Landesbeauftragte
für Datenschutz
und Akteneinsicht

# Tätigkeitsbericht 2021
## Datenschutz

**Titelbild**

Motiv: Medienzentrum Universität Potsdam in Golm

Bildrechte: Marcus Ebener Fotografie

**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: ARNOLD group

# Tätigkeitsbericht Datenschutz

# der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zum 31. Dezember 2021

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat nach Artikel 59 Datenschutz-Grundverordnung und nach § 37 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz jeweils einen Jahresbericht über ihre Tätigkeit zu erstellen und dem Landtag sowie der Landesregierung zu übermitteln. Diese Berichte decken den Zeitraum vom 1. Januar bis zum 31. Dezember 2021 ab.

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

# Vorwort

Liebe Leserinnen, liebe Leser,

auch im Jahr 2021 war die Auswahl von Themen für den Tätigkeitsbericht Datenschutz wieder groß. Entschieden habe ich mich für Beschwerdefälle, Beratungsanfragen und Begleitungen von Projekten, die für viele von Ihnen interessant sein dürften. Auch über solche datenschutzrelevante Vorhaben, die künftig für unseren Alltag wichtig werden, möchte ich Sie informieren.

Der letztgenannten Kategorie ist das erste Schwerpunktthema zuzuordnen – die Digitalisierung von Verwaltungsleistungen. Obwohl das Onlinezugangsgesetz dem Land und den Kommunen vorschreibt, ihre Verwaltungsleistungen bereits bis Ende 2022 über Verwaltungsportale auch digital anzubieten, wirft die Umsetzung immer neue Probleme auf. Da es sich um ein bundesweites Vorhaben handelt, ist der Abstimmungsbedarf hoch. Meine Behörde sowie die übrigen deutschen Datenschutzaufsichtsbehörden arbeiten daran, dass Sie, liebe Leserinnen und Leser, digitale Verwaltungsleistungen im Ergebnis datenschutzkonform nutzen können.

Ein Thema, das uns alle bereits seit zwei Jahren betrifft, ist die Corona-Pandemie. Für den Datenschutz hat die Nachverfolgung von Kontaktpersonen im Falle von Infektionen weiterhin besondere Relevanz. Hier tragen die kommunalen Gesundheitsämter die Hauptlast. Sie sollen die Kontakte nachverfolgen und die Isolation Infizierter bzw. die Quarantäne von Kontaktpersonen verfügen, um die Ausbreitung des Virus einzudämmen. Als Hilfsmittel standen ihnen unter anderem das Luca-System sowie – für die weitergehende Datenverarbeitung – die Software SORMAS zur Verfügung. Leider mussten wir feststellen, dass beide Systeme dem Datenschutz nicht ausreichend Rechnung trugen. Die Schwierigkeiten, die sich im Verlauf des Berichtsjahres ergaben, stelle ich Ihnen in zwei weiteren Schwerpunktkapiteln vor.

Der erneute Anstieg der obligatorischen Meldungen von Datenschutzverletzungen – der sogenannten Datenpannen – bereitet mir

große Sorgen. Sicherheitslücken und gezielte Hackerangriffe liegen solchen Meldungen häufig zu Grunde. Ein Beitrag meines Berichts beschäftigt sich mit dem wohl prominentesten Beispiel des zurückliegenden Jahres, nämlich einer Sicherheitslücke bei Microsoft Exchange Servern, einer Software, die in Unternehmen, Behörden und Bildungseinrichtungen weit verbreitet ist. Ein weiterer Beitrag zeigt anhand eines ausgewählten Falles auf, welche Risiken sich aus dem Diebstahl von Nutzerdaten ergeben können. Beide Kapitel des Tätigkeitsberichts führen deutlich vor Augen, dass die IT-Sicherheit immer auch eine Voraussetzung für erfolgreichen Datenschutz ist.

Mit datenschutzrechtlichen und technischen Aspekten des Einsatzes von Produkten und Diensten des Unternehmens Microsoft setzen sich die Datenschutzaufsichtsbehörden seit mehreren Jahren auseinander. Im Auftrag der Datenschutzkonferenz leitet das Bayerische Landesamt für Datenschutzaufsicht gemeinsam mit meiner Behörde Gespräche mit dem Unternehmen. Deren Ziel ist es, öffentliche und private Stellen bei ihrem Bestreben zu unterstützen, die derzeit aus unserer Sicht datenschutzrechtlich problematischen Produkte oder Dienste künftig datenschutzkonform einzusetzen. Ein Beitrag zur Entwicklung dieser nicht immer einfachen Gespräche darf in meinem Tätigkeitsbericht nicht fehlen.

Weiterhin hat das sogenannte Schrems II-Urteil des Europäischen Gerichtshofs zum internationalen Datenverkehr eine hohe Bedeutung für brandenburgische Unternehmen. Die Entscheidung hat die Voraussetzungen für eine rechtmäßige Übermittlung personenbezogener Daten in die Vereinigten Staaten von Amerika und andere Drittländer aufgezeigt. Der weit verbreitete Einsatz von Software oder sozialen Medien, die aus solchen Ländern betrieben werden und bei denen die Datenübermittlung quasi unvermeidbar ist, legt nahe, dass es sich hierbei nicht um ein Nischenproblem handelt. In

meinem Bericht stelle ich deshalb eine stichprobenartige Prüfung brandenburgischer Unternehmen vor, die wir im Rahmen eines länderübergreifenden Vorgehens durchführen, um die Einhaltung des Schrems II-Urteils bei der Einbindung außereuropäischer E-Mail- und Webhosting-Dienste sicherzustellen. Auch berichte ich über die Ergebnisse einer weiteren länderübergreifend koordinierten Prüfung von Webseiten verschiedener Medienunternehmen, an der sich meine Behörde beteiligt hat. Dabei ging es um den Einsatz von Tracking-Techniken auf deren Webseiten – eine Datenverarbeitung, die zunehmend Gegenstand von Beschwerden ist.

Mein Bericht informiert zudem über weitere anlasslose Prüfungen, die ich im zurückliegenden Jahr wieder verstärkt durchgeführt habe, über kleinere und größere interessante Fälle sowie über anschauliche Beispiele aus der Praxis meiner Bußgeldstelle. Ich wünsche Ihnen eine interessante Lektüre.

Dagmar Hartge

# Teil A: Bericht nach Art. 59 Datenschutz-Grundverordnung

## I Schwerpunkte

# 1 Verwaltungsmodernisierung

Die Digitalisierung der Verwaltung ist Kernbestandteil der E-Government-Strategien des Bundes und der Länder. Mit dem Onlinezugangsgesetz (OZG) sollen die Voraussetzungen geschaffen werden, insbesondere Bürgerinnen und Bürgern Dienstleistungen der öffentlichen Verwaltung elektronisch anzubieten und ihnen einen digitalen, wenn möglich medienbruchfreien Zugang zu eröffnen. Diese vereinfachte Inanspruchnahme von Verwaltungsleistungen soll dazu dienen, aufwändige Behördengänge zu erübrigen. Gerade die andauernde Corona-Pandemie zeigt, welche Bedeutung und Dringlichkeit ein solcher Zugang hat.

Das Onlinezugangsgesetz verpflichtet Bund und Länder, bis spätestens zum Ablauf des Jahres 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten und diese miteinander zu einem Portalverbund zu verknüpfen. Ein Verwaltungsportal bezeichnet hierbei ein bereits gebündeltes elektronisches Verwaltungsangebot eines Landes oder des Bundes mit entsprechenden Angeboten einzelner Behörden. Unter Verwaltungsleistungen versteht das Gesetz die elektronische Abwicklung von Verwaltungsverfahren und die dazu erforderliche elektronische Information der Nutzerinnen und Nutzer sowie die Kommunikation mit diesen über allgemein zugängliche Netze. Zielgruppe sind natürliche und juristische Personen, Vereinigungen, soweit ihnen ein Recht zustehen kann, oder Behörden.

Der IT-Planungsrat hat 575 Verwaltungsleistungen identifiziert, die im Rahmen der Umsetzung des Onlinezugangsgesetzes zu digitalisieren sind. Er hat diese – nach mehreren Themenfeldern geordnet – einzelnen Bundesländern federführend zur Implementierung zugewiesen. Im Digitalisierungsprogramm Föderal haben sich der Bund und die Länder auf eine arbeitsteilige Umsetzung der einzelnen OZG-Leistungen geeinigt. Die Themenfeldinhaber stellen in der Umsetzungsphase sicher, dass für jede OZG-Leistung ein Online-Service bereitgestellt wird. Diese Lösung kann anschließend von an-

deren Bundesländern bzw. den Kommunen nachgenutzt, d. h. ohne weitere eigene Programmierung angewendet werden.[1]

In die Umsetzung des Onlinezugangsgesetzes ist unsere Behörde intensiv eingebunden. Auf Bundes- bzw. länderübergreifender Ebene koordinierten und leiteten wir im Berichtszeitraum als Vorsitz des Arbeitskreises Verwaltung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) eine Arbeitsgruppe, die die Umsetzung des Onlinezugangsgesetzes aus datenschutzrechtlicher Sicht begleitet. Insbesondere befasst diese sich mit Fragen der länderübergreifenden Realisierung von Verwaltungsleistungen mit Blick auf die Anwendung des „Einer für alle/viele"-Prinzips. Auf Landesebene sind wir vorrangig bei der Umsetzung der Leistungen im Themenfeld „Ein- und Auswanderung" beratend tätig, da das Land Brandenburg Themenfeldinhaber ist.

## 1.1 Arbeitsgruppe der Datenschutzkonferenz zur Begleitung der Umsetzung des Onlinezugangsgesetzes

Die im Auftrag der Datenschutzkonferenz eingerichtete Arbeitsgruppe OZG-Portallösungen, an der Datenschutzaufsichtsbehörden mehrerer Bundesländer unter unserer Leitung mitwirken, befasste sich insbesondere mit der Frage, wie Verwaltungsleistungen nach dem Onlinezugangsgesetz (OZG) datenschutzkonform sowohl landesintern als auch länderübergreifend realisiert werden können. Vor dem Hintergrund der auch vom IT-Planungsrat geforderten Anwendung des „Einer für alle/viele"-Prinzips, das gleichzeitig Strategie der Nachnutzung von Verwaltungsleistungen durch unterschiedliche datenschutzrechtlich verantwortliche Stellen ist, bedarf es zunächst einer genauen Betrachtung der Implementierung von Portalanwendungen und einer Klärung der Verantwortlichkeit. Die Arbeitsgruppe hat auf Basis bestehender Umsetzungsvarianten von Portallösungen und der dahinter liegenden Fachanwendungen für die Erbringung der eigentlichen Dienstleistung mögliche Konstellationen von Betreibermodellen in Bezug auf die datenschutzrechtliche Verantwortlichkeit analysiert und Konsequenzen abgeleitet.

1 Leitfaden zum Digitalisierungsprogramm des IT-Planungsrats unter leitfaden.ozg-umsetzung.de.

Konkret wurden beispielsweise die bereits bestehenden Verwaltungsleistungen der Projekte „Elterngeld Digital“ des Bundesministeriums für Familie, Senioren, Frauen und Jugend, „Bafög Digital“ des Ministeriums für Wirtschaft, Wissenschaft und Digitalisierung des Landes Sachsen-Anhalt sowie „Aufenthaltstitel für Erwerbstätigkeit“ des Ministeriums des Innern und für Kommunales des Landes Brandenburg näher betrachtet. Letzteres unterliegt unserer direkten datenschutzrechtlichen Beratungs- und Aufsichtstätigkeit.[2]

Im Rahmen intensiver Gespräche der Arbeitsgruppe unter Einbeziehung des Bundesministeriums des Innern, für Bau und Heimat wurden die bestehenden Implementierungsvarianten diskutiert und insbesondere Fragen hinsichtlich der datenschutzrechtlichen Verantwortlichkeit und der Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in den jeweiligen Verwaltungsportalen erörtert. Als zentrale Herausforderung im Rahmen der Umsetzung des Onlinezugangsgesetzes stellte sich die korrekte Zuordnung der Verantwortlichkeit nach Artikel 4 Nummer 7 Datenschutz-Grundverordnung (DS-GVO) heraus. Dies gilt auch vor dem Hintergrund, dass die genannte Regelung nach ihrem Wortlaut auf die jeweils handelnde und fachlich zuständige Behörde abstellt und nicht auf die übergeordnete Rechtsträgerin bzw. den übergeordneten Rechtsträger. Es ergibt sich daher die Frage, welche der oftmals zahlreichen bei der Umsetzung eines OZG-Portals beteiligten Stellen tatsächlich in der Rolle des Verantwortlichen ist.

Nach Auswertung der aus den Beispielprojekten bekannten Betreibermodelle zeigte sich, dass die Bewertung der datenschutzrechtlichen Verantwortlichkeit von Portallösungen bei der Erhebung personenbezogener Daten und Übermittlung an die zuständigen Fachbehörden schwierig ist. Nicht in jedem Fall ist eine fachliche Zuständigkeit der Betreiberin oder des Betreibers auf Grundlage der derzeitigen Fassung des Onlinezugangsgesetzes gegeben. Dies kann im späteren Verlauf der Umsetzung des Gesetzes auch weitere Portale betreffen. Um hier Rechtsunsicherheiten zu vermeiden, bedarf es klarer Vorgaben und ggf. einer Änderung der rechtlichen Vorschriften.

2 Siehe A I 1.2.

Die Arbeitsgruppe identifizierte unterschiedliche Varianten der Zuordnung der Verantwortlichkeit und somit der Abbildung der Betreibermodelle in den Portallösungen. So können u. a. eine Auftragsverarbeitung nach Artikel 28 DS-GVO, eine gemeinsame Verantwortung nach Artikel 26 DS-GVO oder eine getrennte bzw. nacheinander bestehende Kettenverantwortlichkeit mehrerer Stellen vorliegen. Des Weiteren besteht dem Grundsatz nach auch die Möglichkeit, eine Verantwortlichkeit nach Artikel 4 Nummer 7 Halbsatz 2 DS-GVO gesetzlich zuzuweisen. Letzteres ist nach derzeitigem Recht aber wohl nur landesintern und nicht bzw. nur eingeschränkt länderübergreifend möglich.

Ihre Ergebnisse fasste die Arbeitsgruppe in einem Sachstandsbericht zusammen, der von der Datenschutzkonferenz zur Kenntnis genommen und dem Bundesministerium des Innern und für Heimat (nach der Bundestagswahl) übergeben wurde. Der Bericht bildet auf Grundlage der darin festgehaltenen Problemstellungen bei der Umsetzung des Onlinezugangsgesetzes und möglicher Lösungsvarianten die Basis für weitere Gespräche sowie Abstimmungen mit dem Ministerium und ggf. eine Gesetzesanpassung.

Im Rahmen der Nachnutzung von Leistungen ist auch die Plattform Fit-Store der Föderalen IT-Kooperation (FITKO), einer von Bund und Ländern gemeinsam getragenen Anstalt des öffentlichen Rechts zur Unterstützung der Verwaltungsdigitalisierung, mitzubetrachten. Der Fit-Store soll als Marktplatz für digitale Verwaltungsleistungen dienen, Angebote und Nachfragen zu bereits verfügbaren Online-Diensten vermitteln sowie die vergaberechtlich sichere Umsetzung der Nachnutzung von Verwaltungsleistungen ermöglichen. Die Arbeitsgruppe OZG-Portallösungen der Datenschutzkonferenz hat sich von der FITKO Vorschläge für eine mögliche Regelung zur Nachnutzung von Verwaltungsleistungen darlegen lassen (hier basierend auf einer Auftragsverarbeitung nach Artikel 28 DS-GVO). Der FITKO kommt mit dem Fit-Store zwar eine spezielle Rolle im OZG-Verbund bei der Nachnutzung von Diensten zu, diese besteht jedoch oftmals eher in der Vermittlung von Softwarelösungen und nicht in einer tatsächlichen Verarbeitung personenbezogener Daten. Die datenschutzrechtliche Erörterung der Rolle der FITKO ist noch nicht abgeschlossen und eine Fortführung der Gespräche geplant.

Die Umsetzung des Onlinezugangsgesetzes, insbesondere die Nachnutzung von Verwaltungsleistungen nach dem „Einer für alle/viele“-Prinzip, bedarf weiter unserer datenschutzrechtlichen Begleitung. Bei bestimmten Konstellationen des Betriebs von Portallösungen erscheint auch ein gesetzgeberisches Handeln zur rechtlichen Absicherung notwendig. Die Arbeitsgruppe der Datenschutzkonferenz hat mögliche Lösungsansätze aufgezeigt, um ggf. kurzfristig einen datenschutzkonformen Betrieb zu gewährleisten. Ein Austausch und eine Abstimmung mit den Themenfeldinhabern der Länder, dem Bundesministerium des Innern und für Heimat und den anderen Datenschutzaufsichtsbehörden sind weiterhin geboten.

## 1.2 Projekte im Themenfeld „Ein- und Auswanderung“

Im Berichtszeitraum haben wir unsere intensive datenschutzrechtliche Begleitung der Aktivitäten des brandenburgischen Ministeriums des Innern und für Kommunales als Inhaber des Themenfeldes „Ein- und Auswanderung“ bei der Umsetzung des Onlinezugangsgesetzes (OZG) fortgeführt.[3] Im Mittelpunkt standen dabei die Verwaltungsleistungen „Aufenthaltstitel“ sowie „Aufenthaltskarten und aufenthaltsrelevante Bescheinigungen“, konkret „Daueraufenthaltsbescheinigungen“. Das Ministerium hat unsere Behörde frühzeitig in die Pilotierung der Antragsverfahren sowie die datenschutzrechtliche Befassung mit der umgesetzten technischen Implementierung eingebunden. Hervorzuheben ist, dass es selbst hier nicht als datenschutzrechtlich Verantwortlicher handelt. Dies obliegt weiterhin vollständig den jeweils fachlich zuständigen Ausländerbehörden der Landkreise und kreisfreien Städte des Landes Brandenburg.

Umgesetzt werden die genannten Verwaltungsleistungen als Auftragsverarbeitung im Sinne von Artikel 28 DS-GVO, wobei die Ausländerbehörden jeweils ein Antragsformular als Komponente in ihre Internetpräsenz einbinden. Die Erhebung der personenbezogenen Antragsdaten und anschließende Weiterleitung an die zuständige Behörde erfolgt über die eingebettete Komponente durch die Anstalt für Kommunale Datenverarbeitung in Bayern als eingebundene Dienstleisterin. Diese ist Unterauftragnehmerin des Brandenbur-

3 Tätigkeitsbericht Datenschutz 2020, A V 1.2.

gischen IT-Dienstleisters. Insofern besteht seitens der nutzenden brandenburgischen Kommunen lediglich ein Auftragsverarbeitungsverhältnis gemäß Artikel 28 DS-GVO mit dem Landesdienstleister, der seinerseits ein Auftragsverarbeitungsverhältnis mit der bayerischen Anstalt hat. So muss diese nicht mit allen brandenburgischen Ausländerbehörden (und potenziell vielen weiteren kommunalen Behörden in Deutschland) jeweils eigene Verträge abschließen.

Die Übermittlung der personenbezogenen Antragsdaten an die zuständige Fachbehörde erfolgte im Pilotstadium des Verfahrens über das besondere elektronische Behördenpostfach (beBPo) der Kommunen bzw. Landkreise unter Nutzung der IT-Basiskomponenten gemäß § 11 Brandenburgisches E-Government-Gesetz. Mit Fortentwicklung der Datenaustauschformate der Koordinierungsstelle für IT-Standards (KoSIT) und der Implementierung des Standards XAusländer kann perspektivisch eine direkte Datenübergabe in die Fachanwendung erfolgen.

Bei der Pilotierung der genannten Verwaltungsleistungen waren wir in die Erarbeitung der umfangreichen Projektdokumentation eingebunden und wirkten u. a. an der Erstellung des Rahmenkonzepts, des Datenschutzkonzepts und der IT-Sicherheitsbetrachtung mit. Hier waren wir nicht nur direkt in Kontakt mit dem Ministerium des Innern und für Kommunales sowie dem Brandenburgischen IT-Dienstleister, sondern auch mit den Verantwortlichen auf kommunaler Ebene. Kritisch ist anzumerken, dass die Einbindung der kommunalen Datenschutzbeauftragten erst spät erfolgte oder sie nur vereinzelt an den Beratungen der Projektgruppe und der Steuerungsgremien teilnahmen. Dies führte dazu, dass uns kurz vor Einführung und Produktivsetzung des Pilotverfahrens von Seiten der kommunalen Datenschutzbeauftragten oder der jeweils für die Freigabe zuständigen kommunalen Stelle Anfragen zur datenschutzrechtlichen Bewertung der Umsetzung der Verwaltungsleistungen erreichten.

Mit der Weiterentwicklung der Dienste ist auch die notwendige Programmdokumentation, deren Vorliegen eine Grundvoraussetzung für die Nachnutzung ist, fortzuschreiben. Das betrifft ggf. auch die Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO aufgrund der Vielzahl möglicher betroffener Perso-

nen sowie der Sensitivität zumindest eines Teils der Antragsdaten. Der Brandenburgische IT-Dienstleister richtete diesbezüglich mehrere behördenübergreifende Workshops mit unserer Beteiligung aus.

Die genannten Verwaltungsleistungen können durch interessierte Kommunen nachgenutzt werden. Dies ist sowohl in Brandenburg als auch länderübergreifend auf Grundlage entsprechender Auftragsverarbeitungsverträge gemäß Artikel 28 DS-GVO über die Anstalt für Kommunale Datenverarbeitung in Bayern möglich. Das Ministerium des Innern und für Kommunales steht im Rahmen seines Steuerungsauftrags als Themenfeldinhaber in Kontakt mit Interessenten aus anderen Bundesländern. Die Möglichkeit der Nachnutzung wurde bereits über ein entsprechendes Angebot im Fit-Store der Föderalen IT-Kooperation (FITKO) publiziert.

