternehmen ermöglichen muss. Für den Versand elektronischer Dokumente durch Behörden sowie für den elektronischen Zugang zur Verwaltung sind geeignete Verschlüsselungsverfahren zu nutzen bzw. anzubieten. Verlangt ein Verwaltungsverfahren die Feststellung der Identität einer Person, kann dies mit Hilfe des elektronischen Personalausweises bzw. des elektronischen Aufenthaltstitels erfolgen. Behörden haben Informationen über ihre Dienstleistungen in elektronischer Form bereitzustellen, Formulare sollen digital angeboten werden. In Verwaltungsverfahren vorzulegende Nachweise können auch elektronisch eingereicht oder durch die zuständige Behörde mit Einwilligung der betroffenen Person elektronisch von der ausstellenden öffentlichen Stelle eingeholt werden. Öffentliche Auftraggeber müssen elektronische Rechnungen annehmen und verarbeiten können. Behörden der Landesverwaltung haben ab spätestens November 2024 ihre Akten grundsätzlich nur noch elektronisch zu führen, Verwaltungsabläufe sind zu optimieren.

Endlich Vorgaben zum E-Government

Unsere Unterstützung findet auch die Regelung, dass IT-Basiskomponenten wie z. B. ein elektronisches Identitätsmanagement (eID-Service), die virtuelle Poststelle des Landes, eine elektronische Bezahlplattform oder ein Landesserviceportal mit Servicekonten zentral vom Land bereitgestellt und von allen Landesbehörden gemeinsam

21 siehe Landtags-Drucksache 6/8728

22 Gesetz über die elektronische Verwaltung im Land Brandenburg vom 23. November 2018 (GVBl. I Nr. 28).

genutzt werden. Kommunen ist die kostenfreie Mitnutzung dieser IT-Basiskomponenten des Landes möglich. Entwickeln sie eigene IT-Basiskomponenten, kann deren (Mit-)Nutzung durch andere öffentliche Stellen des Landes vereinbart werden. Das Gesetz enthält auch Vorgaben zur Arbeit des Computersicherheits-Ereignis- und Reaktionsteams (CERT) bei der Abwehr von Gefahren für die Sicherheit der Informationstechnik des Landes, der Analyse von Sicherheitslücken und der Aufklärung von Sicherheitsvorfällen.

Viele Regelungen des Brandenburgischen E-Government-Gesetzes haben enge Bezüge zum Datenschutz und zur Informationssicherheit. Im Rahmen unserer Kontakte auf Arbeitsebene sowie der offiziellen Stellungnahmen gegenüber Landesregierung und Landtag haben wir sowohl die positiven Aspekte des Gesetzentwurfs hervorgehoben als auch u. a. die folgenden kritischen Hinweise gegeben:

- An mehreren Stellen des Gesetzes ist vorgesehen, einzelne Vorschriften durch Rechtsverordnungen zu konkretisieren und weiter auszugestalten. Dies betrifft z. B. Einzelheiten des elektronischen Verwaltungszugangs, der Verschlüsselung der Kommunikation, des elektronischen Rechnungsverkehrs, der elektronischen Aktenführung oder des Betriebs der IT-Basiskomponenten. Allerdings ist der Erlass der Verordnungen meist optional. Wir hatten mehr Verbindlichkeit angeregt, um divergierende und ggf. inkompatible Lösungen oder unnötige Mehrarbeit der Verantwortlichen zu verhindern. Die Landesregierung ist dieser Anregung nur teilweise gefolgt.

- Ursprünglich war geplant, dass der Brandenburgische IT-Dienstleister nicht nur für die Einrichtung und den Betrieb der IT-Basiskomponenten zuständig ist, sondern für alle diese Komponenten auch die Rolle des (alleinigen) Verantwortlichen im Sinne von Artikel 4 Nummer 7 Datenschutz-Grundverordnung (DS-GVO) übernimmt. Wir hatten hiermit erhebliche Schwierigkeiten, da der Dienstleister dann die volle datenschutzrechtliche Verantwortung auch für solche Verarbeitungen personenbezogener Daten zu übernehmen gehabt hätte, für die er dies faktisch gar nicht kann. Zu denken ist hier beispielsweise an die Sicherung der Rechtmäßigkeit der Verarbeitung gemäß Artikel 6 DS-GVO oder die Gewährleistung der Betroffenenrechte gemäß Artikel 12 ff. DS-GVO. Die Landesregierung hat diese Kritik insofern aufgenommen, als datenschutzrechtliche Verantwortlichkeiten

im Zusammenhang mit den IT-Basiskomponenten nun in einer Rechtsverordnung geklärt werden, die verbindlich zu erlassen ist.

- Hinsichtlich der Verarbeitung personenbezogener Daten beim CERT zur Analyse und Aufklärung von Sicherheitsvorfällen sieht das Gesetz eine frühzeitige Pseudonymisierung dieser Daten vor, soweit dies automatisiert möglich ist. Das ist zu befürworten. Darüber hinaus sollten jedoch nach Beendigung der Abwehrmaßnahmen betroffene Personen benachrichtigt werden, wenn sie bekannt sind oder das Pseudonym aufgelöst und die Personen reidentifiziert werden können sowie darüber hinaus keine überwiegenden schutzwürdigen Belange Dritter entgegenstehen. Obwohl die beabsichtigte Transparenz zu begrüßen ist, sahen wir in der zweiten Alternative einen Verstoß gegen die Datenschutz-Grundverordnung. Diese verpflichtet den Verantwortlichen nicht, zusätzliche Informationen zur Identifizierung betroffener Personen nur deshalb aufzubewahren, um die Einhaltung der Verordnung zu ermöglichen – hier die Erfüllung der Informationspflichten. Wenn eine Kenntnis der tatsächlichen Identität der betroffenen Person jedoch nicht für die Verarbeitungszwecke erforderlich ist, sind die Daten zu löschen. Die Landesregierung verzichtete daraufhin auf die genannte Alternative.

Zu kritisieren ist weiterhin, dass die Gesetzesinitiative nicht dazu genutzt wurde, die Themen Verwaltungstransparenz und Open Data durch eine Änderung des Akteneinsichts- und Informationszugangsgesetzes zu regeln.

Das Brandenburgische E-Government-Gesetz ist im November 2018 in Kraft getreten. Für einige Vorschriften gibt es eine längere Übergangsfrist (z. B. für den Umstieg auf eine komplett elektronische Aktenführung in der Landesverwaltung). Jetzt kommt es darauf an, die Konkretisierung einzelner Regelungen auch auf datenschutzrechtlichem Gebiet durch die vorgesehenen Rechtsverordnungen vorzunehmen. Darüber hinaus sind die geplanten IT-Basiskomponenten (falls noch nicht geschehen) einzurichten und in die routinemäßige Nutzung zu überführen. Es ist darauf hinzuweisen, dass der Brandenburgische IT-Dienstleister für den dauerhaften, ordnungsgemäßen, sicheren und datenschutzgerechten Betrieb dieser Komponenten die erforderlichen Ressourcen benötigt.

Und letztlich darf nicht vergessen werden, dass E-Government nicht ohne digitalisierte Verwaltungsverfahren funktioniert. Die Landesregierung hat mit der kürzlich veröffentlichten Zukunftsstrategie „Digitales Brandenburg“[23] zunächst konzeptionelle Vorarbeiten geleistet. Diese gilt es nun, praktisch umzusetzen.

1.3 Heilberufsgesetz

Das Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie legte uns bereits Ende 2017 den Entwurf eines Gesetzes zur Änderung des Heilberufsgesetzes zur Stellungnahme vor. Im Gesetzentwurf waren zunächst im Wesentlichen nur sprachliche Anpassungen an die ab Ende Mai 2018 geltende Datenschutz-Grundverordnung vorgesehen.

Inhaltlich regten wir in unserer Stellungnahme an, die im Entwurf an verschiedenen Stellen vorgesehenen Datenschutzregelungen in einer Vorschrift zusammenzufassen und insgesamt eine Anpassung an das Europarecht, die über das Auswechseln einzelner Begriffe hinausging, vorzunehmen. Wichtig war uns außerdem, dass die Verarbeitung besonderer Kategorien personenbezogener Daten wie Gesundheitsdaten bedacht wird (z. B. für Datenverarbeitungen durch Fürsorgeeinrichtungen der Kammern und Versorgungswerke). Beiden Anregungen hat das Ministerium Rechnung getragen.

Bereits in unserem letzten Tätigkeitsbericht hatten wir angeregt, berufsrechtliche Bestimmungen zur Durchbrechung der Schweigepflicht sowie Voraussetzungen und Grenzen der Inanspruchnahme von Dienstleistern durch Heilberufsangehörige landesrechtlich zu regeln. Unser Vorschlag, eine entsprechende Befugnisnorm in das Heilberufsgesetz aufzunehmen, lehnte das Ministerium ab. Es signalisierte uns, dass sich u. a. die Bundesärztekammer mit dieser Thematik befasst, da sowohl ein Interesse an der Erhaltung der Satzungsautonomie der Heilberufskammern als auch an bundesweit weitestgehend einheitlichen Berufsausübungsregelungen besteht.

Das Gesetz trat Ende Juni 2018 in Kraft.[24]

---

23 https://digitalesbb.de

24 Gesetz zur Änderung des Heilberufsgesetzes und weiterer Gesetze vom 29. Juni 2018 (GVBl I Nr. 14).

1.4 Brandenburgisches Krankenhausentwicklungsgesetz

Den Entwurf für ein Zweites Gesetz zur Änderung des Brandenburgischen Krankenhausentwicklungsgesetzes, der u. a. eine Anpassung des Datenschutzteils an die Datenschutz-Grundverordnung beinhaltet, hat uns das Ministerium für Arbeit, Gesundheit, Soziales, Frauen und Familie Mitte April 2018 vorgelegt.

Uns war zunächst wichtig zu klären, welche landesrechtlichen Verarbeitungsvorschriften im Krankenhausrecht durch die Datenschutz-Grundverordnung überflüssig geworden sind und welche Vorgaben des Europarechts bei der nationalen Regelung über die Verarbeitung von Daten besonderer Kategorien (insbesondere Gesundheitsdaten) im Einzelfall zu beachten sind. Im Ergebnis wurde beispielsweise die Vorschrift über die (mutmaßliche) Einwilligung gestrichen, da die Datenschutz-Grundverordnung diese Fälle bereits regelt. Bei den in der Datenschutz-Grundverordnung ebenfalls normierten Auskunftsrechten der betroffenen Personen fiel hingegen die Entscheidung, die landesrechtliche Regelung beizubehalten, da deren Vorgaben und Einschränkungen speziell auf die besondere Situation von Patientinnen und Patienten Rücksicht nehmen.

Ein wichtiger Aspekt ist die Vorschrift über dezentrale klinische Krankheitsregister. Wir haben uns dafür eingesetzt, dass im Gesetz konkrete Schutzmaßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorgegeben werden, indem die Genehmigung solcher Register an die Einhaltung bestimmter Auflagen und Bedingungen zu knüpfen ist. Die Auswahl solcher Maßnahmen darf nicht einer Entscheidung der Einrichtung selbst überlassen bleiben. Stark gemacht haben wir uns auch für ein Widerspruchsrecht der Patientinnen und Patienten gegen die Offenlegung ihrer Daten gegenüber dem Register.

Das Gesetzgebungsverfahren war zum Ende des Berichtszeitraums noch nicht abgeschlossen. Ob unsere Vorschläge und Empfehlungen aufgegriffen werden, bleibt abzuwarten.

1.5 Gesetze zu Landes- und Kommunalwahlen

Mit Anpassung des bereichsspezifischen Landesrechts an die Datenschutz-Grundverordnung sollte neben anderen Änderungen sowohl im Brandenburgischen Landeswahlgesetz als auch im Brandenburgi-

schen Kommunalwahlgesetz eine Rechtsgrundlage für die Veröffentlichung von Bewerberdaten im Internet geschaffen werden. Zu begrüßen war, dass die Privatanschriften der Wahlbewerberinnen und Wahlbewerber von einer Internet-Veröffentlichung ausgenommen und konkret benannte Löschfristen für die veröffentlichten Daten geregelt werden sollten.

Die Landesbeauftragte sah jedoch einen Widerspruch darin, dass zwar die originären Internetveröffentlichungen der Wahlleiterinnen und Wahlleiter nach bestimmten Fristen zu löschen sind, die Angaben in gedruckten Amtsblättern, Tageszeitungen und sonstigen Druckwerken jedoch selbst dann nicht, wenn sie online verfügbar sind. Dadurch werden die Privatanschriften der Kandidatinnen und Kandidaten, die der Gesetzgeber von einer Online-Veröffentlichung auszunehmen beabsichtigt, weiterhin veröffentlicht.

Zwar hielt die Landesbeauftragte ein zeithistorisches Interesse der Öffentlichkeit, zeitlich unbegrenzt Zugang zu Namen von Kandidatinnen und Kandidaten zu haben, durchaus für gegeben. Allerdings erschloss sich ihr nicht, weshalb die Veröffentlichung ihrer genauen Adressen erforderlich sein soll. Dies gilt insbesondere für die Angaben zu unterlegenen, inzwischen ins Privatleben zurückgekehrten Bewerberinnen und Bewerber.

Keine Veröffentlichung von Privatadressen der Wahlbewerberinnen und -bewerber

Aus früheren Beschwerden war uns bekannt, dass durch die Angabe der Adressen der Kandidatinnen und Kandidaten im Internet handfeste Nachteile entstehen können. In einem Fall wurden die Daten durch politische Gegnerinnen und Gegner missbraucht, um Betroffene zu belästigen. Auch hatten wir Kenntnis von Fällen, in denen sich Interessierte, zu deren Gunsten wegen früherer Übergriffe eine Auskunftssperre im Melderegister eingetragen war, daran gehindert sahen, am politischen Prozess überhaupt teilzunehmen, wenn ihre Anschrift im Internet veröffentlicht wird. Auch der Missbrauch von Veröffentlichungen zu strafrechtlich relevanten Zwecken im Internet ist keine Seltenheit. Solche Risiken überwiegen den nur äußerst geringen Erkenntnisgewinn, den die Öffentlichkeit aus der Veröffentlichung der genauen Wohnanschrift ziehen kann, bei Weitem.

Schließlich ist die Eingriffstiefe einer Internet-Veröffentlichung hinsichtlich der Reichweite und der Einfachheit der Informationsbeschaffung auch ungleich gewichtiger als eine Veröffentlichung in Papierform, sodass aus der Unbedenklichkeit der Veröffentlichung in Papierform nicht auf die Verhältnismäßigkeit der Online-Veröffentlichung geschlossen werden kann.

Aus diesen Gründen plädierte die Landesbeauftragte dafür, von vornherein auf die Angabe der Adressen der Betroffenen in den online zu veröffentlichenden Wahlunterlagen zu verzichten, mindestens aber sämtliche Online-Veröffentlichungen, mithin auch die Online-Versionen der Druckwerke, denselben Voraussetzungen und Löschfristen zu unterwerfen.

Diese Vorschläge konnten in den damaligen Beratungen zum Artikelgesetz nicht mehr berücksichtigt werden. Mit einer Entschließung vom 25. April 2018 (Landtags-Drucksache 6/8634) reagierte der Landtag jedoch auf entsprechende Anregungen der Landesbeauftragten in der Anhörung vor dem zuständigen Ausschuss. Er forderte die Landesregierung auf, „die Brandenburgische Landeswahlverordnung und die Brandenburgische Kommunalwahlverordnung dahingehend zu ändern, dass künftig anstelle der Wohnanschriften ausschließlich die Wohnorte der Wahlbewerberinnen und Wahlbewerber in den Verkündungsblättern des Landes und der Kommunen öffentlich bekannt gemacht werden."

In der Folge wurden wir an entsprechenden Vorhaben des zuständigen Ministeriums, die in der Entschließung genannten Vorschriften zu ändern, beteiligt. Eine abschließende Abstimmung steht noch aus.

1.6 Übertragung der Sitzungen von Landtagsausschüssen per Livestream

Die Ausschüsse des Landtages Brandenburg tagen grundsätzlich öffentlich. Die Öffentlichkeit, insbesondere Pressevertreterinnen und Pressevertreter sowie andere interessierte Zuschauerinnen und Zuschauer, haben Zutritt zu den Sitzungen. Nicht alle haben aber die Möglichkeit, den Landtag persönlich aufzusuchen. Um daher auch nicht anwesenden Bürgerinnen und Bürgern die Gelegenheit zu geben, die Ausschusssitzungen zu verfolgen, hat der Hauptausschuss des Landtages beschlossen, die öffentlichen Sitzungen von drei Fachausschüssen – zunächst im Rahmen einer Pilotphase – live

im Internet zu übertragen. Auf diesen Umstand soll auf den an den Zugängen zum Sitzungsraum befindlichen Bildschirmen durch Einblendung eines Laufbands am unteren Bildschirmrand hingewiesen werden. Auch enthalten die Einladungen zur jeweiligen Ausschusssitzung und die Schreiben an Anzuhörende Hinweise auf die Liveübertragung.

Da von einigen Betroffenen und auch von Abgeordneten des Landtages geltend gemacht wurde, dass durch die Liveübertragung der Sitzungen die Persönlichkeitsrechte von Anwesenden verletzt werden könnten, bat der Hauptausschuss die Landesbeauftragte um ihre fachliche Einschätzung.

Die Verarbeitung personenbezogener Daten im Rahmen des parlamentarischen Verfahrens fällt nicht in den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung. Das Parlament unterliegt auch nicht der Aufsicht durch die Landesbeauftragte (§ 2 Absatz 2 Brandenburgisches Datenschutzgesetz). Dementsprechend hat die Landesbeauftragte nur eine gutachterliche Stellungnahme abgegeben und Empfehlungen ausgesprochen.

Durch die Übertragung per Livestream werden personenbezogene Daten der in einer Ausschusssitzung Anwesenden erhoben, gespeichert und an eine unbegrenzte Zahl von Dritten übermittelt. Damit wird in erheblichem Umfang in das Grundrecht auf Datenschutz eingegriffen. Im Vergleich zu den bisher üblichen schriftlichen Protokollen hat diese Form der Datenverarbeitung eine wesentlich höhere Eingriffsintensität. Sie zeigt die Beteiligten in Bild und Ton und dadurch beispielsweise auch ihr Aussehen und ihr nonverbales Verhalten einschließlich Habitus, Gestik und Mimik. Darüber hinaus werden Anwesende sichtbar, die mangels aktiver Beteiligung im schriftlichen Protokoll nicht erscheinen würden. Dies sind nicht nur Journalistinnen und Journalisten, sondern auch die Zuschauerinnen und Zuschauer sowie die anwesenden Beschäftigten der Fraktionen, der Parlaments- und der Ministerialverwaltung. Nicht ausgeschlossen ist ferner, dass Namen und weitere Informationen über nicht anwesende Personen offenbart werden, die im schriftlichen Protokoll anonymisiert werden können, in der Liveübertragung aber offenkundig werden. Auch deren Recht auf Datenschutz ist also tangiert. Die Eingriffsintensität erhöht sich noch dadurch, dass die erhobenen Bild- und Tonaufnahmen durch die Liveübertragung nicht nur der

anwesenden Öffentlichkeit, sondern einer unbegrenzten Zahl von Menschen zur Verfügung gestellt werden.