Ergänzend ist darauf hinzuweisen, dass die o. g. Verwaltungsleistungen nicht komplett digital abgewickelt werden können und sie damit keine vollständigen Leistungen im Sinne des OZG-Reifegradmodells darstellen. Aus rechtlichen und fachlichen Gründen muss z. B. die Identifizierung der betroffenen Person nach wie vor persönlich in der Ausländerbehörde erfolgen. Der Online-Dienst entspricht damit der Stufe 2 (von 4) des OZG-Reifegradmodells. Dies kann sich erst mit dem Vorhandensein, der internationalen Anerkennung und sicheren Integrierbarkeit nationaler elektronischer Identitätsdokumente ändern.

### 1.3 Entwicklungen zur Registermodernisierung

Bereits im Vorjahr berichteten wir über unsere Beteiligung an der Durchführung der an europäischen Vorgaben orientierten Modernisierung der öffentlichen Register.[4] Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hatte gegen die Planungen der Bundesregierung zur Nutzung der Steueridentifikationsnummer als faktischer Personenkennziffer datenschutzrechtliche und verfassungsrechtliche Bedenken geltend gemacht. Sie wurden auch im Gesetzgebungsverfahren nicht aufgegriffen.

4 Tätigkeitsbericht Datenschutz 2020, A V 1.1.

Kernbestandteil des Registermodernisierungsgesetzes[5] ist das Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung, welches die Behandlung der Steuer-ID als Personenkennziffer regelt. Es ermächtigt die Bundesregierung zum Erlass von Umsetzungsverordnungen. Die Landesbeauftragte geht davon aus, dass das Gesetz Gegenstand verfassungsrechtlicher Nachprüfung wird.

Bereits im Jahr 2019 hatte die Datenschutzkonferenz eine Arbeitsgruppe, bestehend aus Mitgliedern verschiedener Arbeitskreise und unter Federführung des Bundesbeauftragten eingerichtet, die die Positionen der Konferenz gegenüber der Bundesregierung vertreten sollte. Deren Arbeit ist noch nicht beendet. Zu ihren weiteren Themen gehört die Schaffung und Anpassung von Rechtsgrundlagen für die Vielzahl neuer Dienste, mit denen der elektronische Zugang zu Verwaltungsleistungen sicher und effizient erfolgen soll. Fraglich ist hierbei etwa, ob und in welchen Bereichen Einwilligungen nach Artikel 6 Absatz 1 Satz 1 Buchstabe a Datenschutz-Grundverordnung (DS-GVO) neben der Rechtsgrundlage nach Artikel 6 Absatz 1 Satz 1 Buchstabe e DS-GVO, die eine Datenverarbeitung erlaubt, wenn sie zur Erfüllung öffentlicher Aufgaben erforderlich ist, bestehen können. Die Landesbeauftragte hat sich in diesem Zusammenhang dafür ausgesprochen, weitgehend auf konkurrierende Einwilligungslösungen zu verzichten und staatliche Datenverarbeitung auf klare gesetzliche Grundlagen zu stützen.

Ein weiterer Schwerpunkt liegt in einer Organisation der Dienste, die die Einhaltung des Erforderlichkeitsprinzips sichert und die Transparenz gegenüber den jeweiligen Nutzerinnen und Nutzern garantiert. Dies betrifft die nicht abschließend geklärten und nach der Entscheidung für die Steuer-ID als Ordnungsmerkmal besonders wichtigen Fragen der Verteilung der datenschutzrechtlichen Verantwortlichkeit zwischen den beteiligten Institutionen.

Zum Ende des Berichtszeitraums war – da die Bundestagswahl vorüber und die Bildung einer neuen Bundesregierung absehbar war – wieder eine erhöhte Dynamik im Verfahren erkennbar. So richtete

5 Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz), BGBl. I Nr. 14 vom 6. April 2021, S. 591.

das Bundesministerium des Innern und für Heimat Anfang Dezember 2021 das „Forum Registermodernisierung“ aus. Weitere Beratungen sind geplant.

# 2 SORMAS – Kontaktverfolgung in der Corona-Pandemie

Wie schon im letzten Jahr bestimmte die Corona-Pandemie auch in diesem Berichtszeitraum einen Großteil unserer Tätigkeit. Ein wesentlicher Schwerpunkt war dabei die Verarbeitung der Daten infizierter Personen im Rahmen der Kontaktnachverfolgung. Gemäß §§ 25, 28a Infektionsschutzgesetz sind die Gesundheitsämter mit dieser Aufgabe betraut. Sie sind demzufolge Verantwortliche im Sinne von Artikel 4 Nummer 7 Datenschutz-Grundverordnung (DS-GVO) und müssen die datenschutzrechtlichen Anforderungen erfüllen. Um eine Vereinheitlichung der Kontaktnachverfolgung zu erreichen und die Gesundheitsämter, die laut Medienberichten bereits zu Beginn der Pandemie Kapazitätsprobleme hatten, zu unterstützen, rief das Bundesministerium für Gesundheit das Forschungsprojekt SORMAS ÖGD ins Leben. Kern des Projekts war die Anpassung der Software SORMAS X durch das Helmholtz-Zentrum für Infektionsforschung an die Bedürfnisse des Öffentlichen Gesundheitsdienstes. SORMAS[6] (Surveillance Outbreak Response Management and Analysis System) dient dem Management und der Analyse von Infektionsausbrüchen, wie beispielsweise COVID-19. Die Software wurde seit dem Jahr 2014 im Zuge der Ebola-Bekämpfung in Westafrika entwickelt.

## 2.1 Erste Phase: Projektbegleitung durch unsere Behörde

Bereits zum Ende des vorherigen Berichtjahres erfuhren wir im Kontext der Anfrage eines Gesundheitsamtes, dass das Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz am 5. November 2020 im Rahmen seiner Fachaufsicht den Einsatz von SORMAS in allen brandenburgischen Gesundheitsämtern angewiesen

6 Zur besseren Lesbarkeit wird im Folgenden nicht mehr zwischen den Versionen unterschieden.

hatte. Auch die Konferenz der Bundeskanzlerin und der Ministerpräsidentinnen und Ministerpräsidenten der Länder empfahl im November 2020 den flächendeckenden Einsatz von SORMAS.

Im Austausch mit den Kolleginnen und Kollegen der anderen Bundesländer und des Bundesbeauftragen für den Datenschutz und die Informationsfreiheit erfuhren wir anschließend, dass die bislang vorliegende Dokumentation zu SORMAS unvollständig war und einen mangelhaften Reifegrad hatte. Entsprechend haben wir noch im Dezember 2020 das brandenburgische Gesundheitsministerium auf die schwerwiegendsten datenschutzrechtlichen Mängel hingewiesen und um Intervention gegenüber dem Bundesgesundheitsministerium und dem Helmholtz-Zentrum für Infektionsforschung gebeten. Nachdem uns die Dokumentation Anfang Januar 2021 zugänglich gemacht wurde, sind uns u. a. fehlende oder unklare Ausführungen zu den Datenflüssen, zum Berechtigungskonzept, zu kryptographischen Verfahren, zu den rechtlichen Grundlagen für die Datenverarbeitung, dem Löschkonzept und den Schnittstellendokumenten aufgefallen. Es bestanden insofern ernsthafte Zweifel, ob die Verantwortlichen im Land die Anforderungen von Artikel 5 Absatz 2 DS-GVO zur Rechenschaftspflicht erfüllen und die Einhaltung der Grundsätze der Datenverarbeitung bei der Nutzung von SORMAS hätten nachweisen können.

Vor dem Hintergrund der hohen Belastung der Gesundheitsämter in der Pandemie und ihrer begrenzten Möglichkeiten, den genannten Mängeln abzuhelfen, erschien es uns zielführend, einem Lösungsvorschlag des Bundesbeauftragten zu folgen: Er bot an, die Rückmeldungen der Datenschutzaufsichtsbehörden zur Dokumentation von SORMAS zu bündeln und weiterzuleiten. Im Anschluss sollte das Helmholtz-Zentrum für Infektionsforschung eine verbindliche Frist zur Behebung der Mängel und zur Fertigstellung der Dokumentation benennen. Auch sollte die Dokumentation so gestaltet werden, dass die Gesundheitsämter diese einfach übernehmen und erforderlichenfalls auf ihre eigenen Bedürfnisse anpassen können (z. B. durch das Ergänzen von Vorlagen für lokale Teilkonzepte). Im Gegenzug würden die Aufsichtsbehörden dem Betrieb von SORMAS unter Vorbehalt und temporär zustimmen.

Mit der Annahme dieses Vorschlags übermittelte das Bundesgesundheitsministerium den Aufsichtsbehörden im Februar 2021 auch einen Terminplan mit den Fristen zur Beseitigung der festgestellten Mängel durch das Helmholtz-Zentrum. Manche Fristen waren zu diesem Zeitpunkt bereits abgelaufen, aber spätestens für den 24. Juni 2021 war die Fertigstellung aller Dokumente geplant. Allerdings verbesserte sich die Situation auch im weiteren Projektverlauf nicht entscheidend: die erstellten Dokumente hatten zum Großteil einen ungenügenden Reifegrad; sie enthielten oft Platzhalter oder kopierte Textpassagen aus Normen und Standards, welche an sich zwar zutreffend, jedoch ohne Ausführungen zur Umsetzung unzureichend waren. Auch waren einige Dokumente wie z. B. die Datenschutz-Folgenabschätzung methodisch derart unausgereift, dass diese vollständig zu erneuern waren. Des Weiteren deutete sich in einigen Punkten bereits an, dass Mängel auch an der Implementierung der Software vorlagen. Dieser Zustand änderte sich auch nicht bis zum Auslaufen der von den Projektverantwortlichen selbst gesetzten Fristen.

## 2.2 Zweite Phase: Die SORMAS-Arbeitsgruppe

Parallel regte der Bundesbeauftragte die Gründung einer eigenen Arbeitsgruppe zu Datenschutzfragen im Zusammenhang mit SORMAS an. Hintergrund war die Rückmeldung des Helmholtz-Zentrums für Infektionsforschung, wonach datenschutzrechtliche Detailfragen den zeitnahen Abschluss des Projekts immer wieder hinauszögern würden. Entsprechend fanden ab Juli 2021 monatliche Beratungen von Vertretern einiger Datenschutzaufsichtsbehörden (zu denen auch wir gehörten), des Helmholtz-Zentrums, dessen Projektpartnerinnen und -partnern und teilweise des Bundesgesundheitsministeriums statt. Wie schon zu Beginn des Jahres verzichteten wir darauf, formal in aufsichtsrechtlichen Verfahren gegen die Verantwortlichen für die Datenverarbeitung mit SORMAS im Land Brandenburg vorzugehen und strebten stattdessen an, zentral Verbesserungen für alle teilnehmenden Behörden zu erreichen.

Zu den wesentlichen Erfahrungen, die wir im weiteren Projektverlauf machen mussten, und den zum Ende des Berichtszeitraums weiter bestehenden Mängeln gehören insbesondere:

- Nichteinhaltung selbstgesetzter Fristen: Das ursprüngliche Ziel der Arbeitsgruppe bestand in der Behebung der Mängel und Fertigstellung der Dokumentation zu SORMAS im Rahmen von durch das Helmholtz-Zentrum selbst gesetzten großzügigen Fristen. Im Verlauf des Projekts wurden diese immer wieder verlängert. Als Begründung wurden im Wechsel zu hohe Anforderungen der Datenschutzaufsichtsbehörden, fehlende Zuarbeiten von anderen Projektteilnehmern oder eine Überlastung des Projektteams angegeben. Auch stand zeitweise die Auffassung im Raum, dass eine abschließende Dokumentation aufgrund der Dynamik des Projekts gar nicht möglich sei. Als letzte Frist ist aktuell das Ende des 1. Quartals 2022 festgelegt. Somit wäre SORMAS in brandenburgischen Gesundheitsämtern auf Weisung des Gesundheitsministeriums mehr als ein Jahr in einem nicht rechtskonformen Zustand im Einsatz.

- Erweiterung der Verarbeitungszwecke und unzureichende Rechtsgrundlagen: Zunächst wurde kommuniziert, SORMAS werde lediglich für die Kontaktnachverfolgung eingesetzt. Hierauf bezog sich auch die temporäre Zustimmung unter Vorbehalt für den Betrieb, die seitens der Aufsichtsbehörden ausgesprochen wurde. Nachdem die Arbeitsgruppe sich in ersten Treffen auf ca. 50 für die Kontaktnachverfolgung erforderliche Datenfelder geeinigt hatte, wurde dies im späteren Projektverlauf bestritten. Mittlerweile sind bis zu 548 Datenfelder vorgesehen. Diese sollen auch eine Datenübermittlung aus SORMAS an das wesentlich umfassendere Deutsche Elektronische Melde- und Informationssystem für den Infektionsschutz (DEMIS) sowie eine Nutzung der Daten für Forschungszwecke ermöglichen. Allerdings sind die aktuell angeführten Rechtsgrundlagen der Verarbeitung aus dem Infektionsschutzgesetz für eine Erweiterung der Verarbeitungszwecke auf Forschungsfragen nicht hinreichend.

- Fehlende Dokumente: Weiterhin mussten wir feststellen, dass manche Querverweise in der Dokumentation zu Unterlagen führten, die nicht Projektbestandteil waren oder wegen Sicherheitsbedenken den Aufsichtsbehörden zunächst nicht zur Prüfung bereitgestellt wurden. So ließ das Helmholtz-Zentrum gegen Ende 2020 einen Penetrationstest für die SORMAS-Umgebung durchführen und verwies mehrfach auf diesen, um die Sicherheit des Verfahrensbetriebs im Auftrag der Gesundheitsämter nachzuweisen. Trotz mehrmaliger Aufforderung wurden die Ergebnisse dieses und eines aktuelleren Tests den Aufsichtsbehörden erst gegen Ende des Berichtszeitraums übermittelt.

- Inhaltlich unzureichende Dokumente: Zwar erhöhte sich im Projektverlauf der Umfang der Dokumentation, jedoch war dies nicht mit einer Verbesserung ihrer Qualität verbunden. Zum Teil bestanden Dokumente weiter aus Anforderungsblöcken, die nahezu vollständig aus Normen und Standards kopiert wurden, jedoch keine eigenen Inhalte zur konkreten Umsetzung im Projekt lieferten. Auch sind nach wie vor Dokumente mit vielen Platzhaltern zu noch ausstehenden Zuarbeiten versehen. Bereits mehrfach geforderte Beschreibungen zu Datenflüssen (z. B. in Form von Sequenzdiagrammen) wurden nicht geliefert. Die einzigen Darstellungen hierzu existieren in einem Teil der Schnittstellendokumentation, wobei wichtige Aspekte wie z. B. die Authentifizierung von Entitäten, der Schlüsselaustausch oder die konkret übermittelten Daten ausgespart oder deutlich zu oberflächlich dargestellt werden. Festzustellen war auch, dass in Dokumenten oftmals zwar an den Punkten gearbeitet wurde, zu denen Rückmeldungen der Datenschutzaufsichtsbehörden vorlagen, jedoch andere noch offene Teile ausgelassen wurden. Auch erwies sich, dass für Dokumente zum Teil voreilig der Status „fertig“ gesetzt wurde.

- Ausstehende Implementierungen: Bei der Prüfung der Unterlagen zu SORMAS ergaben sich Hinweise darauf, dass die aktuelle Implementierung des Verfahrens nicht vollständig datenschutzkonform ist. So finden sich z. B. im Entwurf des Pseudonymisierungs- und Anonymisierungskonzepts lediglich Platzhalter zu der Frage, welche Daten für Forschungszwecke anonymisiert

werden müssten. Der aktuelle Entwurf des Löschkonzeptes wiederum enthält die Aussage, dass eine Einschränkung der Datenverarbeitung durch betroffene Personen zwar erforderlich, gegenwärtig aber nicht möglich ist.

- Nutzung von SORMAS zur langfristigen Aufbewahrung: Auch die Frage der Löschung und Aufbewahrung der personenbezogenen Daten wurde in der Arbeitsgruppe erörtert. Wegen unterschiedlicher landesspezifischer Regelungen und einem erheblichen Mehraufwand bei der Implementation, falls diese Berücksichtigung fänden, wurde abgesprochen, SORMAS als reines Produktivsystem einzusetzen. Im späteren Projektverlauf wurde diese Absprache stillschweigend übergangen und SORMAS wieder als Aufbewahrungs- und Produktivsystem aufgefasst. Dies kann jedoch die Gesundheitsämter vor erhebliche Probleme stellen, die Aufbewahrungsfristen von bis zu 10 Jahren umzusetzen: Gegenwärtig wird SORMAS auf einer Cloud-Infrastruktur bei einem Dienstleister im Rahmen einer Auftragsverarbeitung betrieben. Deren Finanzierung ist jedoch zurzeit nur bis Ende 2022 gesichert. Damit die Gesundheitsämter auch ihren Verpflichtungen zur Aufbewahrung nachkommen können, wäre es zwar möglich, SORMAS als lokale Software zu betreiben. Diese Variante setzt allerdings erhebliches Fachwissen voraus. Im Übrigen wären auch der Support und die Nachbesserung der Software z. B. bei Sicherheitsmängeln voraussichtlich nicht gewährleistet.

### 2.3 Dritte Phase: weiteres Vorgehen

Alle aufgeführten Kritikpunkte der Datenschutzaufsichtsbehörden sind dem Helmholtz-Zentrum für Infektionsforschung direkt bzw. den Projektpartnerinnen und -partnern im Dialog oder schriftlich übermittelt worden. In den meisten Fällen hatte dies zwar die Zusage der Verbesserung und Abstellung der Mängel zur Folge, in großen Teilen ist eine solche aber noch nicht erfolgt oder erst für die Zukunft geplant. Wir haben als Konsequenz aus den unzureichenden Projektfortschritten während des vergangenen Jahres unsere Mitarbeit in der Arbeitsgruppe – zumindest temporär – eingestellt.

Zusammenfassend müssen wir feststellen, dass unsere Entscheidung, das Helmholtz-Zentrum und die anderen Projektvertreter zu beraten, nicht mit einem Erfolg verbunden war. Dies steht im Widerspruch zu anderen Projekten, in denen wir zumeist sehr positive Ergebnisse mit einem konstruktiv beratenden Ansatz erzielen konnten. Bedauerlicherweise hatten hierunter auch andere Verantwortliche im Land Brandenburg zu leiden, die sich an uns mit der Bitte um eine datenschutzrechtliche Beratung und Begleitung ihrer Projekte wandten, wegen fehlender Ressourcen unserer Dienststelle jedoch nicht zum Zuge kamen.

## Erleichterung für Gesundheitsämter nicht geglückt

Nach unseren Erfahrungen im Projekt ist nicht nachvollziehbar, dass die Gesundheitsämter zum Einsatz von SORMAS als einem nicht vollständig datenschutzkonformen Produkt gedrängt wurden. Einige Ämter äußerten uns gegenüber, dass sie zuvor bereits gut funktionierende Lösungen zur Kontaktnachverfolgung genutzt hatten und der Umstieg auf SORMAS einen signifikanten Mehraufwand (mitten in der Pandemie) ohne hinreichenden Mehrwert gegenüber der vorherigen Lösung verursacht hätte. Auch für die Datenübermittlung an das Robert-Koch-Institut wären etablierte Lösungen verfügbar gewesen, deren Entwicklung und Betrieb vom Bundesbeauftragten umfassend datenschutzrechtlich begleitet wurden.

Nach Ablauf der letzten uns bekannten, selbstgesetzten Fristen des SORMAS-Projektteams zur Fertigstellung aller Nachweise, die für einen datenschutzkonformen Einsatz des Verfahrens erforderlich sind, werden wir auf die Verantwortlichen im Land Brandenburg zugehen und datenschutzrechtliche sowie technische Prüfungen vornehmen. Wegen seiner Weisung an die Gesundheitsämter, SORMAS einzusetzen, werden wir dabei auch das Ministerium selbst in die Pflicht nehmen. Da es im vorliegenden Fall über die Mittel der Datenverarbeitung (mit)entschieden hat, ist es unserer Ansicht nach gemäß der Definition der Datenschutz-Grundverordnung selbst als Verantwortlicher zu qualifizieren.

# 3 Verarbeitung von Daten aus dem Luca-System zur Kontaktnachverfolgung

Im Frühjahr 2021 schloss das Land Brandenburg einen Kooperationsvertrag mit der Berliner culture4life GmbH zur Nutzung des Luca-Systems. Das von dem genannten Unternehmen betriebene digitale System sollte zum einen die Erhebung von Kontaktdaten in der Corona-Pandemie erleichtern. Hierzu waren Betreiberinnen und Betreiber von gastronomischen Einrichtungen, Beherbergungsstätten, Sportanlagen, Einrichtungen des Gesundheits- und Sozialwesens sowie zur Erbringung körpernaher Dienstleistungen, Veranstalterinnen und Veranstalter und andere nach der damals geltenden Eindämmungsverordnung des Landes verpflichtet. Vor dem Einsatz des Luca-Systems nutzten sie zur Kontaktdatenerhebung in der Regel Papierformulare.[7] Diese Praxis sollte nun durch den Austausch von QR-Codes per Mobiltelefon und die zentrale Speicherung von Anwesenheitsinformationen bei der Luca-Betreiberin abgelöst werden.