Dem Grundrecht der Beteiligten auf Datenschutz steht aber der aus dem verfassungsrechtlichen Demokratieprinzip abgeleitete Grundsatz der Öffentlichkeit der staatlichen Beratungs- und Entscheidungsprozesse gegenüber. Die Öffentlichkeit der Ausschussberatungen macht den parlamentarischen Willensbildungsprozess für die Bürgerinnen und Bürger nachvollziehbar. Sie erhalten dadurch die für ihre politische Willensbildung erforderlichen Informationen, die sich letztlich auch in Wahlen ausdrückt. Eine transparente parlamentarische Arbeit ist mithin in einer Demokratie ein hohes Gut, dessen konkrete Ausgestaltung sich im Laufe der Zeit aufgrund der digitalen Entwicklung deutlich gewandelt hat.

Beide Verfassungsgebote, das Grundrecht auf Datenschutz und das aus dem Demokratieprinzip hergeleitete Öffentlichkeitsprinzip, müssen so weit wie möglich verwirklicht und gleichzeitig so weit wie möglich miteinander in Einklang gebracht werden. Die Landesbeauftragte hat deshalb verschiedene technische und organisatorische Maßnahmen vorgeschlagen, durch die der Grundrechtseingriff bestenfalls vermieden, zumindest aber eingeschränkt werden könnte, ohne dass der Zweck der Liveübertragung wesentlich eingeschränkt würde. Je nach betroffener Personengruppe fielen die Empfehlungen und Hinweise unterschiedlich aus.

Liveübertragung datenschutzgerecht gestalten

Beispielsweise hat die Landesbeauftragte vorgeschlagen, die an die Mikrofone gekoppelten Schwenkkameras so einzurichten, dass sie nur das gerade redende Ausschussmitglied oder die Anzuhörende oder den Anzuhörenden erfasst, nicht aber etwa daneben sitzende Mitarbeiterinnen und Mitarbeiter oder sonstige Dritte. Bei den Abgeordneten, den Regierungsmitgliedern wie auch den Beschäftigten der Fraktionen und des Landtages sah die Landesbeauftragte es als den entsprechenden Funktionen immanent an, dass sie in der Öffentlichkeit stehen. Die Mitarbeiterinnen und Mitarbeiter sollten allerdings, gerade auch bei Neueinstellungen, über die Art und Weise der Verarbeitung ihrer personenbezogenen Daten informiert werden. Auch sollte ihre Anwesenheit auf das notwendige Maß beschränkt werden.

Da die Teilnahme von Anzuhörenden in der Regel freiwillig ist, hat der Ausschuss bei Ablehnung eines Liveauftritts durch eine eingeladene Person die Möglichkeit, die Liveübertragung zu unterbrechen oder auf die anzuhörende Person zu verzichten.

Hinsichtlich der Grundrechte der anwesenden Zuschauerinnen und Zuschauer hielt die Landesbeauftragte den bisher geplanten Hinweis auf den Bildschirmen vor den Sitzungsräumen für nicht ausreichend. Sie regte an, weitergehende Informationen über die Tatsache der Filmaufnahmen und über Art, Zweck und Umfang ihrer Nutzung durch Aushang oder durch Informationsblätter im Sitzungssaal zur Verfügung zu stellen. Nur bei Kenntnis dieser Informationen können sich die Zuschauerinnen und Zuschauer frei für oder gegen eine Teilnahme an der Sitzung entscheiden und, sofern sie bleiben, damit konkludent in die Liveübertragung und eine damit eventuell verbundene Verarbeitung ihrer Daten einwilligen.

Schließlich machte die Landesbeauftragte auf die besondere Verantwortung der Ausschussvorsitzenden aufmerksam. Denn in Fällen, in denen über nicht anwesende Personen gesprochen wird und deren personenbezogene Daten offengelegt werden, sollten die Vorsitzenden unverzüglich eingreifen, indem sie etwa die Rednerin oder den Redner ermahnen oder das Mikrofon ausschalten.

Der Hauptausschuss hat sich letztlich dafür entschieden, das Pilotprojekt „Livestream-Übertragung öffentlicher Ausschusssitzungen im Landtag Brandenburg“ mit zwei Fachausschüssen bis zum Ende der 6. Wahlperiode fortzuführen. Den anderen Ausschüssen wurde es freigestellt, bei hohem medialen Interesse die jeweilige Sitzung ebenfalls live im Internet zu übertragen. Die endgültige Entscheidung über eine generelle Liveübertragung öffentlicher Ausschusssitzungen im Internet wird dem Landtag der 7. Wahlperiode überlassen.

2 Projekte

2.1 Herzinfarktregister Brandenburg

Die Medizinische Hochschule Brandenburg und das Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie baten uns, das Datenschutzkonzept für ein Herzinfarktregister in drei brandenburgischen Modellregionen zu prüfen. Ziel des Projektes ist, die Ursachen für die überdurchschnittlich hohe Herzinfarktsterblichkeit in

Brandenburg zu untersuchen und entsprechende Präventionsmaßnahmen abzuleiten.

Das Registerzentrum sollte als eigenverantwortliche Außenstelle der Hochschule in den Räumlichkeiten des Städtischen Klinikums Brandenburg untergebracht werden. In kooperierenden Krankenhäusern waren sog. Erhebungszentren angedacht. Ausgewählte Personen der Hochschule („Study Nurses“) sollten regelmäßigen Zugang zu den betroffenen Patientenakten haben und die für das Herzinfarktregister erforderlichen Daten erheben.

Für die Übermittlung von Kontaktdaten der Patientinnen und Patienten liegt ein gesetzlicher Erlaubnistatbestand vor, der es den Krankenhäusern zur Durchführung des Forschungsprojekts erlaubt, diese Daten ohne Einwilligung und Kenntnis der Betroffenen an die Außenstelle der Hochschule weiterzuleiten. Die Befragungen der Patientinnen oder Patienten sind jedoch für sie freiwillig. Von der zunächst geplanten fernmündlichen Einwilligungserklärung der betroffenen Personen haben wir wegen der Gefahr eines Überrumpelungseffekts abgeraten. Auch die Komplexität und der Umfang der Erklärung und der dazu gehörigen Aufklärung sprachen für ein schriftliches Einverständnis. Der Umstand, dass der Widerruf der Einwilligungserklärung nur schriftlich erfolgen sollte, war ein weiteres Argument für unsere Auffassung. Außerdem ist bei einer rein telefonischen Einwilligungserklärung eine zweifelsfreie Authentifizierung von Betroffenen problematisch. Gerade vor dem Hintergrund der Verarbeitung sensitiver Gesundheitsdaten ist daher eine schriftliche Einwilligung wesentlich.

Forschungen im Register sollten mit pseudonymisierten Daten vorgenommen werden. Im Laufe der Beratung ergab sich jedoch, dass keine unabhängige Vertrauensstelle existiert, die eine Pseudonymisierung gewährleisten könnte. Wir wiesen auch darauf hin, dass Art und Menge der Angaben nicht in jedem Einzelfall eine Personenbeziehbarkeit der Daten ausschließen.

In Bezug auf die Sicherheit der Datenverarbeitung betonten wir, dass das Herzinfarktregister sowie alle Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreifen müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Um dies nachzuweisen, sind eine Risikoanalyse und ein IT-Sicherheitskonzept für das Registerzentrum, die Erhebungszentren und die

beteiligten Auftragsverarbeiter erforderlich. Aufgrund des voraussichtlich hohen Risikos der Verarbeitung wird außerdem eine Datenschutz-Folgenabschätzung notwendig sein.

2.2 Hinweise des Bildungsministeriums zur Umsetzung der Datenschutz-Grundverordnung in Schulen

Auch Schulen stellt das Wirksamwerden der Datenschutz-Grundverordnung vor große Herausforderungen. Obwohl sich tatsächlich datenschutzrechtlich wenig geändert hat, sind dennoch viele Schulleitungen verunsichert, wie sie den vermeintlich neuen Anforderungen an einen sensiblen Umgang mit den Daten von Lehrkräften, der Schülerinnen und Schüler sowie deren Erziehungsberechtigten nachkommen können. Fragen stellten sich zum Beispiel hinsichtlich der Benennung einer oder eines Datenschutzbeauftragten, der Erstellung eines Datenschutzkonzepts, der Aufteilung von Verantwortlichkeiten, der Sensibilisierung der Lehrkräfte und der Auswahl und Umsetzung technisch-organisatorischer Maßnahmen in der täglichen Schulpraxis. Möglicherweise ist eine gewisse Vernachlässigung des Datenschutzes in der Vergangenheit mitursächlich für diese unnötige allgemeine Verunsicherung.

Eine umfassende Handlungsempfehlung des Ministeriums für Bildung, Jugend und Sport, die sich an Schulen in öffentlicher Trägerschaft richtet, nimmt diese und ähnliche Fragen auf. Sie liefert Erläuterungen zu den Rechtsgrundlagen, enthält Muster und Formulare für ausgewählte Datenverarbeitungen (wie beispielsweise Einwilligungserklärungen für Fotoaufnahmen) und beantwortet häufig gestellte Fragen. Bereits frühzeitig hatten wir die Gelegenheit, an der Erstellung der Handlungsempfehlung beratend mitzuwirken und datenschutzrechtliche Hinweise zu geben. Die Zusammenarbeit mit dem Ministerium war sehr konstruktiv.

Ziel der Handreichung ist es, die am Schulalltag Beteiligten mit den Vorgaben der Datenschutz-Grundverordnung vertraut zu machen und ihnen Hilfestellung in der täglichen, praktischen Umsetzung zu geben. Das Ministerium beabsichtigt, die „Hinweise zur Datenschutz-Grundverordnung in den Schulen in öffentlicher Trägerschaft“ zum 2. Schulhalbjahr 2018/2019 herauszugeben.

3 Jahrestreffen mit den behördlichen Datenschutzbeauftragten

Schon traditionell haben wir im Berichtszeitraum wieder die Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Kommunen zu einer ganztägigen Beratung in unsere Dienststelle eingeladen. Es handelte sich um die mittlerweile 15. Veranstaltung dieser Art.

Wie bereits zuvor haben die Datenschutzbeauftragten eine Vielfalt an Themen eingebracht. Sie entstammten ihrer täglichen Arbeit. Die Beschäftigten unserer Dienststelle gaben Hilfestellungen zur Auslegung und Anwendung von Rechtsnormen. Gemeinsam besprachen wir verschiedene Praxisprobleme und erarbeiteten Hinweise zur bestmöglichen Umsetzung. Die Beratungen der Datenschutzbeauftragten haben sich nach unserer Auffassung für alle Beteiligten bewährt. Die Aufsichtsbehörde erörtert ihre Rechtsauffassung gemeinsam mit den Vertreterinnen und Vertreter aus den Kommunen und gewinnt einen wichtigen Einblick in die tägliche Behördenpraxis; die Datenschutzbeauftragten profitieren zudem von den Erfahrungen der Kolleginnen und Kollegen in anderen Verwaltungen.

Inhaltlich stand das Treffen ganz im Zeichen der neuen Vorschriften der Datenschutz-Grundverordnung (DS-GVO). Schwerpunkte waren z. B. die Zweckänderung bei der Datenverarbeitung, insbesondere hinsichtlich der Übermittlung von Daten an andere Stellen, die Melde- bzw. Benachrichtigungspflicht bei Datenschutzverletzungen nach Artikel 33 und 34 DS-GVO, der Umgang mit Datenträgern als Fundsachen, die Nutzung von WhatsApp auf dienstlichen Geräten, Aufbewahrungs- und Löschfristen, Anforderungen an den Betrieb behördlicher Webseiten und die Erfüllung der Informationspflichten nach Artikel 12 ff. DS-GVO bei Vollstreckungen, bei der Verwaltungstätigkeit von Ordnungsbehörden oder bei Telefonaten.

Kapitel VI
Dienststelle

VI Dienststelle

1 Öffentlichkeitsarbeit

Die Einführung des neuen Datenschutzrechts stellte unsere Dienststelle im Berichtszeitraum vor die Herausforderung, alle bisherigen Publikationen daraufhin zu überprüfen, ob sie weiterhin für die Öffentlichkeitsarbeit eingesetzt werden können. Im Ergebnis haben wir zahlreiche Veröffentlichungen überarbeitet und das Internetangebot weitgehend der neuen Rechtslage angepasst.

Sehr gefragt sind weiterhin die wichtigsten Rechtstexte zu Datenschutz und Informationsfreiheit; wir haben deshalb die Datenschutz-Grundverordnung als Broschüre neu herausgegeben. Sie enthält neben dem Verordnungstext die für das Verständnis der Regelungen wichtigen Erwägungsgründe. Neu gedruckt liegen außerdem das Bundesdatenschutzgesetz, das Brandenburgische Datenschutzgesetz und das Akteneinsichts- und Informationszugangsgesetz vor. Alle drei Rechtsgrundlagen hatte der Gesetzgeber zuvor an die neuen europarechtlichen Regelungen angepasst.

Dem enormen Beratungsbedarf, der sich aus dem Wirksamwerden der Datenschutz-Grundverordnung ergab, sind wir unter anderem durch Handreichungen nachgekommen, die wir in unserem Internetangebot zur Verfügung stellen. In einem Papier erläutern wir die Informationspflichten, die Verantwortliche gegenüber den betroffenen Personen haben, in einem weiteren gehen wir auf die gerade in der Einführungsphase häufig gestellten Fragen zur Verarbeitung personenbezogener Daten bei Fotografien ein. Auch den Datenschutz im Verein, die Rechte der betroffenen Person sowie die Voraussetzungen, unter denen Verantwortliche eine oder einen Datenschutzbeauftragten benennen müssen, erläutern wir in jeweils separaten Handreichungen. Fragen der Zulässigkeit einer Videoüberwachung in der Nachbarschaft – ein „Dauerbrenner“ in unserer Beratungspraxis – beantwortet ein Faltblatt, das wir aktualisiert haben.

Ebenso wie dieser Tätigkeitsbericht erscheinen künftig auch alle weiteren Publikationen der Landesbeauftragten in einem neuen, zeitgemäßen Design. Dieses geht zurück auf Gestaltungsrichtlinien, die wir im Berichtszeitraum haben erarbeiten lassen. Das neue Erscheinungsbild der Landesbeauftragten zeichnet sich durch eine klare

Formensprache aus und kommt auch beim regulären Schriftverkehr sowie anderen öffentlichkeitswirksamen Auftritten unserer Behörde zum Einsatz.

Bereits vor dem Wirksamwerden der neuen Rechtslage haben wir – in Zusammenarbeit mit anderen Datenschutzaufsichtsbehörden – ein Papier mit Hilfestellungen für kleine und mittlere Unternehmen bei der Umsetzung der Datenschutz-Grundverordnung angeboten. In 19 Kurzpapieren, die wir ebenfalls im Internet zur Verfügung stellen, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder unter Mitwirkung der Landesbeauftragten eine erste Orientierung für den praktischen Vollzug der wichtigsten Regelungen der Datenschutz-Grundverordnung erarbeitet. Neben Hinweisen der Konferenz zu den verpflichtenden Verzeichnissen von Verarbeitungstätigkeiten halten wir hierfür Muster zum Herunterladen bereit, mittels derer die Verantwortlichen bzw. Auftragsverarbeiter eine strukturierte Datenschutzdokumentation erreichen können.

Desgleichen skizzieren wir in einer Formulierungshilfe für einen Auftragsverarbeitungsvertrag, wie die Auslagerung klassischer IT-Dienstleistungen auf eine datenschutzgerechte Grundlage gestellt werden kann. Jeweils für den öffentlichen und den nicht öffentlichen Bereich bieten wir Listen von Verarbeitungsvorgängen an, für die eine Datenschutz-Folgenabschätzung durchzuführen ist. Von großer Bedeutung sind auch die Leitlinien des Europäischen Datenschutzausschusses, die wir ebenfalls in unserem Internetangebot zur Verfügung stellen.

Unter Mitwirkung der Landesbeauftragten gibt die Datenschutzkonferenz Orientierungshilfen heraus, die ausführliche, fachbezogene Hilfestellungen enthalten. Viele dieser Papiere stammen aus der Zeit vor dem Wirksamwerden der Datenschutz-Grundverordnung und müssen noch überarbeitet werden. Im Berichtszeitraum hat die Konferenz fünf neue Orientierungshilfen herausgegeben, und zwar zu Online-Lernplattformen im Schulunterricht, zum Standard-Datenschutzmodell, zur Einholung von Selbstauskünften bei Mietinteressenten, zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung sowie zu Whistleblowing-Hotlines.

Auf einer neuen, zentralen Informationsplattform (www.datenschutzkonferenz-online.de) stellt die Konferenz der unabhängigen

Datenschutzaufsichtsbehörden des Bundes und der Länder aktuelle Entschließungen, Beschlüsse, Orientierungshilfen, Kurzpapiere und Protokolle zur Verfügung. Auf dieser Homepage der Datenschutzkonferenz finden sich auch Links zu den Aufsichtsbehörden, den verschiedenen Landesdatenschutzgesetzen sowie den europäischen Datenschutzgremien. Die Plattform wird vom Bayerischen Landesamt für Datenschutzaufsicht unter finanzieller Beteiligung der Konferenzmitglieder, also auch der Landesbeauftragten, betrieben, und ist auch von unserem Angebot aus erreichbar.

In unserem eigenen Internetangebot halten wir ein Formular zur Mitteilung der Kontaktdaten der oder des Datenschutzbeauftragten an die Aufsichtsbehörde bereit. Verantwortliche können ihren Mitteilungspflichten uns gegenüber dadurch ohne großen Aufwand nachkommen. Für die Übertragung der Daten ist grundsätzlich eine Transportverschlüsselung vorgesehen. Wie von der Datenschutz-Grundverordnung vorgesehen, stellen wir auch ein Beschwerdeformular zur Verfügung, das gleichermaßen online ausgefüllt und versandt werden kann. Abhängig von der verwendeten Technik werden die Beschwerdedaten auf dem Wege einer Ende-zu-Ende-Verschlüsselung an uns übertragen.

Vielfältige Informationen zum neuen Recht

Insgesamt brachte die neue Rechtslage eine umfangreiche Neuordnung der Inhalte unseres Internetangebots mit sich. Die ebenfalls erforderliche Neugestaltung des Internetauftritts konnte aus Kapazitätsgründen im Berichtsjahr nicht mehr erfolgen.