Zum anderen war geplant, die zuständigen Gesundheitsämter durch die elektronische Übermittlung der Anwesenheitsnachweise mittels Luca-System in die Lage zu versetzen, die Kontakte von Personen mit einer bestätigten COVID-19-Infektion effektiv nachzuverfolgen. Im Zusammenhang mit dem Vertragsabschluss mit der culture4life GmbH änderte die Landesregierung die entsprechende Verordnung und ließ die Erhebung der Kontaktdaten auch in elektronischer Form – zum Beispiel mittels einer speziellen Anwendungssoftware (hier: der Luca-App) – unter der Voraussetzung zu, dass die erhobenen Daten unverzüglich dem zuständigen Gesundheitsamt zur Verfügung gestellt werden können.

Da insgesamt 13 Bundesländer Kooperationsverträge mit der Betreiberin des Luca-Systems abgeschlossen hatten und darüber hinaus auch andere technische Lösungen zur Kontaktnachverfolgung bundesweit eingesetzt wurden, befasste sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) bereits frühzeitig mit dem Thema. Sie verabschiedete hierzu im Frühjahr des Berichtszeitraums meh-

7 Siehe A IV 5 sowie Tätigkeitsbericht Datenschutz 2020, A I 1, A I 2 und A I 3.

rere Stellungnahmen, die eine entsprechende Entschließung mit allgemeinen datenschutzrechtlichen Forderungen, welche aus dem Vorjahr stammte, ergänzten und hinsichtlich des Luca-Systems präzisierten. Darüber hinaus veröffentlichte die Konferenz eine Orientierungshilfe, in der die datenschutzrechtlichen Voraussetzungen sowie technische und organisatorische Maßnahmen beschrieben werden, die bei der Entwicklung und dem Betrieb von digitalen Diensten zur Kontaktnachverfolgung zu berücksichtigen sind. Alle Dokumente können in unserem Internetangebot abgerufen werden.

### 3.1 Gespräche mit dem Gesundheitsministerium

Wegen des Sitzes der culture4life GmbH im Land Berlin ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit für die datenschutzrechtliche und technische Prüfung des Luca-Systems sowie die Kontrolle des Betreiberunternehmens zuständig. Unsere Beratungs- und Kontrolltätigkeit erstreckte sich ausschließlich auf Verantwortliche im Land Brandenburg. Insbesondere strebten wir an, mit dem Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz sowie ausgewählten Gesundheitsämtern einheitliche Vorgaben und Musterdokumente für die Nutzung der Daten aus dem Luca-System abzusprechen bzw. zu erarbeiten (z. B. für Regelungen, Vorgehensweisen und datenschutzrechtlich erforderliche Unterlagen). Das Ministerium hätte diese anschließend im Rahmen seiner Aufsicht allen 18 brandenburgischen Gesundheitsämtern zur Anpassung an die jeweils lokalen Besonderheiten zukommen lassen können. Unser Ziel war, die in der Pandemie ohnehin stark beanspruchten Ämter durch zentrale Vorgaben und Hilfen zu unterstützen und möglichst wenig zusätzlich zu belasten.

In diesem Zusammenhang führten wir im Frühjahr des Berichtszeitraums mehrere Gespräche mit dem Gesundheitsministerium. Es hatte den o. g. Kooperationsvertrag für das Land unterzeichnet und ermöglichte damit die Nutzung des Luca-Systems sowohl durch die zur Kontaktdatenerhebung Verpflichteten als auch durch die Gesundheitsämter im Rahmen der Kontaktnachverfolgung. Wir informierten das Ministerium insbesondere über die Haltung der Datenschutzkonferenz zum Luca-System und die von ihr veröffentlichten

Dokumente. Weiterhin machten wir es auf die Einhaltung der datenschutzrechtlichen und technischen Anforderungen der Datenschutz-Grundverordnung (DS-GVO) und des Brandenburgischen Datenschutzgesetzes (BbgDSG) in den Gesundheitsämtern aufmerksam, wenn dort Daten aus dem Luca-System zur Kontaktnachverfolgung erhoben und weiterverarbeitet werden. Wir brachten auch zum Ausdruck, dass das Ministerium nach unserer Auffassung eine koordinierende Funktion hinsichtlich der Erarbeitung der o. g. zentralen datenschutzrechtlichen Vorgaben einnehmen sollte.

Darüber hinaus wiesen wir das Gesundheitsministerium auf unsere grundsätzlichen Bedenken hinsichtlich des Luca-Systems hin. Immerhin hatten zu diesem Zeitpunkt IT-Sicherheitsexpertinnen und -experten, Forscherinnen und Forscher sowie andere Interessierte Sicherheitslücken im System identifiziert und nachgewiesen, dass eine missbräuchliche Nutzung zumindest zeitweise möglich war. Auch die Berliner Beauftragte für Datenschutz und Informationsfreiheit stand als Aufsichtsbehörde in engem Kontakt mit dem Betreiberunternehmen und versuchte, mehrere sicherheitstechnische Verbesserungen zu erreichen. Darüber hinaus war für uns auch die grundsätzliche Eignung des Luca-Systems für die damit verfolgten Zwecke fraglich. Zum einen konnten durch die Ausnutzung von Sicherheitslücken „unechte“ Kontaktdaten hinterlegt werden, die eine geregelte Kontaktverfolgung durch Gesundheitsämter verkomplizierten. Zum anderen war klar, dass mit steigenden Infektionszahlen auch die Zahl der infizierten Personen zunimmt, die von den Gesundheitsämtern kontaktiert und gebeten werden müssen, die Historie ihrer Besuche in Gaststätten, Sporteinrichtungen und bei anderen zur Kontaktdatenerhebung Verpflichteten im Luca-System freizugeben. Da erst im Anschluss bei den Verpflichteten jeweils die Daten der Kontaktpersonen Infizierter ermittelt und diese dann selbst über eine mögliche Infektion informiert werden können, sahen wir eine erhebliche Zeitverzögerung, die das Ziel der Kontaktverfolgung, nämlich Infektionsketten schnell zu unterbrechen, konterkarierte. Wir wiesen das Ministerium stattdessen darauf hin, dass die Corona-Warn-App eine direkte Weitergabe der Information zwischen infizierter Person und deren Kontakten ohne Umweg über das Gesundheitsamt ermöglichte. Allerdings standen zu diesem Zeitpunkt die rechtlichen Regelun-

gen der Eindämmungsverordnung des Landes einer solchen datensparsamen Alternative entgegen.

Das Gesundheitsministerium hielt trotz unserer Bedenken an seiner grundsätzlichen Entscheidung zur Nutzung des Luca-Systems fest. Es informierte uns sowie die Gesundheitsämter, dass es im Ergebnis einer eigenen Prüfung keine datenschutzrechtlichen Bedenken habe. Insbesondere sah das Ministerium keine datenschutzrechtliche Verantwortung der Ämter bei der Nutzung des Luca-Systems zur Ermittlung von Kontaktdaten. Nach seiner Auffassung ändern sich auch die Datenverarbeitungsprozesse zur Kontaktnachverfolgung mit dem Erheben von Luca-Daten durch die Gesundheitsämter im Vergleich zur Verarbeitung von Meldungen Verpflichteter, die via E-Mail, Post oder Telefon eingehen, nicht. Daraus wurde geschlussfolgert, dass keine besonderen Sicherheitsmaßnahmen gemäß Artikel 32 DS-GVO für die Schnittstelle zum Luca-System, keine Fortschreibung der Datenschutz-Folgenabschätzung gemäß Artikel 35 DS-GVO und keine (erneute) Freigabe des Verfahrens gemäß § 4 Absatz 1 BbgDSG erforderlich waren.

## Schwierige Gespräche mit dem Gesundheitsministerium

Die Auffassung des Ministeriums teilen wir nicht: Wenn Gesundheitsämter das Luca-System aktiv nutzen, um infizierte Personen zu kontaktieren, deren Besuchshistorie zu ermitteln, die Verpflichteten zur Freigabe der Kontaktdaten aufzufordern und letztere zu entschlüsseln, um Kontakte der Infizierten nachzuverfolgen, sind sie hierfür im datenschutzrechtlichen Sinn nach Artikel 4 Nummer 7 DS-GVO Verantwortliche – genauso wie für die anschließende Weiterverarbeitung der Daten. Die Nutzung des Luca-Systems halten wir darüber hinaus für eine wesentliche Änderung des Verarbeitungsverfahrens zur Kontaktnachverfolgung, da eine zusätzliche, digitale Schnittstelle als Quelle der Erhebung personenbezogener Daten verwendet wird. Gemäß § 4 Absatz 1 BbgDSG erfordern auch wesentliche Änderungen von Verarbeitungsverfahren eine Freigabe. Zuvor ist zu untersuchen, ob die Änderungen eine Ergänzung der technischen und organisatorischen Sicherheitsmaßnahmen verlangen und ob die Datenschutz-Folgenabschätzung fortzuschreiben ist. Gerade die Überprüfung der Sicherheitsmaßnahmen erwies sich im vorliegenden Fall als zwingend, da im Kontext des Abrufs von Kontaktdaten

aus dem Luca-System durch die Ausnutzung einer Sicherheitslücke Schadcode auf die IT-Systeme der Gesundheitsämter hätte gelangen können. Die Lücke bestand für eine begrenzte Zeit, bis sie von dem Betreiberunternehmen des Luca-Systems geschlossen wurde.

Schriftlich sicherte uns das Ministerium zu, hinsichtlich der datenschutzrechtlichen und technischen Thematik weiter mit uns im Austausch bleiben und einzelne Fragen vertiefen zu wollen. Ergänzend betonte es, als zuständiges Ministerium auch die Koordinierung gegenüber den Gesundheitsämtern im Land zu übernehmen. Jedoch riss der Gesprächsfaden im Sommer des Berichtszeitraums ab – neben einem personellen Wechsel im Ministerium könnten dafür auch die zur Jahresmitte erheblich zurückgehenden Infektionszahlen ursächlich gewesen sein, womit eine dringende Befassung mit den offenen Punkten bei den Verantwortlichen aus dem Blick geriet.

## 3.2 Nutzung des Luca-Systems durch brandenburgische Gesundheitsämter

Lange Zeit lagen weder uns noch dem Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz genaue Informationen zur tatsächlichen Nutzung des Luca-Systems durch die Gesundheitsämter im Land Brandenburg vor. Wir initiierten deshalb eine entsprechende Umfrage – auch vor dem Hintergrund, uns eine bessere Unterstützung und Beratung bei der Erfüllung der datenschutzrechtlichen und technischen Anforderungen zu ermöglichen. Um die während der Pandemie ohnehin an der Belastungsgrenze operierenden Gesundheitsämter nicht unnötig zu beanspruchen, formulierten wir unsere Fragen in der Regel so, dass sie mit einem einfachen Ja oder Nein beantwortet werden konnten. Das Ministerium baten wir um die Versendung des Fragebogens und die statistische Auswertung der Antworten, da uns zunächst nicht vordergründig an der Identifizierung derjenigen Ämter gelegen war, die Mängel bei der Erfüllung der gesetzlichen Anforderungen aufwiesen.

Insgesamt können die Ergebnisse der Umfrage, welche uns gegen Ende des Berichtszeitraums erreichten, nicht zufriedenstellen. Von den insgesamt 18 Gesundheitsämtern im Land beteiligten sich 15 an

der Umfrage. 13 Ämter gaben an, eine Schnittstelle zur Nutzung des Luca-Systems eingerichtet zu haben, jedoch hatten nur vier von ihnen bereits Daten aus dem Luca-System zur Kontaktnachverfolgung verwendet bzw. dies versucht. Nur ein einziges Gesundheitsamt teilte mit, es habe in einem Fall Kontaktdaten aus dem Luca-System zur Kontaktnachverfolgung eingesetzt, allerdings sei dies ohne praktische Relevanz gewesen. Über 50 % der Befragten erklärten dagegen, durch das Luca-System keine Erleichterungen bei der Kontaktnachverfolgung zu erwarten. Sie planten dementsprechend auch nicht, das System dauerhaft einzusetzen.

Hinsichtlich der Beziehungen zur culture4life GmbH als Betreiberin des Luca-Systems gaben nur zwei Gesundheitsämter an, einen Auftragsverarbeitungsvertrag nach Artikel 28 DS-GVO mit dem Unternehmen geschlossen zu haben. Die anderen verwiesen in der Regel auf den Kooperationsvertrag, den das Ministerium für das Land unterzeichnet hatte. Dieser Vertrag erfüllt jedoch nach unserem Kenntnisstand nicht die gesetzlichen Anforderungen an eine Auftragsverarbeitung. Im Übrigen hätten wir es begrüßt, wenn das Ministerium im Wege einer Vereinbarung nach Artikel 26 DS-GVO eine datenschutzrechtliche Teilverantwortung für die Nutzung des Luca-Systems in den Gesundheitsämtern übernommen und z. B. einen Auftragsverarbeitungsvertrag mit der culture4life GmbH geschlossen hätte. Dies hätte auch die Möglichkeit geboten, die Anforderungen der Gesundheitsämter zur Anpassung und Weiterentwicklung des Luca-Systems landesweit zu koordinieren und die Kontrolle der Auftragsausführung durch die Systembetreiberin an einer Stelle zu konzentrieren.

Hinsichtlich der weiteren datenschutzrechtlichen Anforderungen gaben von den 15 an der Umfrage teilnehmenden Gesundheitsämtern nur drei an, das nach Artikel 30 DS-GVO zu führende Verzeichnis der Verarbeitungstätigkeiten um die Datenerhebung aus dem Luca-System ergänzt zu haben. Obwohl gut die Hälfte der Ämter mitteilte, technische und organisatorische Maßnahmen nach Artikel 32 DS-GVO zur Absicherung der Schnittstelle zum Luca-System umgesetzt zu haben, hatte nur ein Drittel diese auch dokumentiert und nur ein einziges Amt die entsprechenden Angaben im Verzeichnis der Verarbeitungstätigkeiten fortgeschrieben. Auch eine vollständige Dokumentation des Prozesses der Datenerhebung durch das

Luca-System sowie eine entsprechende Dienstanweisung lagen nur in einem Gesundheitsamt vor.

Nur zwei Ämter informierten in der Umfrage darüber, dass sie eine Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO für die Kontaktnachverfolgung unter Nutzung des Luca-Systems durchgeführt hätten. Ein weiteres gab an, die für die Verarbeitung personenbezogener Daten ohnehin im Gesundheitsamt bestehende Datenschutz-Folgenabschätzung um Luca-spezifische Teile ergänzt zu haben. Und kein Gesundheitsamt beantwortete die Frage, ob für die Erhebung von Kontaktdaten über das Luca-System (entweder eigenständig oder als wesentliche Änderung eines bestehenden Verfahrens) die Freigabe gemäß § 4 Absatz 1 BbgDSG erteilt wurde, mit einem Ja.

Die Ergebnisse der Umfrage zeigen deutlich auf, dass die große Mehrheit der Gesundheitsämter im Land keine hinreichenden datenschutzrechtlichen Vorkehrungen getroffen hat, um Kontaktdaten mit Hilfe des Luca-Systems zu erheben und weiterzuverarbeiten. Nach den gesetzlichen Vorschriften muss dies jedoch erfolgen, bevor erstmals personenbezogene Daten in einem Verfahren verarbeitet werden. Ob die Resultate dadurch beeinflusst sind, dass die übergroße Mehrheit bisher gar keine Daten aus dem Luca-System abgerufen und verarbeitet hat und dies auch nicht dauerhaft plant, wissen wir nicht.

## Falsche Sicherheit durch ungenutzte Daten

Allerdings sollte – nicht nur aus datenschutzrechtlicher Sicht – Folgendes zu denken geben: Viele Bürgerinnen und Bürger hinterlassen gemäß den Festlegungen der Eindämmungsverordnung des Landes ihre Daten bei den zur Kontaktdatenerhebung Verpflichteten, zu einem großen Teil geschieht dies über die Luca App. Sie erwarten dann konsequenterweise auch, dass sie im Fall einer bestätigten COVID-19-Infektion bei einer ihrer Kontaktpersonen schnell vom zuständigen Gesundheitsamt über das bestehende Risiko einer eigenen Infektion informiert werden. Wenn die Ämter die aufgrund der Verordnung gesammelten Daten jedoch nicht abrufen und zur Kontaktnachverfolgung nutzen, steht die Frage im Raum, ob diese Daten überhaupt rechtmäßig oder nur auf Vorrat gespeichert werden. Letzteres wäre rechtswidrig. Darüber hinaus

würden die nicht über eine Infektion in ihrem Umfeld informierten Personen sich in falscher Sicherheit wiegen und u. U. zumindest für einen gewissen Zeitraum selbst zur Verbreitung des Virus beitragen können.

Kurz nach Ablauf des Berichtszeitraums erreichte uns die Information, dass das Ministerium der Landesregierung empfielt, den Vertrag mit der culture4life GmbH zur Nutzung des Luca-Systems wegen Datenschutzbedenken und der geringen Verwendung durch die Gesundheitsämter zu kündigen. In der zu diesem Zeitpunkt gültigen Corona-Eindämmungsverordnung des Landes war die Nutzung der datensparsamen Corona-Warn-App zur Registrierung per QR-Code und Kontaktnachverfolgung bereits vorgesehen und somit möglich.

# 4 Werbe-Tracking: Prüfung eines brandenburgischen Medienunternehmens

Viele Anbieterinnen und Anbieter von Internetseiten verfolgen die Online-Aktivitäten der Nutzerinnen und Nutzer mit verschiedenen Techniken, um z. B. Informationen über deren Verhalten, ihre Interessen und Vorlieben zu gewinnen, zielgerichtet personalisierte Werbung anzeigen zu können sowie die Angebote zu optimieren.

## 4.1 Cookies und die Versteigerung von Werbeplätzen auf Webseiten

Eine der beliebtesten Techniken zum Erheben der Daten ist in diesem Zusammenhang die Verwendung von sogenannten Cookies. Cookies sind kleine Textdateien, die auf dem Gerät der Nutzerin bzw. des Nutzers im Webbrowser gespeichert werden. Sie können entweder vom Webserver an den Browser gesendet oder durch ein JavaScript-Programm erstellt werden, das automatisch beim Aufruf der Webseite startet. Die in den Cookies gespeicherten Informationen werden im Zuge des Datenverkehrs zwischen dem Webbrowser und dem Server der Webseite ausgetauscht. Werkzeuge wie Google Analytics speichern eine eindeutige Nutzerkennung (ID) im Cookie, sodass die Nutzerin bzw. der Nutzer bei weiteren Besuchen dieser oder anderer Webseiten, die ebenfalls Google Analytics implemen-

tiert haben, wiedererkannt werden kann. Solche Cookies haben in der Regel eine Lebensdauer von mehreren Monaten bis zu einigen Jahren. Diese Frist beginnt jedoch mit jedem Besuch der Webseite neu. Werden die Cookies nicht gelöscht, kann deshalb eine Nutzerhistorie über einen sehr langen Zeitraum erstellt werden, die weit über die Lebensdauer des zuletzt gesetzten Cookies hinausgeht, die ggf. in der Datenschutzerklärung der Webseite angegeben ist.

Cookies werden auch dazu verwendet, auf die Nutzerin oder den Nutzer zugeschnittene Werbung auszuspielen. Sehr viele Webseiten setzen in diesem Zusammenhang das sogenannte „Real Time Bidding“ (Echtzeitversteigerung) ein. Ruft eine Nutzerin bzw. ein Nutzer eine Webseite auf, die solche Techniken implementiert hat, findet im Hintergrund sofort eine Echtzeitversteigerung der Online-Werbeplätze auf der Webseite statt. Für diese Versteigerung werden die erfassten Daten der Nutzerin bzw. des Nutzers gemeinsam mit einer Gebotsanfrage an viele, ggf. Hunderte von Unternehmen übermittelt. Die Bieter der Versteigerung, also die Werbeanbieter, können nun entscheiden, ob und in welcher Höhe sie Gebote dafür abgeben, der Nutzerin bzw. dem Nutzer, basierend auf den Informationen, die sie oder er mit der Gebotsanfrage erhalten hat, zielgerichtet und in Echtzeit personalisierte Werbung anzeigen zu lassen. Es dauert weniger als eine Sekunde, bis die Werbeanzeige, die die Auktion gewonnen hat, auf der Webseite geladen ist.

Die Gebotsanfrage enthält in der Regel eine Vielzahl personenbezogener Informationen über die Nutzerin bzw. den Nutzer. Darin können der Standort, verschiedene individuelle Kennungen (z. B. Gerätekennung, Werbe-ID), konsumierte Webinhalte, das Alter und das Geschlecht der betroffenen Person enthalten sein. Außerdem können Teile des erstellten Nutzerprofils übermittelt werden, die beispielsweise Aufschluss über religiöse Überzeugungen oder politische Meinungen geben bzw. Daten zur Gesundheit oder zum Sexualleben enthalten.

Für die Verarbeitung dieser personenbezogenen Daten benötigen Verantwortliche von Webseiten eine Rechtsgrundlage. Sie können beispielsweise durch ein konform gestaltetes Cookie-Banner die Einwilligung der Nutzerin bzw. des Nutzers einholen. Die Gestaltung der Cookie-Banner ist sehr unterschiedlich und weist oft sogenann-

te „Nudging“-Techniken auf. Hierunter werden Maßnahmen verstanden, die geeignet sind, das Nutzungsverhalten entsprechend den Interessen der Anbieterinnen und Anbieter von Webseiten sowie der Werbetreibenden zu lenken und zu manipulieren. Beispiele sind die optische Hervorhebung der Zustimmungsoption durch Größe oder Farbe, die Verhinderung einer sofortigen Ablehnung durch Verlagerung auf die zweite Ebene oder die komplizierte Gestaltung des Cookie-Banners. Genervte Nutzerinnen bzw. Nutzer wählen dann jene Option, die ihnen spontan ins Auge sticht, um das lästige Banner möglichst schnell wegzuklicken. Häufig wird auch der Widerruf einer einmal erteilten Einwilligung durch ähnliche Methoden erschwert.