Als Mitglied der Datenschutzkonferenz war die Landesbeauftragte an der zentralen Veranstaltung anlässlich des zwölften Europäischen Datenschutztages am 29. Januar 2018 in Berlin beteiligt. Die Veranstaltung wird traditionell durch den Vorsitz in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder aus dem Vorjahr organisiert – dies war die Landesbeauftragte für den Datenschutz Niedersachsen. Die Teilnehmerinnen und Teilnehmer der Tagung diskutierten die Frage „Souveränität in der digitalen Welt – eine Illusion?“

Mit einem eigenen Informationszelt nahm die Landesbeauftragte am 25. und 26. August 2018 am Brandenburg-Tag in Wittenberge teil. Wir präsentierten in der Prignitzstadt anhand eines Modells aktu-

elle technische Möglichkeiten der Gesichtserkennung, erläuterten die Grenzen der Zulässigkeit einer Videoüberwachung in der Nachbarschaft, thematisierten die Videoüberwachung zusätzlich in einem Preisrätsel und standen zwei Tage lang für Fragen und Gespräche zur Verfügung, in denen es vor allem um die neue Rechtslage zum Datenschutz ging.

2 Pressearbeit

Im Berichtsjahr drehte sich die aktive Pressearbeit im Wesentlichen um die neue Rechtslage im Datenschutz, die mit dem 25. Mai 2018 wirksam wurde. Die Landesbeauftragte informierte beispielsweise über die umfangreiche Schulungstätigkeit für Unternehmen und Verwaltungen, die wir in der ersten Jahreshälfte in Kooperation mit Wirtschaftsverbänden, Industrie- und Handelskammern, Bildungs- und Sozialeinrichtungen, Ministerien sowie Landkreisen und anderen Kommunalverwaltungen durchgeführt haben. Ihren Tätigkeitsbericht 2016/2017 stellte die Landesbeauftragte am 18. April 2018 auf einer Pressekonferenz im Landtag Brandenburg vor. Sie gab gleichzeitig eine umfangreiche Presseinformation mit einer Zusammenfassung der wichtigsten Beiträge des Berichts heraus. Am Vortag der Einführung der Datenschutz-Grundverordnung haben wir auf die unmittelbar bevorstehenden Änderungen sowie auf die Bedeutung des gleichzeitig in Kraft getretenen, neu gefassten Brandenburgischen Datenschutzgesetzes für öffentliche und des Bundesdatenschutzgesetzes für private Stellen hingewiesen.

Im Juni nahmen wir ein Urteil des Europäischen Gerichtshofs sowie eine darauf basierende Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zum Anlass, Verantwortliche auf die datenschutzrechtliche Mitverantwortung beim Betrieb von Facebook-Fanpages aufmerksam zu machen. Auf die Präsenz der Landesbeauftragten auf dem Brandenburg-Tag am 25. und 26. August 2018 in Wittenberge haben wir in einer Presseinformation kurz vor dem Landesfest hingewiesen. Die durch das neue Datenschutzrecht verschärfte Verpflichtung der verantwortlichen Stellen, die Aufsichtsbehörde im Falle eines Verstoßes gegen den Datenschutz zu informieren, war im Oktober Gegenstand einer ausführlicheren Presseinformation. Darin haben wir eine erste Zwischenbilanz zu den im Vergleich zu den Vorjahren wesentlich häufigeren Meldungen solcher Datenpannen gezogen sowie Einzelheiten der Meldepflicht erläutert.

Ebenfalls im Oktober wurden bundesweit zahlreiche Gewerbetreibende von dem Werbeangebot eines vorgeblich in Brandenburg ansässigen Unternehmens überrascht. Es forderte dazu auf, ein Formular auszufüllen und zu unterschreiben, um Anforderungen der Datenschutz-Grundverordnung nachzukommen, die es in Wirklichkeit gar nicht gibt. Wer dies tat, unterschrieb vielmehr einen Vertrag und nahm ein kostenpflichtiges „Leistungsangebot Basisdatenschutz“ an. In ihrer Presseinformation empfahl die Landesbeauftragte, gewerbliche Unterstützungsangebote zur Umsetzung datenschutzrechtlicher Anforderungen genau zu prüfen, und wies auf unsere kostenfreien Informationsangebote hin.

Es überraschte nicht, dass sich im Berichtsjahr auch die Anfragen der Journalistinnen und Journalisten auf die Einführung der Datenschutz-Grundverordnung konzentrierten.[25] Neben den neuen Rechten der Bürgerinnen und Bürger sowie den Pflichten für die Unternehmen und Behörden stand die Aufsichtstätigkeit der Landesbeauftragten im Zentrum dieser Anfragen. Von Interesse war zunächst, ob die Datenschutzaufsichtsbehörde ausreichende personelle Kapazitäten hat, um den erweiterten Aufgaben aus der Datenschutz-Grundverordnung nachzukommen, und wie sie dies konkret zu tun beabsichtigt. Gerade in den Wochen um den 25. Mai 2018 war die Verunsicherung über die Auswirkungen der neuen Rechtslage groß, was sich in den Presseanfragen widerspiegelte: Wird die Landesbeauftragte zum Stichtag hart durchgreifen und jeden Verstoß gleich sanktionieren? Bereits wenige Wochen später interessierten sich zahlreiche Medien für die ersten Erfahrungen der Aufsichtsbehörde mit dem neuen Recht. Besonders gefragt waren statistische Angaben zu den seit dem 25. Mai 2018 bearbeiteten Beschwerden und zur Sanktionspraxis der Landesbeauftragten. Je weiter das Kalenderjahr fortschritt, umso häufiger wurden wir gebeten, eine erste Bilanz zur Umsetzung des neuen Datenschutzrechts sowie der Ergebnisse unserer Aufsichtstätigkeit zu ziehen.

Großes Presse-Echo zu Erfahrungen mit der DS-GVO

Konkrete statistische Zahlen konnten wir in der Regel nicht anbieten, weil wir bislang weder Beschwerden noch andere Aspekte unserer Tätigkeit regelmäßig statistisch erfasst haben. Wir nehmen das gro-

25 siehe VII 6

ße Interesse der Medien an solchen Zahlen jedoch zum Anlass, die Bearbeitung von Beschwerden künftig so zu strukturieren, dass konkrete statistische Angaben möglich sind.

3 Personal und Organisation der Dienststelle

Für den Doppelhaushalt 2017/2018 hatte der Landtag Brandenburg meiner Dienststelle insgesamt acht neue Stellen bewilligt, davon zwei für das Haushaltsjahr 2018. Erneut zeigte sich, wie schwierig es ist, qualifizierte Mitarbeiterinnen und Mitarbeiter für den technischen Bereich zu gewinnen. Nach mehreren erfolglosen Ausschreibungen zweier Stellen für Informatikerinnen bzw. Informatiker ist uns deren Besetzung erst mit Wirkung zum Beginn des Jahres 2019 gelungen.

Im juristischen Bereich konnte ich eine zusätzliche Mitarbeiterin für die Durchführung von Fortbildungsveranstaltungen zur Datenschutz-Grundverordnung gewinnen. Ohne deren Tätigwerden wäre es nicht möglich gewesen, den Verwaltungen und Unternehmen einen solchen Service anzubieten. Darüber hinaus hat sie uns dabei unterstützt, den erheblichen Anstieg an Beschwerden und Anfragen zu bewältigen.

Für den Doppelhaushalt 2019/2020 hat der Landtag Brandenburg meiner Dienststelle fünf weitere Stellen bewilligt. Dabei handelt es sich um jeweils zwei Stellen für Referentinnen und Referenten im technisch-organisatorischen und im juristischen Bereich sowie um eine Stelle für Sekretariatsaufgaben. Dies war erforderlich, um Personalengpässe bei der Erfüllung von Prüfpflichten im Bereich der inneren Sicherheit zu beseitigen und dem zusätzlichen Beratungsbedarf, insbesondere auf dem Gebiet des Gesundheitswesens und der medizinischen Forschung, gerecht zu werden. Darüber hinaus entsteht neuer personeller Aufwand dadurch, dass den Aufsichtsbehörden mit dem novellierten Bundesdatenschutzgesetz die Akkreditierung von Zertifizierungsstellen zugewiesen wird.

Das Wirksamwerden der Datenschutz-Grundverordnung hat meine Dienststelle auch zum Anlass genommen, interne Verfahren und Prozesse zu überprüfen und zu optimieren. Im Ergebnis wurden verschiedene organisatorische Maßnahmen – wie z. B. die einheitliche Klärung von Grundsatzfragen durch das Justiziariat oder die Bündelung und standardisierte Beantwortung immer wiederkehrender,

einfacher Anfragen – getroffen, um Zeit und Personal bestmöglich einzusetzen.

Mit der Datenschutz-Grundverordnung hat sich die Zusammenarbeit der europäischen Aufsichtsbehörden deutlich intensiviert. Dies betrifft auch die Dienststelle der Landesbeauftragten. Insbesondere Beschwerden über eine grenzüberschreitende Verarbeitung personenbezogener Daten erfordern eine enge Abstimmung zwischen federführender und betroffenen Aufsichtsbehörden. Federführend ist jeweils die für den Hauptsitz des Unternehmens zuständige Behörde. Betroffen kann u. a. jede Behörde sein, in deren Zuständigkeitsbereich eine Beschwerde eingereicht wurde oder Personen, auf die sich die Verarbeitung erheblich auswirkt, wohnen.

Die Landesbeauftragte ist in Europa federführend zuständig für mehrere Unternehmen des eBay Konzerns, wie die eBay GmbH, die eBay Kleinanzeigen GmbH und die mobile.de GmbH. Zudem koordiniert meine Dienststelle nach den Festlegungen des Bundesdatenschutzgesetzes die Bearbeitung aller Beschwerden aus Deutschland zu dem Unternehmen PayPal (Europe) S.à r.l. et Cie, S.C.A., dessen federführende Aufsichtsbehörde die Nationale Kommission für den Datenschutz (CNPD) in Luxemburg ist.