## 4.2 Vorbereitung einer koordinierten Prüfung der Aufsichtsbehörden

Aufgrund der deutlich zunehmenden Zahl an Beschwerden über die Datenverarbeitungen auf Webseiten im Zusammenhang mit dem Tracking für Werbezwecke schlossen sich Datenschutzaufsichtsbehörden aus 13 Bundesländern zusammen, um in einer koordinierten Prüfung die Webseiten verschiedener Medienunternehmen zu untersuchen. Auch unsere Dienststelle beteiligte sich daran.

Um die gemeinsame Prüfung des Einsatzes von Tracking-Werkzeugen auf Webseiten von Online-Medien vorzubereiten, stimmten sich die teilnehmenden Aufsichtsbehörden zuvor über das konkrete Vorgehen ab. Sie entwarfen in diesem Zusammenhang einen einheitlichen Fragebogen, der den Unternehmen übersandt wurde. Mit diesem Fragebogen wurden u. a. die eingesetzten Tracking-Methoden, die damit verbundenen Datenverarbeitungen, Datenflüsse zu (Werbe-) Partnerunternehmen sowie die Rechtsgrundlagen für die Datenverarbeitungen erfragt.

Damit die Antworten der Unternehmen einheitlich bewertet werden konnten, legten die Datenschutzaufsichtsbehörden auch einen Kriterienkatalog fest, der die datenschutzrechtlichen Anforderungen an Cookie-Banner spezifiziert. Nach Artikel 7 Datenschutz-Grundverordnung muss eine wirksame Einwilligung immer vor Beginn der Datenverarbeitung, in informierter Weise und unter Hinweis darauf,

dass sie jederzeit widerrufen werden kann, eingeholt werden. Zudem ist die Einwilligung freiwillig abzugeben. Hiervon kann im Kontext der Ausgestaltung des Cookie-Banners nur ausgegangen werden, wenn eine wirkliche Wahl besteht, der Datenverarbeitung zuzustimmen oder diese abzulehnen. Fehlt beispielsweise die eindeutige Ablehnungsmöglichkeit auf erster Ebene, gilt die Einwilligung als nicht freiwillig erteilt und ist damit unwirksam. Die Datenverarbeitung abzulehnen, darf somit keinen Mehraufwand gegenüber der Zustimmung bedeuten. Der Mehraufwand besteht dabei nicht nur darin, dass die betroffene Person, die eine Ablehnung äußern möchte, einmal mehr klicken muss als für die Zustimmung. Vielmehr müssen die weiteren Informationen und Einstellungsmöglichkeiten, mit denen sie auf einer zweiten Ebene des Einwilligungsdialoges konfrontiert wird, lesen, nachvollziehen und dann unter den weiteren Optionen die richtige auswählen. Dieser Mehraufwand ist ein spürbarer Nachteil für die Betroffenen.

Diese und weitere Kriterien zur Beurteilung der Rechtmäßigkeit der Datenverarbeitungen auf Webseiten fanden auch Einzug in die „Orientierungshilfe der Aufsichtsbehörden für die Anbieter:innen von Telemedien ab dem 1. Dezember 2021“, die in unserem Internetangebot abrufbar ist. Sie berücksichtigt, soweit möglich, bereits die aktuelle Rechtslage unter dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG).[8] Detaillierte Regelungen für Dienste zur Verwaltung erteilter Einwilligungen werden nach § 26 Absatz 2 TTDSG von einer noch durch die Bundesregierung unter Zustimmung des Bundestags und des Bundesrats zu erlassenden Rechtsverordnung getroffen.

### 4.3 Erste Ergebnisse der Prüfung in Brandenburg

Im Rahmen der koordinierten Prüfung der Webseiten von Medienunternehmen wählte die Landesbeauftragte ein ihrer Aufsicht unterliegendes Verlagshaus aus und sandte diesem den abgestimmten Fragebogen zur Beantwortung zu. Die hierauf folgende Auskunft brachte Aufschluss über den Einsatz von bis zu ca. 500 Cookies und

8 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien vom 23. Juni 2021, BGBl. I, S. 1982.

anderen Tracking-Mechanismen, die in einem Webangebot dieses Unternehmens zur Erstellung von Nutzerprofilen für Werbe- und Marketingzwecke verwendet wurden. Darüber hinaus wurde uns mitgeteilt, dass die nutzerspezifischen Daten an bis zu 150 eingebundene Partnerunternehmen übermittelt wurden. Dennoch hatte das Verlagshaus seinerzeit lediglich ein einfaches Hinweisbanner implementiert, das pauschal über den Einsatz von Cookies informierte.

Anlässlich unserer Prüfung nahm das Unternehmen Verbesserungen in dem geprüften Webangebot vor und verwendete eine sogenannte Consent Management-Plattform im Zusammenhang mit dem Cookie-Banner. Hierdurch sollten die Nutzerinnen und Nutzer über die Datenverarbeitung informiert und ihre Einwilligung eingeholt werden. Für die eingesetzte Consent Management-Lösung wurde auf ein Datenschutz-Gütesiegel verwiesen, das von einem dritten Unternehmen ausgestellt worden war und die Einhaltung der Anforderungen der Datenschutz-Grundverordnung belegen sollte. Die Lösung basierte auf dem technischen Standard des Transparency and Consent Framework (TCF) 2.0 des Branchenverbandes Interactive Advertising Bureau (IAB) Europe. Das implementierte Cookie-Banner enthielt neben der Option, alle Cookies zu akzeptieren, auf der ersten Ebene keine Möglichkeit, diese komplett abzulehnen. Stattdessen konnten Nutzerinnen und Nutzer eine Schaltfläche „Optionen“ auswählen, die auf der nächsten Bannerebene Einstellungen zu den Cookies ermöglichte oder erneut das Akzeptieren aller Datenverarbeitungen vorschlug.

Wir wiesen das Verlagshaus auf die oben beschriebenen Bewertungsmaßstäbe für die Gestaltung von Cookie-Bannern hin. Danach kann die Einwilligung in die Datenverarbeitung nur wirksam eingeholt werden, wenn die Möglichkeiten, sie zu erteilen oder abzulehnen, bereits auf der ersten Bannerebene gleichwertig dargestellt sind. Außerdem erging der Hinweis, dass der Einsatz einer Consent Management-Lösung, die die Festlegungen eines Branchenstandards einhält (hier: TCF 2.0 der IAB Europe), nicht von der datenschutzrechtlichen Verantwortlichkeit befreit. Die Verwendung des Standards allein bietet keine Gewähr, dass personenbezogene Daten tatsächlich rechtskonform verarbeitet werden.

Das Unternehmen fragte hierauf, ob eine geringfügige Abwandlung des Cookie-Banners – nämlich die Änderung der Bezeichnung der Schaltfläche „Optionen“ in „Einstellungen oder ablehnen“ – eine datenschutzgerechte Verarbeitung ermöglichen würde. Auch hier wiesen wir den Verantwortlichen darauf hin, dass diese Form des Einwilligungsdialoges ebenso zu einem spürbaren Nachteil und Mehraufwand für die betroffenen Personen führt und dazu dient, in treuwidriger Art und Weise Einfluss auf sie zu nehmen. Wir forderten erneut, eine Schaltfläche auf erster Ebene des Cookie-Banners einzurichten, mit die Nutzerinnen und Nutzer den Einsatz von einwilligungsbedürftigen Cookies und Tracking-Maßnahmen sowie die Einbindung von Drittdiensten ablehnen können.

## Maßgenschneiderte Werbung abwählbar?

In der Folge entschied sich das Verlagshaus dafür, in dem geprüften Webangebot nun das sogenannte PUR-Modell einzuführen. Die Nutzerin bzw. der Nutzer wird mit dieser Ausgestaltung des Cookie-Banners vor die Wahl gestellt, in das Tracking zu Werbezwecken einzuwilligen oder ein kostenpflichtiges Abonnement für die Nutzung der Webseiten abzuschließen und im Gegenzug von dem Werbe-Tracking verschont zu bleiben. Dieses Modell, welches immer mehr Medienunternehmen auf ihren Webseiten verwenden, wird zurzeit noch von den Datenschutzaufsichtsbehörden rechtlich geprüft. Da die Bewertung einer solchen Gestaltung von Webangeboten andauert, ist die Prüfung des brandenburgischen Unternehmens noch nicht vollständig abgeschlossen.

Hinzuweisen ist allerdings auf eine kurz nach dem Berichtszeitraum veröffentlichte Entscheidung der belgischen Datenschutzaufsichtsbehörde, die federführend für den Branchenverband IAB Europe und den Standard TCF 2.0 zuständig ist. Gemäß dieser Entscheidung liegen bei Datenverarbeitungen, die auf dem genannten Branchenstandard beruhen und für die der Verband verantwortlich ist, mehrere Rechtsverstöße vor – insbesondere hinsichtlich der Rechtsgrundlagen und der Transparenz der Datenverarbeitung im Zusammenhang mit Werbe-Tracking für betroffene Nutzerinnen und Nutzer. Die Entscheidung der belgischen Datenschutzaufsichtsbehörde ist mit den europäischen Kolleginnen und Kollegen abgestimmt und hat vo-

raussichtlich Konsequenzen für Cookie-Banner und personalisierte Online-Werbung in der gesamten Europäischen Union. Der Verband muss die gespeicherten personenbezogenen Daten löschen und das weit verbreitete und von vielen Unternehmen genutzte Framework nachbessern. Darüber hinaus wurde eine Geldbuße verhängt.

## II Datenschutzverstöße: Maßnahmen und Sanktionen

## 1 Schadsoftware im Webshop

Der Betreiber eines Webshops informierte uns über einen Datenschutzvorfall. Er teilte mit, dass es Kriminellen gelungen war, Schadsoftware in seine Verkaufsplattform einzuschleusen und hiermit die Kundendatenbank auszulesen. Als Beweis für den erfolgreichen Einbruch legten sie eine Kopie der Daten in einem definierten Verzeichnis auf dem Server ab. Um die Veröffentlichung der Kundeninformationen zu verhindern, sollte der Betreiber eine bestimmte Summe in der Kryptowährung Bitcoin zahlen. Falls keine Zahlung erfolgt, wurde darüber hinaus angedroht, weitere Schäden auf der Plattform zu verursachen – z. B. Kunden- und Kaufdaten zu manipulieren oder zu löschen.

**Kriminelle wildern in Kundendaten**

Von dem Vorfall betroffen waren nach Angaben des Unternehmens insgesamt über 76.000 Kundinnen und Kunden aus Deutschland und Österreich. Zu den personenbezogenen Daten, die ausgelesen werden konnten, gehörten neben Kontaktinformationen wie Name, Vorname, Anschrift und E-Mail-Adressen auch Benutzernamen und (verschlüsselte) Passwörter, die auf der Verkaufsplattform Verwendung fanden. Bei einem vollständigen Zugriff auf alle Daten des Webshops hätten potenziell über 725.000 Datensätze auch von Kundinnen und Kunden mehrerer anderer europäischer Staaten ausgelesen werden können. Der Betreiber erkannte das hohe Risiko für einen Identitätsmissbrauch und informierte alle Nutzerinnen und Nutzer über den Vorfall. Wegen der großen Anzahl geschah dies schrittweise.

Im Verlauf der Untersuchung der Datenschutzverletzung stellte sich schnell heraus, dass die Kriminellen eine spezielle Funktion der Verkaufsplattform ausnutzten. Mit dieser Funktion war es Kundinnen und Kunden möglich, eine Bilddatei auf die Plattform hochzuladen und so die gekauften Produkte persönlich zu gestalten. Die Angreiferinnen oder Angreifer verwendeten eine manipulierte Bilddatei, die auch ausführbaren Schadcode enthielt. Hierüber konnten sie die Daten aus der Kundendatenbank auslesen.

Das Unternehmen hatte es offenbar versäumt, die hochgeladenen Bilddateien der Kundinnen und Kunden sorgfältig daraufhin zu un-

tersuchen, ob dort ausführbarer Schadcode enthalten war und im Fall eines Treffers das Hochladen der Datei zu unterbinden. Darüber hinaus hätte das Unternehmen auch die Ausführung fremden Codes und die Ausleitung großer Datenmengen aus dem Webshop verhindern müssen. Beide Versäumnisse stellen Verstöße gegen die Regelungen der Datenschutz-Grundverordnung (DS-GVO) dar. Artikel 25 Absatz 1 DS-GVO verlangt vom Verantwortlichen, technische und organisatorische Sicherheitsmaßnahmen sowohl zum Zeitpunkt der Entscheidung über die Mittel der Verarbeitung personenbezogener Daten (hier also bei der Konzeption des Webshops) als auch bei der eigentlichen Verarbeitung (hier beim Betrieb des Webshops) zu treffen. Damit soll den Anforderungen der Verordnung entsprochen und die Rechte der betroffenen Personen geschützt werden. Artikel 32 Absatz 1 DS-GVO präzisiert diese Anforderungen und verlangt Maßnahmen, durch die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden.

Bei der Bestimmung der technischen und organisatorischen Maßnahmen sind u. a. die Risiken, die für die Rechte und Freiheiten betroffener Personen durch die Verarbeitung entstehen können, der Stand der Technik und die Implementierungskosten für den Verantwortlichen zu beachten. Festzustellen war, dass der Betreiber des Webshops im vorliegenden Fall die Risiken, die mit dem Hochladen von Dateien auf die Verkaufsplattform für die Sicherstellung der Vertraulichkeit und Integrität der Kundendaten verbunden waren, gar nicht oder nicht sorgfältig genug untersucht und im Ergebnis unterschätzt hatte. Ansonsten hätte ihm auffallen müssen, dass die Bereitstellung einer solchen Funktion Kriminelle geradezu anzieht, um die Plattform zu kompromittieren. Folgerichtig enthalten auch diverse Publikationen zu Sicherheitsmaßnahmen bei Webanwendungen die wichtige Forderung, von Nutzerinnen und Nutzern hochgeladenen Inhalten nicht zu vertrauen und sie stets auf Schadcode zu untersuchen. Dass eine solche Anforderung auch mit vertretbarem Aufwand umzusetzen ist, zeigt die Tatsache, dass der Betreiber im vorliegenden Fall innerhalb weniger Tage eine solche Funktion nachrüstete. Darüber hinaus überprüfte er die Konfiguration des Webshops hinsichtlich der Regelungen zur Ausführung von Code, tauschte alle (in-

ternen) Zugangs- und Verschlüsselungsschlüssel aus und überprüfte auch die Konfiguration der Firewall.

Im Ergebnis haben wir den Betreiber des Webshops nach Artikel 58 Absatz 2 Buchstabe b DS-GVO wegen der genannten Verstöße gegen die Verordnung verwarnt. Zuvor führten wir entsprechend den Regelungen zur Zusammenarbeit zwischen den europäischen Datenschutzaufsichtsbehörden gemäß Artikel 60 ff. DS-GVO eine Abstimmung mit denjenigen Behörden durch, die sich für diesen Fall bei uns als betroffene Aufsichtsbehörden gemeldet hatten. Gegen unseren Vorschlag, eine Verwarnung auszusprechen, gab es dabei keine Bedenken.

## 2 Recht auf Auskunft – Weiterleitung zwecklos

Auch im aktuellen Berichtszeitraum erhielten wir wieder eine Vielzahl an Beschwerden, wonach insbesondere Auskunfts- und Löschungsersuchen betroffener Personen nicht, nicht rechtzeitig oder inhaltlich nicht hinreichend bearbeitet wurde.

Das Recht auf Auskunft nach Artikel 15 Datenschutz-Grundverordnung (DS-GVO) stellt, im Zusammenspiel mit den Informationspflichten aus Artikel 13 und 14 DS-GVO, das zentrale, subjektive Datenschutzrecht dar. Es dient der Rechtmäßigkeitskontrolle und soll zunächst sicherstellen, dass sich die betroffene Person bewusst ist, ob sie betreffende Daten überhaupt verarbeitet werden. Sie soll erfahren können, welche konkreten Daten dies sind und für welche Zwecke diese durch wen und wie lange verarbeitet werden. Das Auskunftsrecht stellt vor diesem Hintergrund faktisch eine unverzichtbare Voraussetzung für die Ausübung weiterer datenschutzrechtlicher Ansprüche wie des Rechts auf Löschung, Berichtigung oder Widerspruch dar. Nur wenn die Betroffenen um die jeweilige Verarbeitung wissen, kann Transparenz erreicht und die Rechtmäßigkeit beurteilt werden.

In einem Fall begehrte die betroffene Person Auskunft gegenüber einem brandenburgischen Unternehmen, das selbstständig agiert und

Teil eines bundesweit tätigen Informationsdienstleisters ist. Es ist auch mit der Einziehung offener Forderungen betraut. Die betroffene Person erhielt zunächst ein Mahnschreiben des Verantwortlichen und nahm dies zum Anlass, bei diesem den Hintergrund der Mahnung zu erfragen, da ihr die geltend gemachte Forderung gänzlich unbekannt sei. Die betroffene Person wandte sich also unter Nennung der ihr genannten Inkasso-Nummer an das hiesige Unternehmen. Anstelle einer unverzüglichen, in jedem Falle jedoch innerhalb eines Monats, zu erfolgenden Information über die ergriffenen Maßnahmen – wie es Artikel 12 Absatz 3 DS-GVO im Grundsatz vorsieht – erhielt sie zunächst überhaupt keine Rückmeldung. Einen Monat nach Stellung des Auskunftsantrages erkundigte sich die betroffene Person telefonisch nach dem Stand, woraufhin ihr zwar der Eingang des Antrages bestätigt, im Übrigen jedoch knapp mitgeteilt wurde, dass das Unternehmen zur Erteilung der Auskunft nicht befugt sei. Sodann beschwerte sie sich bei uns.

Wir hörten das Unternehmen an und erläuterten die Rechtslage. Der Verantwortliche teilte in der Folge mit, dass man als Vertriebspartner innerhalb der Unternehmensgruppe mit einer Vielzahl von Anfragen betroffener Personen konfrontiert sei, die in der Sache jedoch von einem anderen Unternehmen der Gruppe beantwortet werden müssten. Auch das vorliegende Auskunftsersuchen, obgleich konkret auf die Inkassotätigkeit bezogen, sei offenbar in diese Richtung interpretiert worden, sodass eine eigene Recherche unterblieb.

Das verantwortliche Unternehmen sicherte schließlich zu, die mit der Bearbeitung von derartigen Anfragen betrauten Beschäftigten nochmals umfassend und detailliert zu diesem Thema zu schulen. Die Auskunft an die betroffene Person wurde letzten Endes noch erteilt.

Da uns bis zu diesem Zeitpunkt keine weiteren Beschwerden oder Verstöße des Verantwortlichen bekannt geworden sind, haben wir die förmliche Feststellung des Verstoßes gegen datenschutzrechtliche Bestimmungen als ausreichend angesehen und das Unternehmen nach Artikel 58 Absatz 2 Buchstabe b DS-GVO verwarnt.

Hervorzuheben bleibt noch, dass Verantwortliche in jedem Falle verpflichtet sind, auf Ersuchen betroffener Personen zu reagieren. Selbst wenn nach eingehender Recherche keine personenbezogenen Daten vorliegen sollten, ist dies in Form einer Negativauskunft mitzuteilen. Das rein schematische, oberflächliche Bearbeiten von Anfragen betroffener Personen oder Weiterleiten innerhalb der Unternehmensgruppe verbietet sich insoweit.

## 3 Veröffentlichung personenbezogener Daten in Schaukästen eines Vereins

Im Berichtszeitraum beschwerte sich ein Mitglied eines Garagenvereins darüber, dass der Vorstand seine vertrauliche Korrespondenz sowie andere Dokumente in Schaukästen auf dem Vereinsgelände veröffentlicht hatte. Das Vereinsmitglied reagierte nicht auf postalisch zugestellte, offizielle Schreiben. Daraufhin veröffentlichte der Vorstand diese einfach über die Schaukästen. Alle anderen Mitglieder sowie Gäste des Vereins konnten so nicht nur Name und Wohnanschrift des Adressaten zur Kenntnis nehmen, sondern auch Einzelheiten des dem Schriftwechsel zu Grunde liegenden Sachverhalts. Hierüber beschwerte sich das Vereinsmitglied zunächst beim Vorstand, da es sich an den Pranger gestellt fühlte. Die Aufforderung, das Schreiben aus den Schaukästen zu entfernen, wurde vom Vorstand jedoch genauso dort veröffentlicht wie die eigene Reaktion. Davon waren zusätzlich auch Daten dritter Personen betroffen. Als Begründung gab der Verein u. a. an, dass eine solche „offene“ Korrespondenz sowohl von der Vereinssatzung als auch von einem Mitgliederbeschluss umfasst sei.

Das Offenlegen personenbezogener Daten in einem Schaukasten stellt eine Verarbeitung im Sinne der Datenschutz-Grundverordnung (DS-GVO) dar. Hierfür bedarf es entweder einer Einwilligung der betroffenen Person oder einer anderen Rechtsgrundlage nach Artikel 6 DS-GVO. In dem zu prüfenden Verfahren fehlte es an einem solchen Erlaubnistatbestand.

Weder eine Vereinssatzung noch ein Mitgliederbeschluss stellen eine wirksame Einwilligung im Sinne des Artikel 6 Absatz 1 Satz 1

Buchstabe a DS-GVO dar. Die pauschale Einwilligungsklausel in einer Satzung, die sich nicht auf bestimmte Datenverarbeitungszwecke beschränkt, ist unwirksam. Grundsätzlich kann nur die betroffene Person ihre Einwilligung „für einen oder mehrere bestimmte Zwecke“ abgeben. Eine solche Einwilligung hatte der Beschwerdeführer nicht erteilt.