Bereits die ersten Verfahren zeigen, dass die europaweite Kooperation der Datenschutzaufsichtsbehörden sehr aufwendig und zeitintensiv ist. Zur Unterstützung der Zusammenarbeit werden alle Fälle mit grenzüberschreitender Verarbeitung in ein gemeinsames elektronisches Register eingestellt und länderübergreifend bearbeitet. Da dies ausschließlich in englischer Sprache geschieht, entsteht für fast alle Aufsichtsbehörden ein zusätzlicher Übersetzungsaufwand.

Mittlerweile sind auf dem Portal fast 651 Beschwerdefälle in Bearbeitung. Einige hiervon stammen auch aus Brandenburg. In diesen Fällen ist die Landesbeauftragte als betroffene Aufsichtsbehörde durch die federführende Behörde jeweils bei der Klärung des Sachverhalts zu beteiligen, kann eigene Stellungnahmen abgeben und bei der Entscheidungsfindung mitwirken. Aber auch in allen anderen Einzelfällen ist durch uns zu beurteilen, ob eine ähnlich gelagerte Beschwerde einer Brandenburgerin oder eines Brandenburgers vorliegt, oder ob die grenzüberschreitende Datenverarbeitung erhebliche Auswirkungen auf in Brandenburg wohnende Personen hat. Trifft dies zu, ist die Landesbeauftragte auch in diesen Fällen betrof-

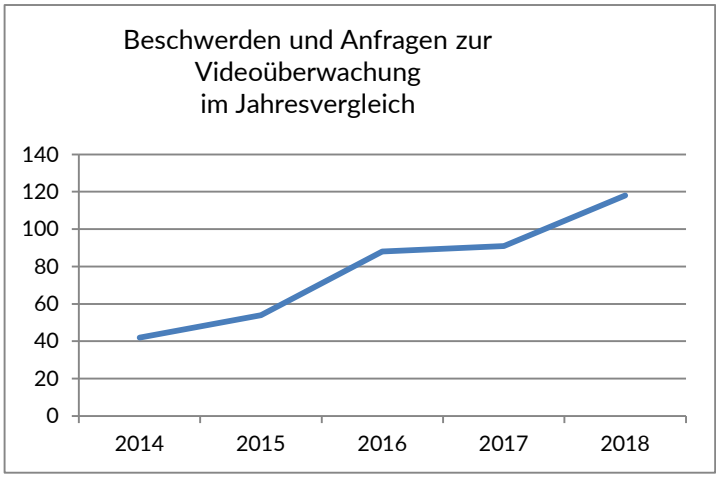
fene Aufsichtsbehörde und an der europaweiten Bearbeitung beteiligt. Die gesetzlich vorgesehene, aktive Teilnahme meiner Dienststelle an diesem Verfahren bindet erhebliche personelle Kapazitäten.

Kapitel VII
Statistiken

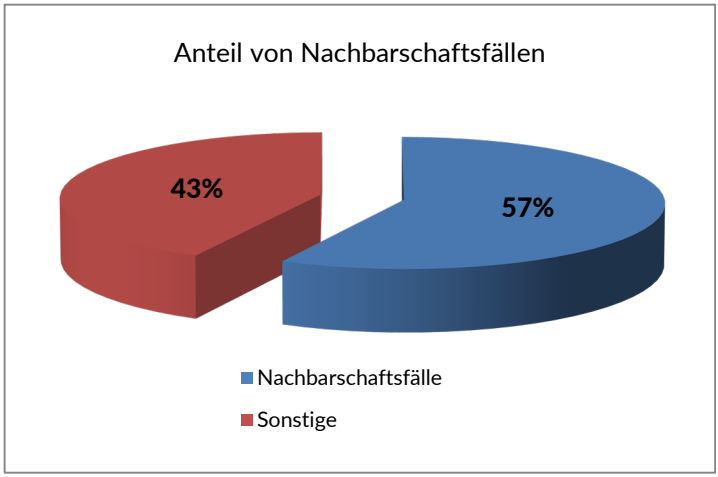
VII Statistiken

1 Videoüberwachung: Beschwerden und Anfragen

Seit Jahren verzeichnet die Landesbeauftragte eine Zunahme von Beschwerden und Anfragen zur Videoüberwachung durch Privatpersonen, Unternehmen und öffentliche Stellen. Haben sich im Jahr 2014 noch 42 Bürgerinnen und Bürger an uns gewandt, stieg deren Zahl im Berichtsjahr auf 118. In 87 Fällen handelte es sich dabei um Beschwerden, die übrigen 31 Fälle waren Anfragen. Erfasst haben wir lediglich schriftliche Beschwerden und Anfragen. Allein aufgrund der Beschwerden im Jahr 2018 waren 360 Videoüberwachungskameras auf ihre Zulässigkeit zu überprüfen.

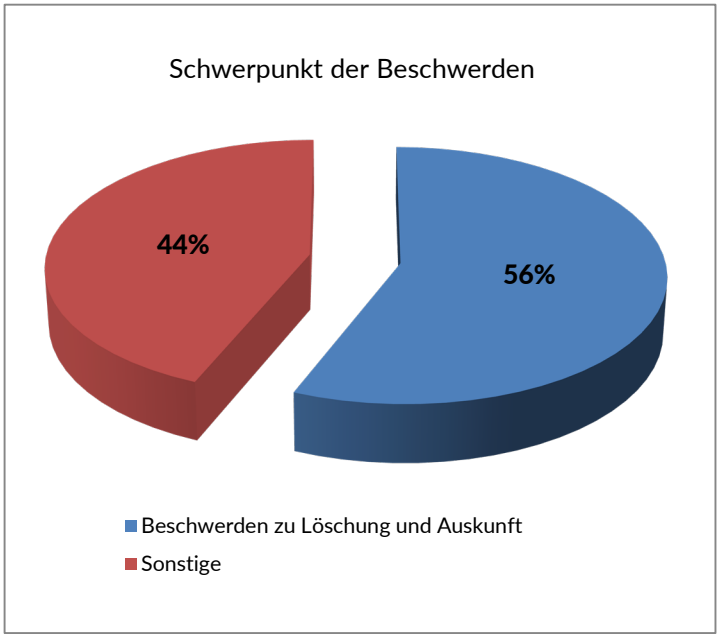


Videokameras sind weit verbreitet; sie werden unter anderem in Unternehmen, in Ladengeschäften, Restaurants und Cafés sowie in Freizeitstätten eingesetzt. In vielen Fällen fühlten sich Beschwerdeführerinnen und Beschwerdeführer durch die Videoüberwachung im öffentlich zugänglichen Raum einem Überwachungsdruck ausgesetzt und dadurch in ihren Persönlichkeitsrechten verletzt. Mehr als die Hälfte der Beschwerden im Berichtszeitraum betraf jedoch Videoüberwachungen in der Nachbarschaft. Oft stehen diese im Zusammenhang mit langjährigen Nachbarschaftsstreitigkeiten.

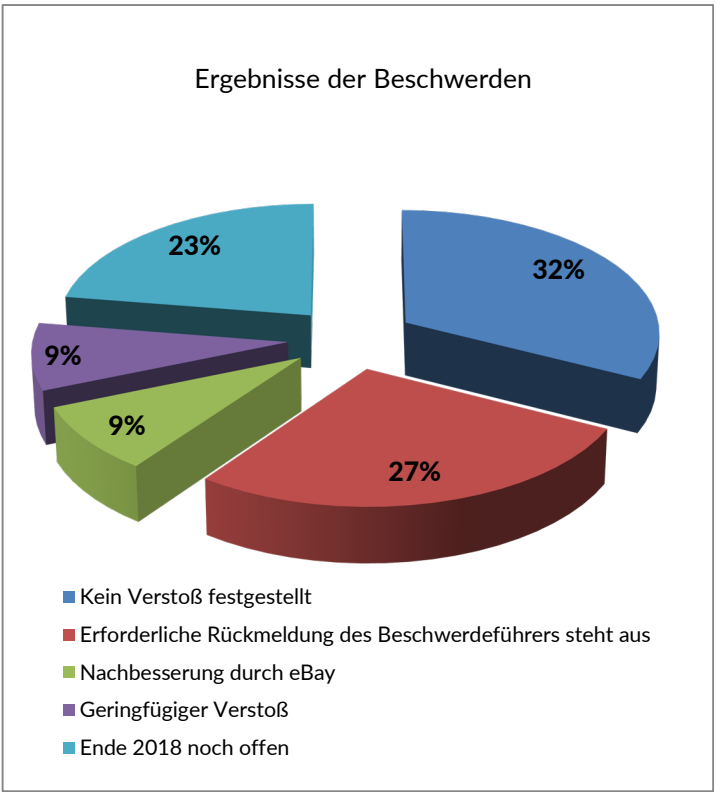


2 Unternehmen des eBay-Konzerns: Beschwerden

Mehrere Unternehmen des eBay-Konzerns haben ihren Sitz in Brandenburg und unterliegen seit Mai 2018 vollständig der Aufsicht der Landesbeauftragten. Seit diesem Zeitpunkt erreichten uns insgesamt 80 Beschwerden, davon der überwiegende Teil zu Datenverarbeitungen durch die eBay GmbH. 56 % der Beschwerden bezogen sich darauf, dass Nutzerinnen und Nutzer der Online-Portale ihr Recht auf Auskunft oder Löschung verletzt sahen. Hierzu zählen auch Beschwerden, in denen die formalen Modalitäten, um eine Auskunft zu erhalten oder eine Löschung zu erreichen, kritisiert wurden. Einen weiteren großen Teil machen Beschwerden über Werbenachrichten und technische Voreinstellungen aus.