Die Offenlegung personenbezogener Daten des Betroffenen im Vereinsschaukasten war auch nicht vom Mitgliedschaftsvertrag gemäß Artikel 6 Absatz 1 Satz 1 Buchstabe b DS-GVO gedeckt. Es fehlte bereits an dem Tatbestandsmerkmal der Erforderlichkeit der Veröffentlichung zur Vertragserfüllung. Diese läge vor, wenn die konkrete Art und Weise der Verarbeitung geeignet wäre, den mit der Datenverarbeitung verfolgten Zweck zu erreichen, und es keine andere, weniger in die Grundrechte und Grundfreiheiten eingreifende Möglichkeit gäbe (sogenanntes milderes Mittel). Soweit eine Reaktion eines Vereinsmitglieds auf postalisch verschickte Schreiben ausgeblieben ist, hätte der Verein unter Nutzung einer Postzustellungsurkunde einen wirksamen Zugang von zum Beispiel Rechnungen oder Kündigungen sicherstellen können.

Mangels Erforderlichkeit konnten die beschriebenen Datenverarbeitungen auch nicht auf Artikel 6 Absatz 1 Satz 1 Buchstabe f DS-GVO gestützt werden, weil sie nicht zur Wahrung berechtigter Interessen des Vereins oder Dritter erforderlich war. Insoweit kam es hier gar nicht mehr auf eine Abwägung der Interessen des Vorstandes mit denen des Mitglieds an.

Wir haben in diesem Verfahren gegen den Verein eine Verwarnung gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO ausgesprochen

# 4 Bericht der Bußgeldstelle

## 4.1 Unzulässige Weitergabe von Behandlungsdaten Minderjähriger

Ein Vater wandte sich an uns, weil die behandelnde Ärztin seiner minderjährigen Kinder zahlreiche Daten an eine zentrale Abrechnungsstelle übermittelt hatte. Bei den zur Rechnungstellung weitergegebenen Daten handelte es sich um Name und Anschrift, Geburtsdatum, Krankenversichertennummer, Datum des Arztbesuches, erbrachte ärztliche Leistungen sowie die gestellten Diagnosen der minderjährigen Patienten.

Die genannten Daten der ärztlichen Heilbehandlung stellen Gesundheitsdaten im Sinne des Artikel 9 Datenschutz-Grundverordnung (DS-GVO) dar. Gemäß Artikel 4 Nummer 15 DS-GVO sind Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Für die Übermittlung an die Abrechnungsstelle war jedoch keine Rechtfertigungsnorm des Artikel 9 Absatz 2 DS-GVO erfüllt.

Mangels einer anderen gesetzlichen Erlaubnisgrundlage kann die Übermittlung von Patientendaten zum Zweck der Abrechnung an eine externe Abrechnungsstelle nur auf Grundlage einer Einwilligungserklärung nach Artikel 9 Absatz 2 Buchtstabe a DS-GVO erfolgen. Dies wurde auch durch die siebente Satzung zur Änderung der Berufsordnung der Landesärztekammer Brandenburg vom 27. August 2020 klargestellt. Nach § 12 Absatz 2 dieser Ordnung ist die Übermittlung von Daten an Dritte zum Zweck der Abrechnung nur zulässig, wenn die Patientin oder der Patient in die Übermittlung der für die Abrechnung erforderlichen Daten nachweisbar eingewilligt hat.

Eine Einwilligung für die Datenübermittlung an die zentrale Abrechnungsstelle hatten die Sorgeberechtigten der minderjährigen Patienten jedoch nie erteilt. Von der unzulässigen Datenübermittlung

waren Kinder betroffen, die nach dem allgemeinen gesetzgeberischen Willen besonders zu schützen sind. Daneben bezogen sich die Datenschutzverstöße auf besondere Kategorien von Daten, nämlich Gesundheitsdaten, die vom Gesetzgeber ebenfalls als besonders schützenswert eingestuft wurden. Deshalb war die Ahndung mit einem Bußgeld geboten.

Die Ärztin hat das festgesetzte Bußgeld in dreistelliger Höhe akzeptiert.

### 4.2 Die ungewollte Filmrolle

Infolge einer Beschwerde erlangten wir davon Kenntnis, dass der Geschäftsführer eines Unternehmens, das Leistungen im Garten- und Landschaftsbau anbietet, eine Videoaufnahme fertigte, auf der der Beschwerdeführer bei der Durchführung von Probearbeiten zu erkennen war. Noch am selben Abend kontaktierte er den Geschäftsführer und bat um die Löschung des Videos und den Verzicht auf die beabsichtigte Veröffentlichung der Aufnahmen im Internet.

Der Geschäftsführer ignorierte die Geltendmachung der Betroffenenrechte durch den Beschwerdeführer und veröffentlichte das Video, das im Zeitraffermodus die Erstellung einer Teichanlage zeigte. Zu Werbezwecken publizierte er die Aufnahmen sowohl im sozialen Netzwerk Facebook als auch auf der Online-Plattform YouTube und der Webseite des Unternehmens. Die Einstellungen erlaubten jedermann einen Zugriff auf das Video.

Im aufsichtsrechtlichen Verfahren klärten wir den Verantwortlichen darüber auf, dass das Video in jedem Fall zu löschen war. Dies galt selbst dann, wenn der Beschwerdeführer zuvor eine wirksame Einwilligung im Sinne von Artikel 6 Absatz 1 Satz 1 Buchstabe a Datenschutz-Grundverordnung erteilt hätte – was im vorliegenden Fall streitig war. Daraufhin löschte der Geschäftsführer das Video zwar von der Webseite des Unternehmens, jedoch nicht auf den beiden genannten Plattformen. Hierzu bedurfte es einer erneuten Aufforderung.

Im Bußgeldverfahren verteidigte sich der Geschäftsführer damit, dass die E-Mail des Beschwerdeführers, in der er zum Ausdruck gebracht hatte, dass er mit einer Veröffentlichung des Videos im Internet nicht einverstanden sei, nicht zwingend als Widerruf einer zuvor erteilten Einwilligung zu verstehen gewesen sei. Der E-Mail des Beschwerdeführers war auch ohne Verwendung des Wortes „Widerruf" deutlich zu entnehmen, dass dieser mit einer Veröffentlichung des Videos nicht einverstanden war. Für die Ausübung von Betroffenenrechten ist es nicht erforderlich, dass Rechtsnormen oder juristische Fachbegriffe verwendet werden, wenn aus dem Inhalt der Mitteilung der Wille und die Geltendmachung eines Betroffenenrechtes deutlich zu erkennen sind.

Die vorsätzliche Veröffentlichung des Videos sowie die unterlassene Löschung haben wir mit einem Bußgeld in vierstelliger Höhe geahndet.

### 4.3 Unzulässige Weihnachtswerbung mit gelöschten Daten?

Eine Immobilienmaklerin kontaktierte einen Bürger mit einem Brief, in dem sie ihm anbot, das in seinem Eigentum stehende Grundstück zu verkaufen. Da er seine Daten selbst nicht an die Immobilienmaklerin weitergegeben hatte, war er erstaunt darüber, woher sie wusste, dass er der Grundstückseigentümer war und wo er wohnte. Deshalb wandte er sich an die Maklerin und fragte, woher sie diese Informationen hatte. Eine klare Antwort erhielt er hierauf nicht. Die Immobilienmaklerin schrieb ihm lediglich, dass sie aus Gründen des Datenschutzes keine Auskunft geben könne. Die Landesbeauftragte versuchte daraufhin, die Angelegenheit im verwaltungsrechtlichen Aufsichtsverfahren zu klären. Die Verantwortliche berief sich jedoch auf ihr Auskunftsverweigerungsrecht und teilte mit, die Daten bereits gelöscht zu haben.

Gemäß Artikel 15 Absatz 1 Buchstabe g Datenschutz-Grundverordnung (DS-GVO) hat der Verantwortliche auf Antrag der betroffenen Person dieser die Herkunft ihrer personenbezogenen Daten mitzuteilen, wenn er sie nicht bei der betroffenen Person erhoben hat. Gemäß Artikel 12 Absatz 4 DS-GVO unterrichtet der Verant-

wortliche die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags, über die Gründe und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, wenn er auf ihren Antrag nicht tätig wird. Das Auskunftsrecht soll betroffenen Personen die Möglichkeit geben, sich über die Verarbeitung ihrer personenbezogenen Daten zu informieren und gegebenenfalls über diese zu bestimmen. Die von der Maklerin verwendete Formulierung, dass die Auskunft aus Gründen des Datenschutzes nicht erteilt werden könne, genügte den Anforderungen von Artikel 12 Absatz 4 DS-GVO nicht. Vielmehr hätte dem Beschwerdeführer eine konkrete Begründung zugestanden, weshalb der Datenschutz die Auskunftserteilung verhindert. Zudem hätte er über die Möglichkeit, gegen die ablehnende Entscheidung einen Rechtsbehelf einlegen oder sich bei der Aufsichtsbehörde beschweren zu können, informiert werden müssen.

Ein halbes Jahr später wandte sich der Beschwerdeführer ein zweites Mal an uns und teilte mit, dass ihn dieselbe Immobilienmaklerin mit einem Weihnachtsbrief erneut kontaktierte. Die zuvor behauptete Löschung seiner Daten zog er damit in Zweifel.

Gemäß Artikel 6 Absatz 1 DS-GVO bedarf jede Verarbeitung personenbezogener Daten einer Erlaubnisnorm. Eine Verarbeitung kann rechtmäßig sein, wenn sie auf einer Einwilligung beruht oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Da die betroffene Person zuvor zum Ausdruck brachte, dass sie mit der Verarbeitung ihrer personenbezogenen Daten durch die Maklerin nicht einverstanden war, lag ihre Einwilligung in die Verarbeitung nicht vor. Auch konnte die Maklerin kein berechtigtes Interesse an der von ihr betriebenen Direktwerbung vorbringen, das die Interessen des Beschwerdeführers überwogen hätte.

## Datenschutz umsetzen auch in jungen Unternehmen

Eine Ahndung der Datenschutzverstöße war angezeigt. Die Immobilienmaklerin räumte im Rahmen der Anhörung zum

Bußgeldbescheid ein, dass die datenschutzrechtlichen Anforderungen in ihrem jungen Unternehmen noch nicht korrekt umgesetzt wurden. Weiterhin teilte sie mit, dass sie bei der Löschung der Daten übersehen habe, dass die Daten des Beschwerdeführers in einem separaten „Weihnachtsgruß“-Ordner ihres IT-Systems weiterhin gespeichert waren. Beide Verstöße ahndeten wir insgesamt mit einer vierstelligen Geldbuße. Hierbei war maßgeblich zu berücksichtigen, dass die Maklerin durch ihr Verhalten die Ausübung der Rechte der betroffenen Person aktiv unterbunden hatte und damit in ihr Grundrecht auf informationelle Selbstbestimmung eingriff.

## 4.4 Unberechtigte Datenverarbeitungen durch Polizeibedienstete

Die Zahl der bußgeldrelevanten Vorgänge im Zusammenhang mit unbefugten Datenverarbeitungen von Polizeibediensteten des Landes Brandenburg ist im Vergleich zum Vorjahr erneut gestiegen. Insgesamt betreffen ca. 26 % unserer Bußgeldverfahren derartige Verarbeitungen. Im Vorjahr waren es ca. 17 %. Die Vorgänge werden insbesondere von den jeweils zuständigen Disziplinarstellen des Polizeipräsidiums des Landes Brandenburg, den Staatsanwaltschaften oder den für die Datenschutzaufsicht zuständigen Beschäftigten der Landesbeauftragten an die Bußgeldstelle abgegeben.

Den Polizistinnen und Polizisten des Landes Brandenburg stehen polizeiliche Auskunftssysteme zur Ausübung ihrer dienstlichen Tätigkeiten zur Verfügung. Hierzu zählen zum Beispiel Datenbanken der Einwohnermeldeämter, das Zentrale Fahrzeugregister, verschiedene polizeiliche Fahndungssysteme und das Waffenregister. Zugriffe hierauf werden technisch protokolliert und bei hinreichendem Verdacht eines nicht dienstlich veranlassten Abrufs ausgewertet. § 32 Absatz 1 Brandenburgisches Datenschutzgesetz (BbgDSG) regelt im Zusammenhang mit §§ 38, 39 Brandenburgisches Polizeigesetz, dass ein Zugriff auf die polizeilichen Systeme nur erlaubt ist, wenn ein dienstlicher Anlass den Abruf erfordert. Ein solcher dienstlicher Anlass liegt in der Regel vor, wenn Abrufende mit der Sachbearbeitung des dem Abruf zugrundeliegenden Falles befasst sind. Bei den von uns zu prüfenden Vorgängen handeln die Täterinnen und Täter

jedoch häufig aus reiner Neugierde. Ein Abruf aus solchen privaten Interessen ist unbefugt und wird mit der Festsetzung einer Geldbuße geahndet.

Aber auch rechtmäßig abgerufene Daten dürfen die Polizeibediensteten nicht einfach weitergeben. Durch eine unbefugte Weitergabe personenbezogener Daten an Dritte wird gleichfalls der Ordnungswidrigkeitentatbestand des § 32 Absatz 1 BbgDSG erfüllt. Auch hier setzt die Landesbeauftragte regelmäßig eine Geldbuße fest.

Es liegt auf der Hand, dass zu Unrecht abgerufene Daten erst recht nicht an Dritte weitergegeben werden dürfen. So lag der Fall zum Beispiel, als ein Polizeibeamter von einer Freundin gebeten wurde, ihr vor dem Hintergrund einer Vernehmung als Beschuldigte Informationen aus den Auskunftssystemen zukommen zu lassen. Über WhatsApp teilte er mit, welche Informationen ihm durch seine unbefugten Abrufe bekannt geworden waren.

In einem anderen Fall hatte ein Polizeibeamter personenbezogene Daten einer Trunkenheitsfahrt bei einem zufälligen Zusammentreffen mündlich an die Mutter des Täters weitergegeben. Er dachte, dass die Mutter als dessen Arbeitgeberin durch Entzug des Dienstwagens eine Wiederholungstat verhindern könnte. Da es sich bei ihr jedoch um eine unbefugte Dritte handelte, durften die Informationen nicht mitgeteilt werden.

Ein Polizeibeamter behauptete in einem weiteren Fall, dass nicht er, sondern andere Kolleginnen oder Kollegen auf das System zugegriffen und den Abruf vorgenommen haben könnten. Da die Bediensteten jedoch dazu verpflichtet sind, ihre Zugangsdaten zu den Systemen geheim zu halten und sich bei Verlassen ihres Arbeitsplatzes aus den IT-Systemen auszuloggen oder sie zu sperren haben, überzeugt diese Verteidigungsstrategie nicht. Zeugenaussagen und die persönlichen Verbindungen der Polizistinnen und Polizisten zu den abgefragten Personen ermöglichen zudem in den meisten Fällen, die unbefugte Verarbeitung aufzuklären.

### 4.5 Beschäftigtendaten auf Abwegen

Eine ehemalige Mitarbeiterin eines Unternehmens hatte sich – als sie noch dort angestellt war – von ihrem dienstlichen Rechner eine Excel-Tabelle mit Beschäftigtendaten von 56 Mitarbeiterinnen und Mitarbeitern an ihre private E-Mail-Adresse zugesandt. Die Tabelle umfasste neben den vollständigen Namen u. a. auch einen Überblick über bereits genommene und verbleibende Urlaubstage, angefallene Krankentage, Lohndaten, geleistete Überstunden und Sozialversicherungsbeiträge. Die betreffende Mitarbeiterin war in der Firma als Sachbearbeiterin für die Aufgabengebiete Lohn und Gehalt beschäftigt. Die Übersendung an die private E-Mail-Adresse erfolgte nach ihrer Aussage zum Eigenschutz und zum Schutz der Kolleginnen und Kollegen, da im ohnehin bereits angespannten Arbeitsverhältnis Streitigkeiten über die ordnungsgemäße Aufgabenerfüllung der Betroffenen bestanden. Das Unternehmen stellte Strafantrag bei der zuständigen Staatsanwaltschaft, die das Verfahren einstellte und den Vorgang zur Verfolgung einer etwaigen Ordnungswidrigkeit an uns abgab.

Die Handlung der ehemaligen Beschäftigten war dem Unternehmen nicht zuzurechnen. Sie war damit selbst Betroffene in dem von uns eröffneten Bußgeldverfahren. Ihre dienstliche Tätigkeit bestand u. a. in der Erfassung und Aufbereitung der Arbeitszeitkonten inklusive der Urlaubs- und Krankentage sowie der Erstellung von Salden für erbrachte Arbeitsleistungen. Mit der Übersendung der personenbezogenen Daten der Mitarbeiterinnen und Mitarbeiter an die private E-Mail-Adresse überschritt sie ihre Kompetenzen und handelte im datenschutzrechtlichen Sinne als Verantwortliche. Zur Erfüllung ihrer betrieblichen Aufgaben war die Übermittlung der Beschäftigtendaten an ihre private E-Mail-Adresse nicht erforderlich und damit rechtswidrig. Diesen Verstoß ahndeten wir mittels Festsetzung einer Geldbuße in dreistelliger Höhe.

### 4.6 Bewerberdaten auf Abwegen

Ein Angestellter leitete von seiner dienstlichen E-Mail-Adresse Bewerbungsunterlagen, die bei seinem Arbeitgeber eingegangen wa-

ren, an seine private E-Mail-Adresse weiter, um sich Anregungen zur visuellen Gestaltung eigener Bewerbungen zu holen. Die Lebensläufe hatte er zuvor nicht anonymisiert, sodass sie weiterhin alle persönlichen und beruflichen Daten der Bewerberinnen und Bewerber umfassten. Dies wurde von seinem Arbeitgeber bemerkt und der Landesbeauftragten als Ordnungswidrigkeit angezeigt.

Im vorliegenden Fall handelte der Angestellte jedoch unbefugt. Die Übersendung der personenbezogenen Daten der Bewerberinnen und Bewerber an die private E-Mail-Adresse gehörte nicht zu seinen Arbeitsaufgaben. Er war damit im datenschutzrechtlichen Sinn als Verantwortlicher anzusehen.

Jede Verarbeitung personenbezogener Daten benötigt eine Erlaubnisnorm, um rechtmäßig zu sein. Diese kann entweder in einer Einwilligung der betroffenen Person oder in einer anderen gesetzlichen Grundlage liegen. Der Beschäftigte konnte sich hier auf keine Rechtsgrundlage für die Übersendung der Unterlagen berufen. Die sich bewerbenden Personen hatten nicht darin eingewilligt, dass er deren Lebensläufe an seine private E-Mail-Adresse weiterleitete. Auch die Abwägung nach Artikel 6 Absatz 1 Satz 1 Buchstabe f Datenschutz-Grundverordnung geht zu ihren Gunsten aus. Selbst wenn das Interesse des Angestellten an den Bewerbungsunterlagen ausschließlich der visuellen Gestaltung gegolten und er es nicht auf die personenbezogenen Bewerberdaten abgesehen hatte, überwogen jedenfalls die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen. Sie hatten ihre Bewerbungsunterlagen im Vertrauen auf den datenschutzrechtlich ordnungsgemäßen Umgang mit ihren personenbezogenen Daten an den Arbeitgeber des Angestellten übersandt. Sie mussten nicht davon ausgehen, dass diese Daten unsachgemäß verwendet werden. Die Verwendung ihrer personenbezogenen Daten durch den Angestellten zum Zweck der Anregung bei der Gestaltung eigener Bewerbungen stellte keinen rechtfertigenden Grund dar, in das Grundrecht auf Informationelle Selbstbestimmung einzugreifen.

Die Landesbeauftragte verhängte wegen der unbefugten Verarbeitung personenbezogener Daten eine dreistellige Geldbuße gegen den Angestellten.

Die Daten waren darüber hinaus für alle diejenigen einsehbar, die Zugriff auf seine E-Mails hatten, entweder beim Transport über das Internet oder während der Speicherung im E-Mail-Konto.

### 4.7 Nutzung von WhatsApp durch eine Ärztin

Eine Ärztin für Kinder- und Jugendlichenpsychotherapie gründete eine WhatsApp-Gruppe mit 230 Teilnehmerinnen und Teilnehmern, um ihre neue Praxisanschrift mitzuteilen. Darüber beschwerte sich die Mutter einer ehemaligen, minderjährigen Patientin und informierte uns, dass die Ärztin hierfür keine Einwilligung eingeholt habe. Die Gruppe bestand u. a. aus Eltern, Therapeutinnen und Therapeuten, Sozialpädagoginnen und Sozialpädagogen sowie Lehrkräften. Allen Gruppenmitgliedern wurden die Telefonnummern der anderen Mitglieder offenbart. Teilweise konnten Gruppenmitglieder, wenn sie andere in ihren eigenen Kontakten führten oder Telefonnummern wiedererkannten, Rückschlüsse darauf ziehen, dass sich Kinder aus ihnen bekannten Familien bei der Ärztin in Behandlung befinden oder befunden hatten.

Wir leiteten gegen die Ärztin ein Bußgeldverfahren wegen der unrechtmäßigen Verarbeitung personenbezogener Daten ein. Nach Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) dürfen personenbezogene Daten nur verarbeitet werden, wenn einer der dort genannten Erlaubnistatbestände vorliegt. Im Datenschutzrecht gilt der Grundsatz, dass eine Datenverarbeitung verboten ist, es sei denn, sie ist ausdrücklich gesetzlich erlaubt oder die betroffenen Personen stimmen der Verarbeitung zu. Im vorliegenden Fall hätten die Mitglieder der WhatsApp-Gruppe in die Aufnahme in die Gruppe und damit in die Offenbarung ihrer Telefonnummern einwilligen oder die Ärztin hätte ein die Interessen der betroffenen Personen überwiegendes berechtigtes Interesse an der Offenbarungshandlung darlegen müssen. Beides war nicht der Fall. Auch die anderen Erlaubnistatbestände trafen hier nicht zu. Daneben war zu berücksichtigen, dass über die Telefonnummern Rückschlüsse auf Gesundheitsdaten gemäß Artikel 9 Absatz 1 DS-GVO der (minderjährigen) Kinder mehrerer Eltern möglich waren.

Darüber hinaus ist die Verwendung von WhatsApp aufgrund der zwangsläufigen Datenverarbeitung in den USA sowie unter Berücksichtigung der Schrems II-Entscheidung des Europäischen Gerichtshofs äußerst kritisch zu bewerten.[9] Wir raten von der Nutzung dieses Messenger-Dienstes insbesondere in Gesundheitsberufen daher ab.

Aufgrund der unberechtigten Datenverarbeitung haben wir gegen die Ärztin ein Bußgeld in vierstelliger Höhe verhängt.

9 Tätigkeitsbericht Datenschutz 2020, A V 2.

# III Anlasslose Prüfungen

# 1 Umsetzung der Schrems II-Entscheidung durch Unternehmen

In seinem viel beachteten Urteil vom 16. Juli 2020 (Rechtssache C 311/18 – „Schrems II“) erklärte der Europäische Gerichtshof den Durchführungsbeschluss der Europäischen Kommission zum sogenannten Privacy Shield für unwirksam. Übermittlungen personenbezogener Daten in die USA waren auf dieser Grundlage somit nicht länger zulässig und mussten entweder auf eine andere Rechtsgrundlage um- oder unverzüglich eingestellt werden. Ferner betonte das Gericht, dass Verantwortliche, soweit Datenexporte nicht auf bestehende Angemessenheitsbeschlüsse gestützt werden können (gegenwärtig etwa für Andorra, Argentinien, Guernsey, die Färöer-Inseln, Isle of Man, Israel, Japan, Jersey, Kanada, Neuseeland, die Republik Korea, die Schweiz, das Vereinigte Königreich und Uruguay), unabhängig von der Rechtsgrundlage für den Transfer zu prüfen haben, ob in dem Drittland ein der Europäischen Union gleichwertiges Schutzniveau besteht oder ob zur Sicherstellung eines im Wesentlichen gleichwertigen Schutzniveaus zusätzliche rechtliche, technische oder organisatorische Maßnahmen ergriffen werden müssen. Dabei dürfe die Wirksamkeit solcher Maßnahmen durch die jeweilige Rechtsordnung im Drittland nicht beeinträchtigt werden. Diese Prüfpflicht findet sich nunmehr gleichsam in den neugefassten Standarddatenschutzklauseln der Europäischen Kommission. Auch der Europäische Datenschutzausschuss hat seine „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ angepasst und in der endgültigen Fassung am 18. Juni 2021 beschlossen. Beide Dokumente sind unserem Internetangebot zu entnehmen.

Im Rahmen einer länderübergreifenden Prüfung haben wir stichprobenartig brandenburgische Unternehmen verschiedener Branchen angehört, um die Einhaltung datenschutzrechtlicher Vorgaben und insbesondere des Schrems II-Urteils bei der Einbindung außereuropäischer E-Mail- und Webhosting-Dienste zu kontrollieren. Dabei fiel auf, dass eine Vielzahl der befragten Verantwortlichen in diesem Zusammenhang identische Unternehmen mit der Erbringung der Dienste beauftragt hat und häufig auf deren vertragliche Muster

zurückgreift, um den Transfer mittels Standarddatenschutzklauseln mit zusätzlichen Maßnahmen abzusichern. Das reicht jedoch nicht aus. Vielmehr ist zu beachten, dass es weiterhin bei der Pflicht des Verantwortlichen bleibt, die ergriffenen Maßnahmen auf ihre Tauglichkeit hin zu überprüfen und Vorlagen von Auftragsverarbeitern gegebenenfalls auch kritisch zu hinterfragen. Die ausgewählten Unternehmen konnten ganz überwiegend darlegen, dass interne Prüfungen und in Teilen Umstrukturierungen bereits veranlasst wurden. Damit einher gehen in einigen Bereichen Vertragsanpassungen mit den Dienstleistungsunternehmen. Lediglich in einem Fall verwies der Verantwortliche noch über ein Jahr nach der Schrems II-Entscheidung zur Rechtfertigung eines Transfers personenbezogener Daten in die USA auf den inzwischen unwirksamen Durchführungsbeschluss der Europäischen Kommission zum Privacy Shield, sodass hier größerer Anpassungsbedarf bestand. Ein anderes Unternehmen nahm unser Anhörungsverfahren dagegen zum Anlass, den Transfer in Drittländer in Gänze einzustellen.

Soweit nach Prüfung der eingesetzten Produkte und Dienste auch unter Berücksichtigung der Umstände der Übermittlung und etwaiger zusätzlicher Maßnahmen festzustellen bleibt, dass keine geeigneten Garantien vorgehalten werden, um den unverhältnismäßigen Zugriff auf die exportierten Daten zu unterbinden und wirksamen Rechtsschutz gegen diesen zu ermöglichen, ist die Übermittlung personenbezogener Daten durch die Verantwortlichen auszusetzen oder zu beenden. Ansonsten sind nach Auffassung des Europäischen Gerichtshofes die Aufsichtsbehörden verpflichtet, die fraglichen Datenübermittlungen zu verbieten.

Soweit nach Prüfung der eingesetzten Produkte und Dienste auch unter Berücksichtigung der Umstände der Übermittlung und etwaiger zusätzlicher Maßnahmen festzustellen bleibt, dass keine geeigneten Garantien vorgehalten werden, um den unverhältnismäßigen Zugriff auf die exportierten Daten zu unterbinden und wirksamen Rechtsschutz gegen diesen zu ermöglichen, ist die Übermittlung personenbezogener Daten durch die Verantwortlichen auszusetzen oder zu beenden. Ansonsten sind nach Auffassung des Europäischen Gerichtshofes die Aufsichtsbehörden verpflichtet, die fraglichen Datenübermittlungen zu verbieten.

## 2 Prüfung von Maklerbüros

Einen in unserer behördlichen Aufsichtspraxis wiederkehrenden Sachverhalt stellt die gezielte postalische Kontaktaufnahme mit Immobilieneigentümerinnen und -eigentümern durch Maklerinnen und Makler zum Zweck der Eigenwerbung dar. Dabei wird oft auf eine bestimmte Immobilie der betroffenen Personen Bezug genommen, ohne die Herkunft der Information über die Eigentumsverhältnisse zu offenbaren. Werden jedoch personenbezogene Daten bei einem Dritten und nicht unmittelbar bei der betroffenen Person selbst erhoben (sogenannte „Dritterhebung“), so ist der Verantwortliche dazu verpflichtet, der betroffenen Person die unter Artikel 14 Datenschutz-Grundverordnung (DS-GVO) aufgeführten Informationen mitzuteilen. Vor diesem Hintergrund und auch um nähere Einblicke in die Arbeitsweise der Branche zu erhalten, wurden mehrere Immobilienmaklerinnen und Immobilienmakler im Land Brandenburg nach dem Zufallsprinzip ausgewählt, um eine angekündigte Prüfung an ihrem Geschäftsort durchzuführen. Den Schwerpunkt bildeten die Transparenz bei der Verarbeitung der Kundendaten sowie die für ihre Verarbeitung notwendigen technisch-organisatorischen Maßnahmen.

Zunächst haben wir uns jeweils den Prozess der Kundendatenverarbeitung zur Erfüllung der Maklerverträge erläutern lassen. Verkäuferinnen und Verkäufer würden grundsätzlich – informiert durch die eigenen Webseiten der Maklerinnen und Makler – den Kontakt per Telefon oder E-Mail aufnehmen. Käuferinnen und Käufer hingegen würden überwiegend auf die Immobilieninserate reagieren. Die geprüften Maklerlinnen und Makler haben uns gegenüber dargelegt, die Daten ihrer Kundinnen und Kunden nicht über Dritte, sondern bei ihnen direkt zu erheben.

Die Informationspflichten bilden die Basis für die Ausübung der Betroffenenrechte (insbesondere der Artikel 15 ff. DS-GVO). Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben. Die bei der Direkterhebung gemäß Artikel 13 DS-GVO notwendigen Informationen wurden bei den Maklerinnen und Maklern grundsätzlich auf den jeweiligen Webseiten zum Abruf bereitgehalten, im Falle einer

Eingangsbestätigung per E-Mail mitübersandt oder in Form eines Papierausdrucks bei Abschluss des Maklervertrages direkt übergeben.

Artikel 17 Absatz 1 DS-GVO bestimmt, dass personenbezogene Daten auf Verlangen der betroffenen Person oder unter bestimmten Voraussetzungen auch ohne ausdrückliches Verlangen der betroffenen Person eigenständig durch den Verantwortlichen unverzüglich gelöscht werden müssen, es sei denn, die weitere Speicherung ist rechtlich zulässig.

Bei den von uns geprüften Maklerinnen und Maklern wurde die Löschung der Kundendaten nach unterschiedlichen Konzepten grundsätzlich zum Jahresende durchgeführt. Für die Entsorgung von Datenträgern wurden Dienstleistungen von Entsorgungsunternehmen im Wege der Auftragsdatenverarbeitung in Anspruch genommen. Papierakten wurden entweder selbst oder durch Entsorgungsunternehmen vernichtet. Papierdokumente sind mit Aktenvernichtern zu zerkleinern. Bei normalem Schutzbedarf sollten hierfür Aktenvernichter der Sicherheitsstufe P-3 nach DIN 66399 genutzt werden. Geräte mit dieser Sicherheitsstufe verringern die Schnipselgröße auf maximal 320 mm² oder Streifen beliebiger Länge mit höchstens 2 mm Breite.

Die für die eigenverantwortliche Entsorgung verwendeten Schredder entsprachen jedoch nicht in allen Fällen den aktuellen Sicherheitsstandards, sodass wir die Anschaffung eines Aktenvernichters mindestens der Sicherheitsstufe P-3 empfohlen haben.

Für die Löschung der elektronisch gespeicherten Daten nutzen die Maklerinnen und Makler die üblichen Möglichkeiten der verwendeten Bürosoftware. Wir machten darauf aufmerksam, dass die einfachen Löschkommandos der jeweiligen Betriebssysteme und auch die Formatierung der entsprechenden Datenträger nicht ausreichen, um dort gespeicherte Daten sicher zu löschen und forderten, spezielle Software zur Löschung von Daten einzusetzen oder Dienstleistungsunternehmen mit der Vernichtung der Speichermedien zu beauftragen.

# 3 Maßnahmen gegen Diebstähle in Kindertagesstätten

Im Berichtszeitraum wurden unserer Dienststelle erneut viele Meldungen gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) zu Verletzungen des Schutzes personenbezogener Daten übermittelt, die Daten von Kindern betrafen. Eine bestimmte Art von Datenschutzverletzungen kam dabei in verhältnismäßig großem Umfang vor. Wie auch bereits im letzten Jahr kam es häufig zu vielen Einbrüchen und Diebstählen in Kindertagesstätten. Die Diebstähle geschahen sowohl während als auch außerhalb der Öffnungszeiten der Einrichtungen. In den meisten Fällen wurden elektronische Geräte gestohlen, wie zum Beispiel Kameras, Laptops oder Massenspeichergeräte (z. B. externe Festplatten, USB-Sticks). Hierbei schien es regelmäßig eher um den materiellen Wert des Diebesgutes als um darauf befindliche personenbezogene Daten zu gehen, da Papierakten (z. B. Entwicklungsdokumentationen zu den Kindern) in der Regel nicht entwendet wurden, dafür aber auch Kaffeekassen und ähnliche Gegenstände von Wert. So kann zwar angenommen werden, dass es die Diebe vorwiegend nicht auf den Missbrauch der Daten abgesehen hatten, allerdings kann dieser auch nicht ausgeschlossen werden.

Gemäß Artikel 4 Nummer 12 DS-GVO ist eine 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 beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert, oder auf sonstige Weise verarbeitet wurden. Sowohl durch den Zugang zu den Daten für unbefugte Dritte als auch durch den eventuellen Verlust (bei fehlenden Datensicherungen) sind somit die Bedingungen für eine Datenschutzverletzung erfüllt. Da von den Diebstählen in Kindertagesstätten in der Regel Daten von Kindern betroffen sind und diese gemäß Erwägungsgrund 75 DS-GVO unter besonderem Schutz stehen, ist grundsätzlich davon auszugehen, dass bei solchen Vorfällen Risiken für die Rechte und Freiheiten der betroffenen Kinder entstehen können und sie somit nach Artikel 33 DS-GVO an unsere Dienststelle zu melden sind.

Im Rahmen der Aufklärung der Ursachen für diese Datenschutzverletzungen starteten wir eine Befragung mehrerer öffentlicher und nicht öffentlicher Trägerinnen und Träger von Kindertagesstätten. Darin stellten wir verschiedene Fragen, zum Beispiel zu genutzten Geräten und deren Aufbewahrung oder zu technischen und organisatorischen Sicherheitsmaßnahmen, die in den Einrichtungen getroffen werden. Weiter wollten wir wissen, ob in den vergangenen Jahren Einbrüche zu verzeichnen waren und welche Maßnahmen speziell nach einem erfolgreichen Einbruch und einem Diebstahl ergriffen wurden, um den Schutz der personenbezogenen Daten der Kinder gewährleisten zu können.

## Daten von Kindern sicher verwahren

Erste Auswertungen der noch nicht vollständig vorliegenden Antworten zeigen, dass in den Einrichtungen der von uns befragten Trägerinnen und Träger von Kindertagesstätten die Geräte zumindest nach Dienstschluss meist verschlossen aufbewahrt werden. Oftmals werden hierfür stabile Büroschränke genutzt, selten hingegen Tresore. Nur in sehr wenigen Einrichtungen sind Alarmanlagen installiert, da diese gemäß der Rückmeldungen üblicherweise von der Eigentümerin oder dem Eigentümer des Gebäudes – oftmals einer Kommunalverwaltung – gestellt werden müssen.

Da viele der uns gemeldeten Diebstähle tagsüber während der Öffnungszeiten der Kindertagesstätten stattfanden, ist anzuraten, die Geräte nicht nur nach Dienstschluss zu verschließen, sondern direkt nach Gebrauch. Zudem empfiehlt es sich, z. B. bei Kameras die Aufnahmen nur möglichst kurz auf den Geräten bzw. Speicherkarten abzulegen, sie direkt in ein geschütztes Speichersystem zu überführen und anschließend von den mobilen Geräten zu löschen. Um die teils sensitiven Daten der Kinder (z. B. Gesundheitsdaten gemäß Artikel 9 DS-GVO, Entwicklungsberichte) zu schützen, ist es nach unserer Auffassung unabdingbar, dass in den IT-Systemen, wo immer dies möglich ist, verschlüsselte Datenträger eingesetzt werden.

Den Datenschutzbeauftragten der Kindertagesstätten bzw. ihrer Trägerinnen und Träger legten wir nahe, die Themen Einbruch und Diebstahl mit den Beschäftigten intensiv zu besprechen und sie zu schulen. Auch sollten derartige Vorfälle mit dem Personal ausgewertet

und die Umsetzung zusätzlicher technischer und organisatorischer Sicherheitsmaßnahmen geprüft werden. Zielführende Hinweise zur Sicherheit beim Umgang mit mobilen Geräten und Datenträgern, z. B. beim Transport, können unserer Handreichung „Technische und organisatorische Maßnahmen zur Umsetzung des Datenschutzes bei Heimarbeit“ entnommen werden, welche in unserem Internetangebot zu finden ist.

## 4 Prüfung von Sozialbehörden im Rahmen der Leistungsgewährung nach dem Asylbewerberleistungsgesetz

Im Berichtszeitraum haben wir damit begonnen, die Einhaltung der datenschutzrechtlichen Vorgaben bei der Aufgabenwahrnehmung nach dem Asylbewerberleistungsgesetz durch die Sozialbehörden von drei Landkreisen zu überprüfen. Hintergrund waren verschiedene Anfragen, die einen erheblichen Beratungsbedarf der zuständigen Behörden erkennen ließen. Unter Berücksichtigung der anhaltenden Maßnahmen zur Eindämmung der Covid-19-Pandemie führten wir die Prüfung schriftlich durch. Hierfür wurde ein umfassender Fragenkatalog zu den rechtlichen Vorgaben und den implementierten technischen und organisatorischen Maßnahmen erstellt. Zudem kontrollierten wir die datenschutzgerechte Aktenführung mittels einer Stichprobe.

Bei den Vorschriften des Asylbewerberleistungsgesetzes handelt es sich zwar um solche des Sozialrechts. Grundsätzlich finden sich die sozialdatenschutzrechtlichen Vorschriften in den §§ 67 ff. Zehntes Buch Sozialgesetzbuch (SGB X). § 9 Absatz 4 Asylbewerberleistungsgesetz (AsylBLG) erklärt diese Vorschriften jedoch nicht für anwendbar. Es ist daher für eine rechtmäßige Verarbeitung der personenbezogenen Daten auf § 5 Absatz 1 Brandenburgisches Datenschutzgesetz (BbgDSG) als Datenverarbeitungsbefugnis zurückzugreifen. Danach dürfen personenbezogene Daten verarbeitet werden, wenn dies für eine gesetzlich übertragene Aufgabe erforderlich ist. Diese findet sich in § 3 Absatz 1 Landesaufnahmegesetz. Bei der Prüfung mussten wir feststellen, dass nur eine der kontrollierten So-

zialbehörden die richtige Rechtsgrundlage der Datenverarbeitung kannte.

Eine korrekte Aktenführung gibt sowohl den Betroffenen als auch der Behörde die Möglichkeit, sich einen umfassenden Überblick über die Entscheidungsgrundlage für die Leistungen zu verschaffen. Eingereichte Unterlagen müssen im Zusammenhang mit der Leistungsgewährung stehen und den Entscheidungsprozess dokumentieren. Insbesondere bei Ermessensentscheidungen muss erkennbar sein, welche Angaben der Entscheidungsfindung zu Grunde lagen. Erhebungen und Speicherungen von Daten sind nach den datenschutzrechtlichen Regelungen auf das notwendige Mindestmaß zu beschränken. Jegliche darüber hinausgehende Datenverarbeitung ist unzulässig.

## Leistungsakten datensparsam führen

Im Leistungsspektrum befinden sich gemäß § 4 AsylBLG auch Gesundheitsleistungen bei Krankheit und Schwangerschaft. Gleichfalls fallen durch die Darlegung der Leistungsberechtigung nach § 1 AsylBLG auch personenbezogene Daten an, die z. B. den Grund des Asylantrages widerspiegeln. Es sind daher in besonderem Maße sensitive Daten nach Artikel 9 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) betroffen. Ein vertraulicher Umgang mit solchen Daten ist strikt einzuhalten. Aus diesem Grunde sind Unterlagen wie zum Beispiel Arztbriefe, Atteste oder Krankenhausentlassungsberichte nur ausnahmsweise und unter weiteren Schutzmaßnahmen zur Akte zu nehmen. Bewährt hat sich aus unserer Perspektive etwa, die Unterlagen in einem verschlossenen Umschlag abzulegen. Irrelevante Daten sind aus den Dokumenten zu schwärzen, wenn die Speicherung des Dokuments im Übrigen tatsächlich notwendig ist. Die Aktenführung zeigte, dass bei den zuständigen Behörden erhebliche Defizite im Umgang mit eben solchen sensitiven Daten bestehen.

Die Prüfung der datenschutzgerechten Führung der übersandten Leistungsakten konnten wir abschließen. In allen 12 überprüften Leistungsakten befanden sich personenbezogene Daten von an dem jeweiligen Verfahren unbeteiligten Personen. Teilweise waren Listen der vollständigen Namen, Geburtsdaten und Krankenversicherungsnummern von über 40 verschiedenen Personen gespeichert. Da es

sich hierbei auch um Aufstellungen von gewährten Gesundheitsleistungen handelte, waren Rückschlüsse auf den gesundheitlichen Zustand der unbeteiligten Personen möglich. Solche Verzeichnisse gehen nicht nur weit über das Maß an erforderlichen Daten hinaus, sie stellen auch eine unüberwindbare Hürde bei der Ausübung von Betroffenenrechten dar. Denn die oder der Betroffene weiß nicht, dass die eigenen Daten in einer fremden Leistungsakte gespeichert sind. Auch die Behörde kann diese Daten mangels Querverweisen nicht mehr auffinden. Somit wird beispielsweise auch die Durchsetzung des gesetzlichen Löschanspruchs aus Artikel 17 Absatz 1 DS-GVO für die Betroffenen praktisch unmöglich.

Zahlreiche Leistungsakten enthielten Rezepte, Überweisungsträger und auch Diagnosen von behandelnden Ärztinnen und Ärzten. Ihnen war somit ein detailliertes Bild des gesundheitlichen Zustands der betroffenen Personen zu entnehmen. Keine der Akten wies besondere, der hohen Sensitivität dieser Gesundheitsdaten angemessene Schutzmaßnahmen auf, denn die Unterlagen waren in dem regulären Aktenverlauf einsortiert. Zum Nachweis von Schwangerschaften wurden Kopien des Mutterpasses angefertigt, wobei mehr Gesundheitsdaten ersichtlich waren als nur die bestehende Schwangerschaft mit Geburtstermin. So fanden sich auf den Kopien Angaben zum psychischen Zustand der werdenden Mütter, chronischen Erkrankungen wie Diabetes und auch Angaben zu familiären Erbkrankheiten. Diese Daten sind zur Leistungsgewährung nicht notwendig.