Viele der bei der Landesbeauftragten eingereichten Beschwerden ließen sich im Kontakt mit den betroffenen Personen klären, indem wir ihnen die rechtlichen Grundlagen für die Datenverarbeitungen durch die Unternehmen des eBay-Konzerns sowie die praktischen Folgen erläuterten. In etwas mehr als einem Drittel der Fälle hat die Landesbeauftragte Untersuchungen gegenüber den Verantwortlichen eingeleitet. In der Gesamtschau zeigte sich, dass der Anteil jener Fälle, in denen – zumal meist nur geringfügige – Verstöße gegen das Datenschutzrecht zu verzeichnen waren, im Verhältnis zur Größe des Konzerns und der Reichweite seiner Datenverarbeitung niedrig ausfiel.



Wie viele dieser Fälle Abhilfemaßnahmen – z. B. Verwarnungen, Anweisungen oder die Verhängung von Geldbußen – nach sich ziehen werden, ist angesichts der Tatsache, dass eine Reihe von Verfahren zum Redaktionsschluss dieses Berichts noch andauerte, offen.

Grundsätzlich ist festzustellen, dass sich der Kontakt mit den Unternehmen seit Beginn unserer Zuständigkeit sehr konstruktiv gestaltet, Hinweisen nachgegangen und aufgezeigten Mängeln abgeholfen wird.

3 Meldungen von Datenschutzverletzungen

Seit dem 25. Mai 2018 stieg die Anzahl der nach Art. 33 DS-GVO bei der Landesbeauftragten zu meldenden Datenschutzverletzungen spürbar an. Insgesamt 124 Datenschutzverletzungen wurden von den Verantwortlichen gemeldet. 62 Meldungen entfielen dabei auf nicht öffentliche, ebenfalls 62 auf öffentliche Stellen. Nicht immer erfolgten die Meldungen innerhalb der gesetzlichen Frist von 72 Stunden nach Bekanntwerden des Vorfalls.

Einen großen Teil der Datenschutzverletzungen nahm der Fehlversand von Unterlagen ein. Dies geschah in den meisten Fällen aufgrund menschlicher Fehler: Beispielsweise wurden Schriftstücke vertauscht, weil sich die Namen der Empfängerinnen und Empfänger ähnelten. Dokumente für verschiedene Adressatinnen und Adressaten gelangten versehentlich in ein und dasselbe Kuvert. Auch kam es vor, dass manuell ins System eingetragene Daten nicht den tatsächlichen Anschriften entsprachen. Selbst wenn solche Fälle nie ganz verhindert werden können, sind Verantwortliche aufgefordert, diese Risiken durch regelmäßige Sensibilisierungen für den Datenschutz zu minimieren.

Daneben gab es Diebstähle bzw. Verluste von Datenträgern mit personenbezogenen Daten, die zu melden waren. In diese Kategorie fiel beispielsweise der Fall eines Behördenmitarbeiters, der die Akte für einen Vor-Ort-Termin beim Losfahren auf dem Autodach vergaß oder der Diebstahl einer Digitalkamera einer Kita mit Kinderfotos.

Einen nennenswerten Anteil nahmen auch Angriffe auf Computer (-netzwerke) ein, bei denen E-Mail-Adressen der Mitarbeiterinnen und Mitarbeiter bzw. Kundinnen und Kunden entwendet wurden. Gerade in diesen Fällen sind regelmäßig viele Personen von der Datenschutzverletzung betroffen und hierüber ggf. zu informieren.

4 Fälle mit grenzüberschreitender Verarbeitung

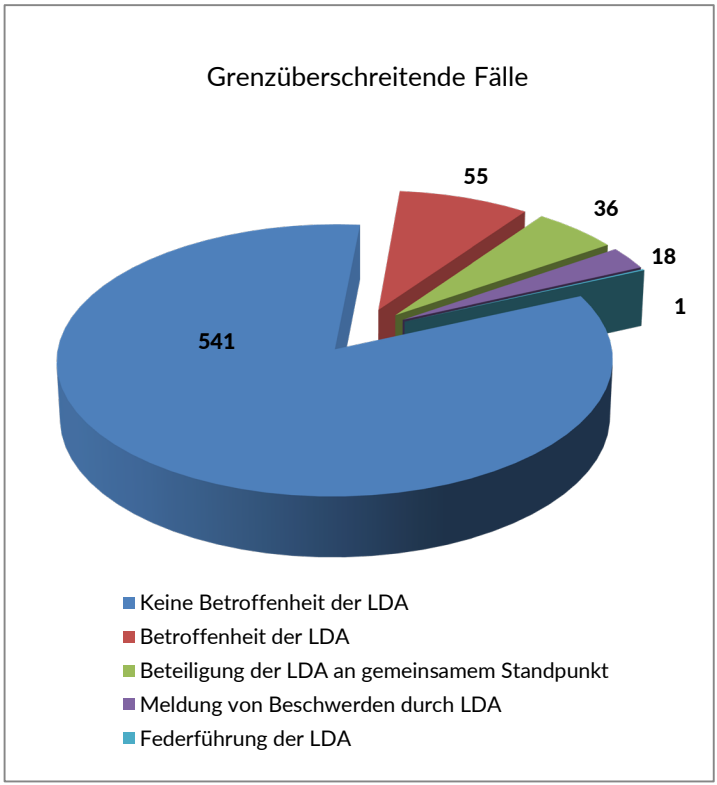
Das Ziel der seit Mai 2018 wirksamen Datenschutz-Grundverordnung (DS-GVO) ist eine Harmonisierung und eine Vereinheitlichung des Datenschutzes in der Europäischen Union. Zur Unterstützung der Kooperation der Datenschutzaufsichtsbehörden enthält sie eine

Reihe von Regelungen (z. B. für One-Stop-Shop-Verfahren, gegenseitige Amtshilfe, Kohärenzverfahren). Das Binnenmarkt-Informationssystem der Europäischen Kommission bietet eine technische Plattform für den hierzu erforderlichen Austausch (Näheres zur Zusammenarbeit der europäischen Aufsichtsbehörden siehe VI 3).

Seit dem o. g. Zeitpunkt waren von unserer Behörde insgesamt 597 grenzüberschreitende Fälle daraufhin zu prüfen, ob wir bei den von anderen Aufsichtsbehörden gemeldeten Datenschutzbeschwerden federführende oder betroffene Aufsichtsbehörde sind und entsprechende Verfahrensschritte ergreifen müssen. In 55 Fällen stellten wir die Betroffenheit unserer Dienststelle fest, weil der Verantwortliche eine Niederlassung in Brandenburg hatte oder die gemeldete Verarbeitung personenbezogener Daten erhebliche Auswirkungen auf Bürgerinnen und Bürger unseres Bundeslandes haben könnte. Eine Federführung haben wir in einem Fall angenommen. In den restlichen 541 Fällen entschieden wir uns nach intensiver Prüfung des jeweiligen Vorgangs dafür, uns nicht an dem weiteren Verfahren zu beteiligen, da die beiden genannten Bedingungen nicht erfüllt waren.

Darüber hinaus haben wir in 18 Fällen, aufgrund bei uns eingegangener Beschwerden gegen eine grenzüberschreitende Verarbeitung, die Vorgänge den anderen europäischen Aufsichtsbehörden über das Binnenmarkt-Informationssystem zur Kenntnis gegeben. Diese haben nun die Möglichkeit zu prüfen, ob sie federführende oder betroffene Aufsichtsbehörde in dem eingebrachten Verfahren sind.

In 36 Fällen haben wir uns an Verfahren zur Vorbereitung eines gemeinsamen Standpunktes beteiligt. Dies betraf überwiegend Stellungnahmen zu Listen von Verarbeitungsvorgängen, für die eine Datenschutzfolgenabschätzung nach Artikel 35 Absatz 4 DS-GVO durchzuführen ist.



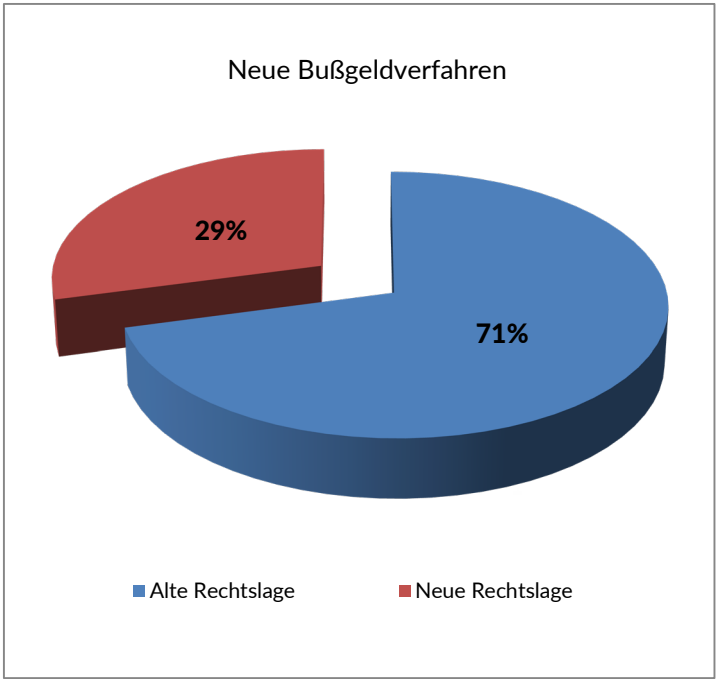
Insgesamt lässt sich festhalten, dass wir seit dem 25. Mai 2018 in 651 Fällen mit grenzüberschreitender Verarbeitung von personenbezogenen Daten bzw. im Wege der gegenseitigen Amtshilfe und Kooperation tätig geworden sind.

5 Bußgeldverfahren

Im Berichtsjahr führten wir 24 neue Ordnungswidrigkeitenverfahren wegen Verstößen gegen datenschutzrechtliche Vorschriften. 17 Fälle leiteten Polizei und Staatsanwaltschaft an die Bußgeldstelle bei der Landesbeauftragten weiter. Sechs Vorgänge erhielt sie von den für Datenschutzaufsicht zuständigen Mitarbeiterinnen und Mitarbeitern der Behörde. In einem Fall führte die Beschwerde eines Bürgers unmittelbar zur Einleitung eines Ordnungswidrigkeitenverfahrens. Im Vergleich zu den beiden Vorjahren blieb die Gesamtzahl

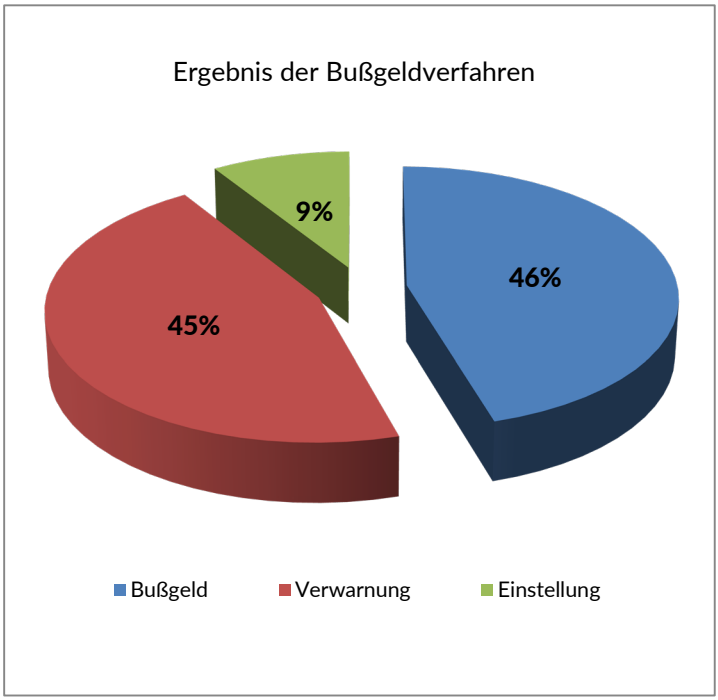
der geführten Verfahren ungefähr konstant. Im Berichtszeitraum 2016/2017 waren es 50.

Noch hat sich das Wirksamwerden der Datenschutz-Grundverordnung nicht auf den Umfang der Bußgeldverfahren ausgewirkt. Von den 24 neuen Verfahren betreffen lediglich sieben solche Sachverhalte, die nach der neuen Rechtslage zu bewerten sind. Die übrigen 17 Fälle waren auf der Grundlage des vor dem 25. Mai 2018 geltenden Datenschutzrechts zu bearbeiten, da Ordnungswidrigkeiten stets nach dem zum Zeitpunkt ihrer Begehung geltenden Recht zu bewerten sind. Schwerpunkt der Tätigkeit der Bußgeldstelle der Landesbeauftragten war im Berichtszeitraum somit die Bearbeitung von Fällen nach altem Recht.



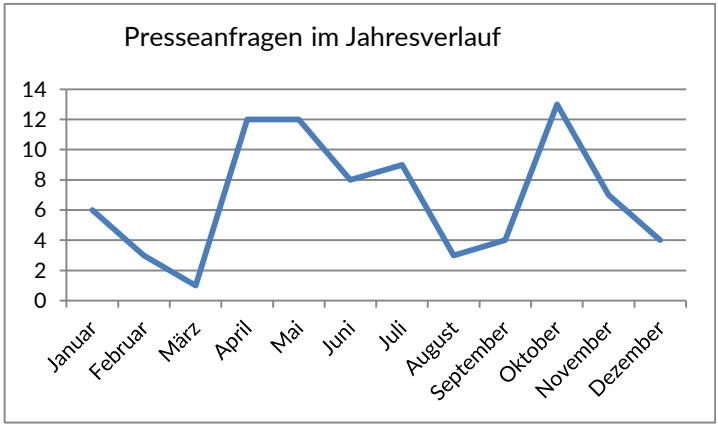
Die Ordnungswidrigkeitenverfahren richteten sich in 18 Fällen gegen nicht öffentliche Stellen und in sechs Fällen gegen einzelne Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen. Insgesamt hat die Landesbeauftragte 11 Verfahren wegen Verstößen gegen das Bundes- und das Brandenburgische Datenschutzgesetz abgeschlossen.

Sie waren bereits teilweise im vorigen Berichtszeitraum eröffnet worden. In fünf dieser Fälle hat sie ein Bußgeld verhängt und in einem Fall eine Verwarnung festgesetzt. Die übrigen fünf Verfahren stellte sie ein. In der Summe beliefen sich die verhängten Bußgelder auf 6.700 Euro.



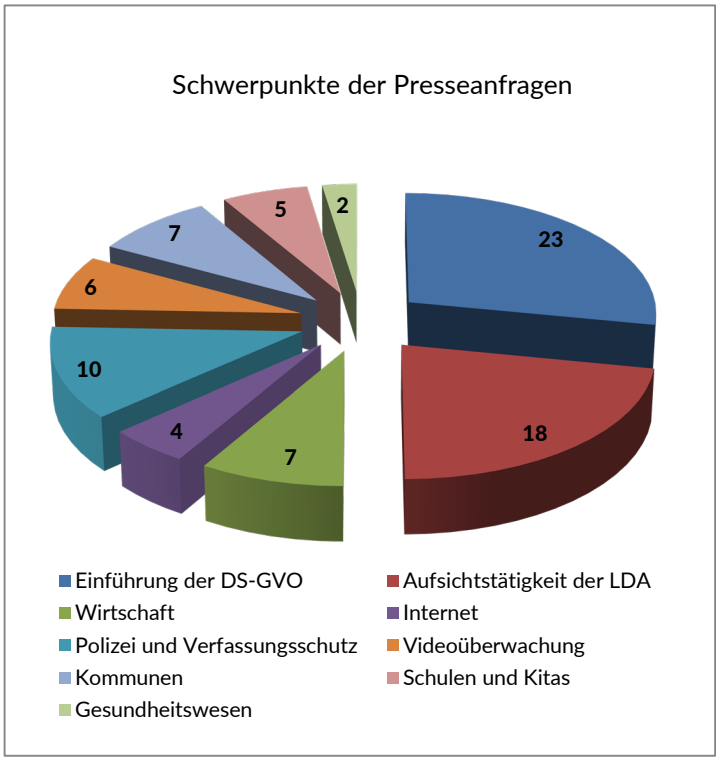
6 Pressearbeit

Die intensive Berichterstattung der Medien über die Einführung der Datenschutz-Grundverordnung spiegelte sich in wesentlich häufigeren Presseanfragen an die Landesbeauftragte wider. Im Vergleich zum Vorjahr, als wir 29 Anfragen verzeichneten, stieg die Zahl der Anfragen im Berichtsjahr auf 82.



Die Datenschutz-Grundverordnung wurde am 25. Mai 2018 wirksam. Dementsprechend waren insbesondere die Monate April und Mai, als die zweijährige Umsetzungsfrist fast vorüber war, von zahlreichen Presseanfragen geprägt. Journalistinnen und Journalisten wollten wissen, welche neuen Rechte und Pflichten aus der Verordnung erwachsen, wie sich Unternehmen und Verwaltungen vorbereitet haben und welche Veränderungen der Aufsichtstätigkeit nach dem 25. Mai 2018 zu erwarten sind. Im Sommer ebbte das Interesse der Medien am Datenschutz ab, um im Herbst, etwa ein halbes Jahr nach der Einführung der Datenschutz-Grundverordnung wieder aufzuflammen. Insbesondere im Oktober zogen die Medien eine erste Bilanz und erkundigten sich bei uns nicht zuletzt danach, in welchem Umfang die Landesbeauftragte bereits von ihren neuen bzw. erweiterten Befugnissen als Aufsichtsbehörde Gebrauch gemacht hat.

Die Darstellung der inhaltlichen Schwerpunkte gestaltet sich schwierig, da die Fragen zur Einführung der Datenschutz-Grundverordnung teilweise auch fachbezogene Aspekte enthielten. Dennoch lässt sich sagen, dass der Datenschutz bei Polizeibehörden, in der Wirtschaft, in den Kommunen sowie in Schulen und Kindergärten für die Journalistinnen und Journalisten am interessantesten war. Querschnittsthemen wie die Zulässigkeit der Videoüberwachung sowie der Datenschutz im Internet waren in etwa gleichem Umfang gefragt.



Ordnet man die Anfragen den verschiedenen Medien zu, lässt sich feststellen, dass sich vorwiegend Tageszeitungen sowie das Fernsehen, aber auch Online-Medien an die Landesbeauftragte wandten.

Die Verbreitung dieser Medien beschränkte sich in der Mehrzahl der Anfragen zwar auf die Region Berlin-Brandenburg, doch nahmen auch bundesweit tätige Medien einen nicht unerheblichen Anteil der Presseanfragen bei der Landesbeauftragten ein.

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