In einer Leistungsakte wurden zur Geltendmachung von Fahrtkosten in ein Klinikum nicht nur eine Aufstellung der Fahrten und der gelösten Fahrscheine gespeichert, sondern zusätzlich noch die Terminvereinbarung mit Befund und Diagnose der behandelten Person. Die Speicherung dieser Gesundheitsdaten war zum Nachweis der Fahrtkosten nicht erforderlich.

Bei der Aufnahme von Arbeitsgelegenheiten forderten die Sozialbehörden von den Leistungsberechtigten Kontoauszüge an. Auf die Möglichkeit der Schwärzung von nicht notwendigen Daten wiesen sie nach Aktenlage nicht hin. Somit war unter anderem ersichtlich, wann die leistungsbeziehenden Personen wo und in welcher Höhe Einkäufe getätigt oder Schulden bezahlt hatten. Da auch diese Daten

nicht zur Leistungsgewährung benötigt werden, liegen die gesetzlichen Voraussetzungen zur Datenverarbeitung nicht vor.

Gleichfalls wurden durch die Behörden die Arbeitsverträge der betroffenen Personen angefordert, sobald diese eine Arbeitsgelegenheit aufgenommen hatten. Teilweise haben die Behörden die vollständigen Verträge in Kopie zur Akte genommen. Von der Speicherung umfasst waren damit auch Nebenbestimmungen des Arbeitsverhältnisses, welche keinen Einfluss auf die Leistungsgewährung haben. Auch für diese Daten lag damit die gesetzliche Voraussetzung der Erforderlichkeit nicht vor.

Zum Prüfungsumfang gehört neben rechtlichen Fragen auch die Begutachtung der von den Sozialbehörden ergriffenen technischen und organisatorischen Maßnahmen. Dazu zählen unter anderem das Löschkonzept, das Berechtigungskonzept, das Kryptokonzept sowie das prozedurale Vorgehen bei Meldungen nach Artikel 33 DS-GVO. Wir erhielten dabei eine weite Bandbreite an verschiedenen Unterlagen mit unterschiedlicher Quantität und Qualität. Eine abschließende Bewertung hierzu steht noch aus.

Wir haben zunächst die Verletzung der datenschutzrechtlichen Vorgaben bei der Aktenführung gegenüber den betroffenen Sozialbehörden moniert und sie zu Korrekturen aufgefordert. Damit konnten wir einen ersten Teilbereich unserer datenschutzrechtlichen Kontrolle abschließen. Derzeit werten wir die uns überlassenden Unterlagen aus und setzen die Prüfung im folgenden Jahr fort.

## 5 Videokonferenzsysteme in Hochschulen

Wie bereits im letzten Tätigkeitsbericht[10] angekündigt, führten wir im Sommer 2021 eine erneute Befragung zum Thema Online-Lehre an den öffentlichen Hochschulen und Universitäten des Landes Brandenburg durch. Hauptsächlich sollte festgestellt werden, wie diese Einrichtungen mit unserer Empfehlung aus dem vergangenen Jahr beim Einsatz von Videokonferenzsystemen umgegangen sind. In dieser Empfehlung rieten wir den öffentlichen Hochschulen davon ab,

10 Tätigkeitsbericht Datenschutz 2020, A I 7.

auf Auftragsverarbeiter zurückzugreifen, bei denen es keine Rechtssicherheit und kein mit dem der Europäischen Union vergleichbares Datenschutzniveau gibt.

Das ernüchternde Resultat der diesjährigen Befragung ist, dass an mindestens sieben der acht öffentlichen Hochschulen nach wie vor Videokonferenzsysteme zum Einsatz kommen, bei deren Nutzung es erhebliche datenschutzrechtliche Bedenken gibt. Es handelt sich hierbei um Systeme amerikanischer Dienstleisterinnen und Dienstleister, die zwar in Sachen Stabilität und Funktionalität punkten können, jedoch in Bezug auf den Datenschutz teilweise gravierende Schwächen aufweisen. Fehlende Transparenz, Datenübertragung in die Vereinigten Staaten von Amerika ohne hinreichende Beachtung des sogenannten „Schrems II"-Urteils des Europäischen Gerichtshofs[11] und die Verarbeitung von personenbezogenen Daten der Nutzerinnen und Nutzer für eigene Geschäftszwecke der Dienstleisterinnen und Dienstleister gelten in diesem Zusammenhang als besonders problematisch.

Seitens der Hochschulen fand eine Abwägung zwischen der Erfüllung des Bildungsauftrags und der Einhaltung des Datenschutzes statt. Durch die anhaltende Corona-Pandemie betrug der Anteil der Präsenzlehre nicht mehr als 50 Prozent. Aus Sicht der Hochschulen machte dies den Einsatz von Videokonferenzsystemen zur Erfüllung des Bildungsauftrages weiter erforderlich. Bei der Wahl der konkreten Systeme spielten verschiedene Faktoren eine Rolle. Beispielsweise erhielt eine Hochschule auf ihre Ausschreibung keine datenschutzkonformen Produktangebote. Eine andere Hochschule berichtete, dass sie zwar über ein datenschutzkonformes System verfügt, welches im Einzelfall eingesetzt werden kann, Tests jedoch gezeigt haben, dass dieses System bei einer großen Anzahl an Teilnehmenden nicht stabil genug läuft. Wieder andere Hochschulen teilten mit, dass sie zwar über datenschutzkonforme Systeme verfügen, aber in einzelnen Vorlesungen auf eine bestimmte Funktionalität des Systems eines nicht datenschutzkonformen Dienstleistungsunternehmens angewiesen sind.

11 Tätigkeitsbericht Datenschutz 2020, A V 2.

Trotz aller Kritik konnten wir auch positive Entwicklungen in Bezug auf den Datenschutz feststellen. So gelang es Hochschulen, Verbesserungen in den Auftragsverarbeitungsverträgen zu erwirken. Die Anforderungen der Datenschutz-Grundverordnung sind damit zwar immer noch nicht vollständig erfüllt, jedoch stehen weitere Nachbesserungen in Aussicht. Positiv hervorzuheben ist auch, dass teilweise eine datensparsame Einwahl der Studierenden in die Videokonferenzen ermöglicht wurde. Hierbei erfolgt die Einwahl ohne Angabe des Namens, der E-Mail-Adresse oder der Matrikelnummer, sondern zum Beispiel ausschließlich mittels eines geteilten Links sowie konferenzbezogenen Passworts. Allerdings sind trotz dieser Maßnahme die durch das Dienstleistungsunternehmen verarbeiteten Metadaten der Nutzenden in der Regel personenbeziehbar und insofern daher das Grundproblem nicht gelöst. Eine weitere positive Entwicklung ist, dass einige Hochschulen Wahlmöglichkeiten umgesetzt haben. Für den Fall, dass eine Studentin oder ein Student Bedenken bezüglich der außereuropäischen Datenverarbeitung äußert, werden die Lerninhalte über eine gleichwertige datenschutzkonforme Alternative vermittelt. Dieses Angebot ist aber aufgrund der fehlenden Stabilität des Systems nur vereinzelt umsetzbar.

Eine einfache Lösung der Gesamtproblematik steht nicht in Aussicht. Unser Lösungsvorschlag sah vor, für große Veranstaltungen auf Videokonferenzen zu verzichten und die Lehrinhalte beispielsweise als Video auf den eigenen Plattformen zum Abruf zur Verfügung zu stellen. Für kleinere Veranstaltungen wie Seminare, Tutorien, Sprechstunden und Vorlesungen mit geringer Anzahl an Teilnehmenden könnten immer noch Videokonferenzsysteme eingesetzt werden – dann allerdings solche, die die Datenschutzvorschriften einhalten. Der Vorteil hierbei wäre, dass zumindest die Anforderung an die Stabilität des Videokonferenzsystems durch die geringere Belastung sinken würde. Der Einsatz von datenschutzkonformen und möglicherweise weniger stabilen Videokonferenzsystemen wäre somit möglich. Auf diesen Lösungsvorschlag wurde seitens der Hochschulen jedoch hauptsächlich erwidert, dass er eine erhebliche Minderung der Qualität der Lehre zur Folge hätte. Hervorgehoben wurden insbesondere eingeschränkte Interaktionsmöglichkeiten sowie fehlende Funktionalitäten.

Um dennoch Lösungen und Kompromisse für die durch die Corona-Pandemie anhaltende Ausnahmesituation an den Hochschulen zu finden, werden wir uns mit dem Ministerium für Wissenschaft, Forschung und Kultur beraten und falls möglich ein gemeinschaftliches Vorgehen mit den Kolleginnen und Kollegen aus anderen Bundesländern abstimmen.

Letztlich ist zu betonen, dass die anhaltende Ausnahmesituation an den Hochschulen kein Dauerzustand werden darf. Auf der einen Seite bedeutet dies, dass positive Weiterentwicklungen in Bezug auf den Datenschutz während der Pandemie stetig gestärkt und gefördert werden müssen. Auf der anderen Seite muss aber auch spätestens zum Ende der Pandemie ein vollständig datenschutzkonformer Zustand im Lehrbetrieb erreicht sein. Der Ankündigung der Hochschulen, dass digitale Lehrformate dauerhaft gefragt sein werden, kann grundsätzlich zugestimmt werden. Allerdings darf das Grundrecht auf informationelle Selbstbestimmung der Nutzerinnen und Nutzer derartiger Angebote nicht hintanstehen.

# IV Ausgewählte Fälle

# 1 Warnstufe rot – Microsoft Exchange Server mit Sicherheitslücken

Microsoft Exchange Server ist eine Software zum Senden, Empfangen und Verwalten von E-Mail-Nachrichten. Darüber hinaus können hiermit z. B. Termine, Kontakte und Aufgaben zentral verwaltet und somit die Zusammenarbeit in Arbeitsgruppen unterstützt werden. In Unternehmen, Behörden und Bildungseinrichtungen nicht nur in Deutschland ist diese Software weit verbreitet.

Wegen des hohen Verbreitungsgrades sowie der Chance, Zugriff auf viele sensitive Daten zu erlangen, stehen IT-Systeme mit Exchange Server regelmäßig im Visier von Angreiferinnen und Angreifern – so auch in diesem Jahr. Anfang März 2021 veröffentlichte Microsoft kurzfristig und außerplanmäßig neue Sicherheitsupdates für das Produkt. Hintergrund waren mehrere bekannt gewordene Sicherheitslücken, die von Kriminellen zielgerichtet aktiv und massiv für Angriffe ausgenutzt wurden. Sie konnten auf diese Weise E-Mails und Adressbücher auslesen und manipulieren sowie Schadsoftware für einen erweiterten Systemzugriff installieren. Besonders problematisch war hierbei die Platzierung von so genannten Web Shells im IT-System der Verantwortlichen. Mit Hilfe einer „virtuellen Kommandozeile“ wäre es darüber auch nach dem Schließen der Sicherheitslücken möglich gewesen, aus der Ferne auf das System zuzugreifen und nachgelagerte Angriffe durchzuführen oder ggf. das komplette IT-System vollständig zu übernehmen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) reagierte sofort und rief die Warnstufe rot aus. Eine Warnung mit dieser höchsten Dringlichkeit besagt, dass die IT-Bedrohungslage extrem kritisch ist, ein Ausfall vieler Dienste zu befürchten ist und ein Regelbetrieb dann nicht aufrechterhalten werden kann. Kurz nach Bekanntwerden der Schwachstellen waren allein in Deutschland bereits zehntausende Unternehmen und zum Teil auch öffentliche Stellen betroffen.

Im Zusammenhang mit den Microsoft Exchange-Sicherheitslücken gingen bei unserer Behörde innerhalb kurzer Zeit 63 Meldungen einer Datenschutzverletzung gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) ein. Über mehrere Wochen hinweg erreichten uns danach weitere derartige Meldungen. Wir reagierten wegen der

hohen Anzahl zunächst mit Standardschreiben und wiesen die für die Datenverarbeitung Verantwortlichen darauf hin, die betroffenen Systeme unverzüglich mit allen aktuellen Sicherheitsupdates zu versorgen. Weiterhin mahnten wir an, die Systeme auf die Installation von Web Shells, Hintertüren, Schadsoftware usw. zu untersuchen. Dabei sollten nicht nur der Exchange-Server, sondern auch angrenzende IT-Systeme in Augenschein genommen werden. Neben der Anwendung automatisierter Werkzeuge zur Untersuchung der eigenen Systeme sollten die betroffenen Verantwortlichen sehr sorgfältig alle Protokolldateien auf unbefugte Aktivitäten prüfen. Von großer Bedeutung war für uns dabei, ob personenbezogene Daten (z. B. Nutzerdaten, Anmeldedaten, Adressbücher, E-Mails usw.) abgeflossen sind oder manipuliert wurden.

**Risiken bewerten, Systeme aktualisieren!**

Viele der von der Datenschutzverletzung betroffenen Stellen reagierten angemessen, professionell und zügig. In einigen Fällen jedoch fehlte den Verantwortlichen anscheinend das entsprechende Verständnis für die Situation. Die eingegangenen Meldungen nach Artikel 33 DS-GVO waren zum Teil unvollständig, nicht aussagekräftig oder in sich widersprüchlich. Auch ob und in welchem Umfang personenbezogene Daten abgeflossen waren, wurde nicht eindeutig mitgeteilt. Bei fünf dieser Stellen vertieften wir unsere Prüfungen. Daraufhin sicherten zwei Verantwortliche ihre volle Unterstützung bei der Aufklärung des Sachverhaltes zu. So reagierte einer von ihnen, in dessen IT-System Kriminelle Web Shells platziert hatten, nun mit einer umfassenden und vollständigen Meldung nach Artikel 33 DS-GVO. Die von ihm durchgeführten Analysen seiner IT-Systeme ließen erkennen, dass ein Abfluss personenbezogener Daten sowie Veränderungen in den Systemen nicht festgestellt werden konnten. Die nach dem Vorfall umgesetzten technischen und organisatorischen Maßnahmen waren zielführend und entsprachen den Empfehlungen des BSI. Zukünftig werden bei diesem Verantwortlichen Sicherheitsupdates unverzüglich eingespielt und die IT-Systeme engmaschig proaktiv auf unbefugte Zugriffe überwacht. Ein ähnliches Ergebnis konnten wir bei der zweiten betroffenen Stelle erreichen. Die drei anderen Verantwortlichen haben den Sachverhalt bislang immer noch nicht ausreichend aufgeklärt bzw. überhaupt nicht auf

unsere Nachfragen reagiert. Wir werden hierzu die nächsten Schritte prüfen und ggf. Sanktionsmaßnahmen einleiten.

Verantwortliche, die personenbezogene Daten verarbeiten, müssen ihre IT-Systeme kontinuierlich, systematisch, gründlich und detailliert daraufhin untersuchen, ob ungewöhnliche Vorfälle, unbefugte Zugriffe auf oder Manipulationen von Daten festzustellen sind. Sie müssen auch regelmäßig überprüfen, ob die von ihnen umgesetzten Sicherheitsmaßnahmen zum Schutz personenbezogener Daten noch wirksam sind oder aktualisiert werden müssen. Dies umfasst auch, die aktuelle Bedrohungslage stets zu beobachten, geeignete Schlussfolgerungen für den eigenen IT-Betrieb zu ziehen und ggf. unverzüglich Gegenmaßnahmen gegen Sicherheitslücken zu ergreifen.

## 2 Kurznachrichtendienst bei einer Pflegeeinrichtung

Bereits seit längerer Zeit beschäftigte uns eine anonyme Eingabe zu einer Pflegeeinrichtung. Darin wurden wir darüber informiert, dass Beschäftigte der Einrichtung den Nachrichtendienst WhatsApp für die Organisation ihrer Arbeit nutzten. Darüber hinaus sollten regelmäßig Fotos, auf denen die Bewohnerinnen und Bewohner der Einrichtung zu sehen waren, über den Dienst ausgetauscht worden sein. Weiter wurde angegeben, dass die Beschäftigten ihre privaten Mobiltelefone für diese Zwecke nutzten.

Wer die öffentliche datenschutzrechtliche Diskussion zu dem genannten Nachrichtendienst verfolgt, kommt schnell zu dem Schluss, dass diese Vorgehensweise die Anforderungen der Datenschutz-Grundverordnung in keinem Fall erfüllte. Bereits die allgemeinen Geschäftsbedingungen von WhatsApp schlossen eine geschäftliche Nutzung aus. Weiterhin war weder der Dienst mit seinen Datenübermittlungen in einen unsicheren Drittstaat für geschäftliche Zwecke rechtskonform nutzbar, noch ließen sich private Mobiltelefone hinreichend für die Verarbeitung sensitiver Daten der Pflegebedürftigen absichern, ohne dass die Besitzerinnen und Besitzer einen Teil ihrer Rechte an den Geräten aufgeben.

Im Verlauf der Vorgangsbearbeitung stellte sich heraus, dass zwei verschiedene WhatsApp-Gruppen eingerichtet waren: In der einen tauschten sich lediglich die Beschäftigten der Pflegeeinrichtung zu Terminen und zur Arbeitsorganisation aus. Die andere stand auch den Bewohnerinnen und Bewohnern sowie deren Angehörigen offen. Über sie wurden Informationen zum Leben in der Einrichtung sowie Gruppenbilder der Pflegebedürftigen publiziert – nach Darstellung des verantwortlichen Geschäftsführers, um das Gemeinschaftsgefühl zu stärken. Zwar war ihm „unwohl" bei der Nutzung von WhatsApp und privater Mobiltelefone für geschäftliche Angelegenheiten; seine Bedenken wogen jedoch nicht so schwer, dass er eine Alternative in Erwägung zog. Im Übrigen konnte er auch keine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten benennen, wirksame Einwilligungserklärungen zum Fertigen der Fotoaufnahmen lagen auch nicht vor.

Erst auf unser Tätigwerden und mehrere Nachfragen hin, schien ein Umdenken einzusetzen. Die Pflegeeinrichtung teilte uns mit, dass der Kurznachrichtendienst in der Zwischenzeit gewechselt worden war. Das neu ausgewählte Produkt habe einen stärkeren Fokus auf Zusammenarbeit und könne neben dem Versand von Nachrichten, Terminen und Aufgaben auch verschiedene Kalender, Projektmanagementfunktionen sowie einen Cloud-Speicher zum Teilen von Dateien integrieren.

Auch hier hatten wir allerdings Grund zur Nachfrage. Zum einen interessierte uns der Vertrag zur Auftragsverarbeitung, zum anderen wollten wir wissen, mit welchen Maßnahmen das Unternehmen den Anforderungen des Schrems II-Urteils[12] des Europäischen Gerichtshofs vom 16. Juli 2020 gerecht werden wollte. Hintergrund war, dass das Dienstleistungsunternehmen seinen Sitz in einem Land außerhalb des Europäischen Wirtschaftsraums ohne angemessenes Datenschutzniveau hat. Und erneut mussten wir darauf hinweisen, dass private Mobiltelefone nicht für geschäftliche Zwecke eingesetzt werden sollten.

Wie schon in der ersten Phase der Bearbeitung des Vorgangs dauerte es mehrere Monate, bis uns eine Antwort erreichte. Die Pflegeein-

12 Siehe Tätigkeitsbericht Datenschutz 2020, A V 2.

richtung bat jeweils um die Verlängerung der Antwortfrist, ließ diese dann jedoch verstreichen, sodass wir weitergehende Maßnahmen ankündigten. Die schließlich eingegangenen Antworten stellten uns erneut nur zum Teil zufrieden. Zwar hatte das Dienstleistungsunternehmen mit der Ergänzung seiner Standardverträge die Risiken, welche sich aus der Datenübermittlung in ein Drittland ergeben, durch Zusatzmaßnahmen zu beherrschen versucht. Auch hatte es diverse technische Vorkehrungen im Produkt verankert, die die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten sollten (wie z. B. verschlüsselte Datenübertragung und -speicherung für die Vertraulichkeit). Uns war jedoch unklar, welche konkreten Maßnahmen die Pflegeeinrichtung tatsächlich aktiviert hatte und welche nur als optional im Datenblatt des Produkts standen.

Letztlich haben wir den Vorgang mit einer Reihe dringender Hinweise an die Pflegeeinrichtung abgeschlossen. Insbesondere empfahlen wir, auf eine Dienstleisterin oder einen Dienstleister in einem Drittstaat zu verzichten und eine Lösung auf der eigenen IT-Infrastruktur oder bei einem Webhoster in Europa vorzuziehen. Vergleichbare technische Angebote mit ähnlichen Funktionen lassen sich in Deutschland für weniger als 10 Euro im Monat mieten. Unabhängig von der Wahl des Dienstleistungsunternehmens rieten wir u. a. dazu, Pseudonyme zur Benennung der Beschäftigten und der Pflegebedürftigen zu nutzen, eine Zwei-Faktor-Authentisierung für die Nutzeranmeldung einzurichten, Zugriffe zu protokollieren sowie die Speicherbegrenzung durch frühzeitiges automatisiertes Löschen durchzusetzen. Weiterhin forderten wir, in gemeinsam genutzten Kalendern lediglich abstrakte Angaben zu hinterlegen und z. B. bei Abwesenheit von Beschäftigten auf die Nennung des konkreten Abwesenheitsgrundes zu verzichten, da dessen Kenntnis aus arbeitsorganisatorischer Sicht nicht erforderlich ist. Die Nutzung privater Mobiltelefone sollte untersagt und dienstliche Geräte verwendet werden.

Eine Kontrolle der Umsetzung dieser Hinweise haben wir uns ausdrücklich vorbehalten. Wir machten auch deutlich, dass wir im Wiederholungsfall von unseren aufsichtsrechtlichen Befugnissen Gebrauch machen und insbesondere die Einleitung eines Ordnungswidrigkeitenverfahrens prüfen werden.

# 3 Videoüberwachung durch Privatpersonen

Um ihr Eigentum zu schützen, verwenden immer mehr Bürgerinnen und Bürger Videokameras. Die Geräte sind schnell gekauft und eingerichtet. Meistens werden gleich mehrere Kameras am Carport, an der Hausfassade, im Garten oder hinter den Fenstern der Wohnung installiert. So ist eine Rundumüberwachung möglich. Hiervon fühlen sich Nachbarinnen und Nachbarn, Passantinnen und Passanten oder andere Verkehrsteilnehmerinnen und Verkehrsteilnehmer jedoch häufig beeinträchtigt und beschweren sich bei unserer Behörde. In vielen Fällen zu Recht, denn mittels der Kameras wird oft nicht nur der eigene Garten, die eigene Grundstückszufahrt oder das eigene Fahrzeug gefilmt, der Erfassungsbereich geht weit darüber hinaus.

Der Einsatz von Kameras durch Privatpersonen kann unter eine Ausnahmereglung der Datenschutz-Grundverordnung fallen. Nach Artikel 2 Absatz 2 Buchstabe c Datenschutz-Grundverordnung (DS-GVO) wird das Datenschutzrecht nicht auf Datenverarbeitungen angewendet, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen werden (sogenanntes Haushaltsprivileg). Dies ist z. B. dann der Fall, wenn eine Tätigkeit keinen beruflichen oder wirtschaftlichen Bezug aufweist (Erwägungsgrund 18 DS-GVO). Soweit sich eine Videoüberwachung auch nur teilweise auf den öffentlichen Raum erstreckt oder Dritte auf einem Privatgrundstück erfasst werden, die dieses in befugter Weise betreten, findet die Ausnahmeregelung keine Anwendung.

Für Privatgrundstücke bedeutet dies, dass die Erlaubnis, das Grundstück zu beobachten, grundsätzlich an dessen Grenze endet. Fehlt es an einer Umfriedung, kann ein Privatgrundstück einem öffentlich zugänglichen Raum gleichen. Dies kann dazu führen, dass beispielsweise Kinder, deren Schutzbedürfnis nach der Verordnung besonders zu berücksichtigen ist, versehentlich in den Erfassungsbereich geraten können. Vorkehrungen, wie beispielsweise Zäune, Hecken, Absperrketten oder Pflanzkästen erlauben Verantwortlichen, eine Begrenzung nach außen hin ausreichend kenntlich zu machen. Zusätzlich schafft ein entsprechendes Hinweisschild Klarheit.

Ermöglicht die Kamera jedoch einen Blick über einen Zaun auf ein angrenzendes Grundstück oder öffentliches Straßenland, liegen die Voraussetzungen des Haushaltsprivilegs nicht vor. In diesem Fall beurteilt sich die Zulässigkeit der Videoüberwachung anhand der Vorschriften der Datenschutz-Grundverordnung. Unsere Prüfungen derartiger Fallkonstellationen ergaben, dass die Datenverarbeitungen überwiegend nicht auf eine Rechtsgrundlage gestützt werden konnten. Wir forderten die verantwortlichen Kamerabetreiberinnen und Kamerabetreiber dazu auf, die Erfassungsbereiche der Geräte derart zu beschränken, dass nur noch das eigene Grundstück erfasst wird. Dies lässt sich beispielsweise dadurch erreichen, dass die Kamera geschwenkt oder ein Teilbereich der Kameralinse abgedeckt bzw. abgeklebt wird. Eine weitere Möglichkeit besteht darin, die unzulässig erfassten Videobildbereiche in der Kamera elektronisch zu maskieren. Das bedeutet, dass die Bilddaten von Nachbargrundstücken oder des öffentlichen Raumes technisch erst gar nicht erhoben werden. Eine nach der Erhebung vorgenommene Verpixelung oder Maskierung wäre hierfür nicht ausreichend.

Gleiches gilt, wenn in einem privaten Haushalt systematisch Dritte – wie beispielsweise Pflegekräfte oder Reinigungskräfte – also Personen, die nicht der privaten familiären Sphäre der Betreiberin oder des Betreibers zuzurechnen sind, mittels der Kameras überwacht werden. Auch hier gilt das Haushaltsprivileg nicht. Die Zulässigkeit ist an Artikel 6 Absatz 1 DS-GVO zu messen. Wir empfehlen, die Beobachtung oder Bildaufzeichnung für den Zeitraum der Anwesenheit der Dritten zu unterbrechen.

## Enge Grenzen beim Einsatz von Videokameras

Beim Filmen eines auf öffentlichem Straßenland parkenden Kraftfahrzeugs verhält es sich ähnlich. Zwar ist es nachvollziehbar, dass Besitzerinnen und Besitzer ihre Fahrzeuge schützen möchten. Allerdings rechtfertigt dies nicht die damit verbundene Erfassung des öffentlichen Verkehrsraums, der von einer Vielzahl haushaltsfremder Personen genutzt wird. Zudem ist das Recht, öffentlich zugängliche Räume zu beobachten, wie etwa Straßen und Plätze, ausschließlich der Polizei vorbehalten. Diese Befugnis darf sich eine Privatperson nicht zu eigen machen, um

beispielsweise selbsttätig Beweismittel für Sachbeschädigungen zu sammeln.

Problematisch gestaltet sich auch der Einsatz von Wechselsprechanlagen mit eingebauten Kameras. Mit sogenannten Klingelkameras bezwecken die Verantwortlichen, Besucher zu identifizieren. Der Betrieb einer Klingelkamera ist häufig der privaten bzw. familiären Sphäre des Verantwortlichen zuzurechnen. Voraussetzung ist allerdings, dass der private Zweck durch die äußeren Umstände erkennbar wird. Der Bundesgerichtshof hat bereits in seinem Urteil vom 8. April 2014, V ZR 210/10, Kriterien festgelegt. So dürfen Videobilder erst nach Betätigung der Klingel und allein in die angeklingelte Wohnung übertragen werden, eine Speicherung der Bildaufnahmen muss ausgeschlossen sein und die Bildübertragung muss nach einigen Sekunden automatisch unterbrochen werden. Aus unserer Sicht darf zudem räumlich nicht mehr abgebildet werden, als beispielsweise ein Blick durch einen Türspion gewähren würde. Eine dauerhafte und anlasslose Bildübertragung öffentlicher Bereiche muss technisch ausgeschlossen sein.

Bürgerinnen und Bürger, die beabsichtigen, eine Videokamera zum Schutz ihres Eigentums und Besitzes einzusetzen, sollten sich zuvor gut über die Zulässigkeitsvoraussetzungen informieren. So vermeiden sie Beschwerden aus der Nachbarschaft oder von anderen betroffenen Personen sowie ein aufsichtsbehördliches Verfahren. Zu beachten ist, dass eine unzulässige Datenverarbeitung nach Artikel 83 DS-GVO eine Ordnungswidrigkeit darstellt und mit einer Geldbuße geahndet werden kann.

Hilfreiche Informationen sind den Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte des Europäische Datenschutzausschuss und der Orientierungshilfe Videoüberwachung durch nicht öffentliche Stellen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu entnehmen. Diese Dokumente sind in unserem Internetangebot abrufbar.

# 4 Angriffe mit gestohlenen Nutzerdaten

Angriffe auf IT-Systeme sind heute alltäglich. Gerade weltweit agierende Internetplattformen für soziale Netzwerke, den Handel von Waren, touristische Angebote, Fitnesskurse, Weiterbildungen, Diskussionsforen usw. sind häufig Ziel solcher Angriffe, da sie in der Regel eine Vielzahl an personenbezogenen Daten verarbeiten. Kriminelle versuchen dabei u. a., Nutzernamen und Passwörter zu erbeuten, die später in Untergrundforen gehandelt und missbraucht werden. Im Berichtszeitraum wurde bekannt, dass zwischen Juni 2020 und Juni 2021 über 5,3 Milliarden Datensätze von über 1 Milliarde Internetnutzerinnen und -nutzern im Zuge von Angriffen auf bekannte Internetplattformen „abhandenkamen."

Ein prominentes Resultat solcher Angriffe und ein Beispiel der anschließenden „Versilberung der Beute" ist die sogenannte Cit0day Breach Collection, die im November 2020 auf einer Webseite angeboten wurde. Diese Sammlung beinhaltete mehr als 23.000 Datenbanken mit Nutzerdaten zu über 226 Millionen eindeutigen E-Mail-Adressen. Neben diesen Adressen waren auch die zugehörigen Passwörter bzw. deren Hash-Werte verfügbar. Zum Teil enthielt die Datensammlung auch weitere Informationen wie Vor- und Nachnamen, Geschlecht und Telefonnummer der Nutzerinnen und Nutzer.

Die gestohlenen Daten machen es Kriminellen oft einfach, die Identität von anderen Personen auf der Internetplattform anzunehmen und in ihrem Namen bei den jeweiligen Anbieterinnen und Anbietern z. B. unbefugt Käufe zu tätigen, Verträge zu schließen oder über Phishing Mails gezielt das Vertrauen Dritter zu erschleichen. Den betroffenen Personen drohen nicht nur Ansehensverlust, sondern zum Teil auch rechtliche Probleme und finanzielle Schäden.

Eine weitere Form von Angriffen, die auf gestohlenen Nutzerdaten aufbaut, ist das so genannte Credential Stuffing. Hier probieren Kriminelle durch automatisierte Massenabfragen aus, ob erbeutete Zugangsdaten wie E-Mail-Adresse und Passwort auch auf anderen Internetplattformen eine Anmeldung ermöglichen. Gelingt dies, können sie unter der Identität des (oft ahnungslosen) Opfers selbst die

Dienste dieser anderen Plattformen nutzen und dort kriminelle Aktionen ausführen.

Im Oktober 2021 meldete uns eine Unternehmensgruppe, die u. a. einen Online-Marktplatz und eine Online-Gebrauchtwagenbörse betreibt, eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 33 Datenschutz-Grundverordnung. Sie berichtete über die Kompromittierung von insgesamt über 250.000 Nutzerkonten durch Credential Stuffing. Der Sicherheitsdienstleister hatte unbefugte Logins Dritter in dem genannten Ausmaß bemerkt und Alarm geschlagen. Die Unternehmensgruppe informierte die betroffenen Nutzerinnen und Nutzer, setzte deren Passwörter zurück und forderte sie auf, neue Passwörter zu vergeben.

Uns liegen außerdem mehrere Beschwerden vor, in denen die betroffenen Personen beklagen, dass ohne ihr Zutun in verschiedenen Chatverläufen auf der Plattform Nachrichten auftauchen. Darin hinterlegen vermeintliche Interessentinnen oder Interessenten für einen Kauf bzw. Verkauf eine Telefonnummer zur weiteren Abwicklung des Geschäfts und bitten um einen Anruf. Da es sich hierbei meist um eine ausländische Nummer handelt, werden betrügerische Absichten vermutet. Ob diese Beschwerden zu „Geisternachrichten“ mit dem gemeldeten Credential Stuffing zusammenhängen, wird derzeit noch geprüft. Auch der bezüglich der Datenschutzverletzung bestehende Sachverhalt ist noch nicht abschließend aufgeklärt.

Selbstverständlich sind Unternehmen, die Internetplattformen für viele Tausend oder Millionen Nutzerinnen und Nutzer betreiben, verpflichtet, sorgsam mit den ihnen anvertrauten Daten umzugehen und alles zu tun, damit die Vertraulichkeit und Integrität dieser Daten gewahrt sind. Die Unternehmen müssen auch Warnsysteme betreiben, durch die Missbräuche in der beschriebenen Art entdeckt werden können.

**Für jeden Internetdienst ein eigenes Passwort**

Allerdings kann auch jede Nutzerin und jeder Nutzer selbst dazu beitragen, dass Angriffe wie Credential Stuffing ins Leere laufen. Besonders wichtig ist in diesem Zusammenhang, auf jeder Plattform bzw. bei jedem Internetdienst ein anderes Passwort zu verwenden, da ansonsten die Kompromittierung

eines Zugangs alle anderen gefährden kann. Es sollten möglichst lange Passwörter gewählt werden, wobei zu beachten ist, dass manche Dienste nur die ersten 8 oder 10 Zeichen prüfen. Je kürzer das Passwort, desto mehr Klassen von Zeichen (wie Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen) sind zu verwenden. Um sich nicht viele verschiedene Passwörter merken zu müssen, ist die Nutzung eines separaten Programms zur Passwortverwaltung zu empfehlen (so genannte Passwort Manager oder Passwort Safes). Falls Internetdienste eine Zwei-Faktor-Authentisierung offerieren, sollte deren Nutzung erwogen werden – auch wenn der Aufwand der Anmeldung damit vergrößert wird.

## 5 Kontaktdatenerhebung in Brandenburg

Als Instrument zur Nachverfolgung von Infektionsketten findet sich die Verpflichtung der jeweils Verantwortlichen zur Erfassung von Kontaktdaten in jeder der im Berichtszeitraum beschlossenen, bisher insgesamt neun Landesverordnungen über den Umgang mit dem bzw. zur Eindämmung der Verbreitung des SARS-CoV-2-Virus. Allen Bestimmungen war gemein, dass Verantwortliche Vor- und Familiennamen, die Telefonnummer oder E-Mail-Adresse sowie Datum und Zeitraum der Anwesenheit der betreffenden Person zu erfassen hatten. Ferner war sicherzustellen, dass eine Kenntnisnahme der Angaben durch Unbefugte ausgeschlossen war.

Gleichwohl erreichten uns auch im zweiten Jahr der Pandemie zahlreiche Hinweise und Beschwerden betroffener Personen zu Verantwortlichen, die öffentlich einsehbare Listen, etwa am Eingang des Lokals, verwendeten oder aber personenbezogene Daten in einem Umfang abforderten, der über die gesetzlichen Vorgaben hinausging. So wurde häufig eine kombinierte Angabe von Telefonnummer und E-Mail-Adresse eingefordert oder zusätzlich nach dem Geburtsdatum oder der Wohnanschrift gefragt. In diesen Fällen wandten wir uns an den Verantwortlichen, erläuterten die jeweils einschlägige Rechtsgrundlage und gaben Hinweise zur rechtmäßigen Umsetzung der Anforderungen, welche überwiegend dankbar aufgenommen und umgesetzt wurden. Darüber hinaus veröffentlichten wir zu Beginn des Jahres auch Musterformulare und allgemeine Hinweise in

Form von „Häufig gestellten Fragen“ auf unserer Webseite. Diese aktualisieren wir seither regelmäßig, um die Verantwortlichen bei der Umsetzung der rechtlichen Anforderungen zu unterstützen.

Ungeachtet dessen gaben einzelne Beschwerden Anlass für weitergehende Untersuchungen. So stellten wir etwa in einem Verfahren fest, dass das verantwortliche Unternehmen zur Erfassung der Kontaktdaten zum Zweck der Nachverfolgung auf das bereits vorhandene Online-Buchungssystem zurückgriff. Durch die erhebliche Anzahl an aus dem bestehenden System für die Kontaktnachverfolgung generierten Datensätzen wurden jedoch nicht die datensparsamen, landesrechtlichen Vorgaben berücksichtigt. Zusätzlich erfolgte auch beim Ticket-Kauf vor Ort eine Erhebung nicht vorgesehener Datenkategorien mithilfe eines Papierformulars. Trotz der erfolgten Anpassung prüfen wir die Einleitung eines Bußgeldverfahrens.

Positiv anzumerken ist im Übrigen, dass mit der Änderung des § 5 Zweite SARS-CoV-2-Eindämmungsverordnung vom 23. November 2021 die Kontaktnachverfolgung nunmehr auch durch die Verwendung der datensparsamen Corona-Warn-App des Robert-Koch-Institutes erfolgen kann. Eine entsprechende Empfehlung hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder bereits im April 2021 ausgesprochen.

# 6 Auskunft zu Daten aus dem Beschäftigungsverhältnis

Jede Person hat das Recht, vom Verantwortlichen Auskunft darüber zu verlangen, ob er sie betreffende personenbezogene Daten verarbeitet. Wenn das der Fall ist, hat die betroffene Person u. a. einen Anspruch darauf zu erfahren, welche Daten dies konkret sind, für welche Zwecke die Daten verarbeitet, an welche Empfängerinnen und Empfänger sie weitergegeben und für welchen Zeitraum sie gespeichert werden. Das Auskunftsrecht ist in Artikel 15 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) enthalten und eines der wichtigsten Rechte betroffener Personen. Es ist Grundlage für die Ausübung weiterer Rechte (z. B. auf Berichtigung oder Löschung der Daten). Nur wer weiß, welche ihrer oder seiner Daten in welchen

Kontexten von einem Verantwortlichen verarbeitet werden, kann ihr oder sein informationelles Selbstbestimmungsrecht wahrnehmen.

Das Auskunftsrecht spielt auch in unserer Arbeit als Aufsichtsbehörde eine wesentliche Rolle. Immer wieder haben Kundinnen und Kunden, Bürgerinnen und Bürger, Beschäftigte oder Vereinsmitglieder Anlass zu Beschwerden – sei es, weil Verantwortliche gar keine oder nur verspätet Auskunft erteilen, die Auskunft falsch, unvollständig oder nicht nachvollziehbar ist oder über die Art und Weise der Bereitstellung einer Kopie der Daten gestritten wird.

So mussten wir uns im Berichtszeitraum mit der Beschwerde eines Beschäftigten befassen, der seinen Arbeitgeber aufforderte, ihm im Sinne des Artikel 15 Absatz 1 DS-GVO Auskunft über während des Beschäftigungsverhältnisses verarbeitete Daten zu erteilen. Konkret ging es dabei insbesondere um Nachweise für ein vermeintliches Fehlverhalten des Beschäftigten und Verstöße gegen interne Richtlinien, auf die das Unternehmen eine Kündigung gestützt hatte. Nach Auffassung des Beschäftigten waren dies lediglich pauschale Behauptungen ohne konkrete Belege. Ein faires Verfahren vor dem Arbeitsgericht, das über die Kündigung verhandelte, sei ohne die Nachweise nicht möglich. Darüber hinaus begehrte der Beschäftigte auch generell Auskunft zu seinen im Beschäftigungsverhältnis verarbeiteten Daten, da er auf Grund von Erfahrungen im Unternehmen datenschutzrechtliche Verstöße und intransparentes Verhalten des Arbeitgebers vermutete.

Wie uns der Rechtsbeistand des Beschwerdeführers mitteilte, hatte das Unternehmen zunächst nur abstrakt und pauschal durch Übersendung der internen Datenschutzerklärung für Beschäftigte auf das Auskunftsbegehren geantwortet. Diese Erklärung sollte nach Darstellung des Unternehmens alle relevanten Angaben enthalten. Es versteht sich jedoch von selbst, dass eine abstrakte Datenschutzerklärung, die allen Beschäftigten eines Unternehmens informativ zur Verfügung gestellt wird, die Auskunftsansprüche von Artikel 15 Absatz 1 DS-GVO nicht umfassend erfüllt. Sie kann beispielsweise keine konkreten Daten des Beschäftigten enthalten. Im vorliegenden Fall war auch zu bemängeln, dass keine weitergehende Auskunft über die Verarbeitung von Daten zum Nachweis der angeblichen

Pflichtverletzungen des Beschwerdeführers erteilt wurde. Insbesondere stand eine Weitergabe von Protokolldaten aus IT-Systemen und deren Auswertung durch einen Dienstleister mit Sitz in den USA im Raum.

Nachdem wir das Unternehmen zur Stellungnahme aufforderten, erhielten auch wir lediglich summarische und pauschale Angaben zur Verarbeitung von Beschäftigtendaten. Weiter teilte das Unternehmen uns mit, dass es die ordnungsgemäße anwaltliche Bevollmächtigung des Rechtsbeistands anzweifelte (im Gegensatz zum Arbeitsgericht) und deshalb zunächst nur mit der internen Datenschutzerklärung für Beschäftigte auf das konkrete Auskunftsbegehren geantwortet hatte. Allerdings habe man im Gerichtsverfahren mittlerweile alle notwendigen Informationen mitgeteilt. Falls noch Daten fehlten, solle der Beschwerdeführer sie doch benennen.

Es bedurfte mehrerer weiterer Schreiben, bis uns eine Reihe von Dateien zuging, die personenbezogene Daten des Beschwerdeführers enthielten und offensichtlich aus den internen IT-Systemen des Unternehmens exportiert worden waren. Die Daten waren bereits auf den ersten Blick weder vollständig noch hinreichend strukturiert. Begleitend hierzu erhielten wir vom Unternehmen eine summarische Auflistung aller möglichen Verarbeitungszwecke für Beschäftigtendaten, aus der jedoch nicht die für diese Zwecke jeweils verarbeiteten Datenkategorien ersichtlich waren. Gleiches galt auch für die möglichen Datenempfängerinnen und -empfänger. Aus deren reiner Aufzählung war nicht erkennbar, welche Stellen in welchem Verarbeitungskontext Daten welcher Kategorien erhielten. Hinsichtlich der Aufbewahrungsfristen der Beschäftigtendaten gab das Unternehmen lediglich pauschal an, dass sie drei bis sechs Jahre nach Beendigung des Arbeitsverhältnisses betragen – auch hier ohne jegliche Differenzierung nach Datenkategorien.

Insgesamt war diese Auskunft an den Beschwerdeführer nach unserer Auffassung nicht geeignet, seine Ansprüche aus Artikel 15 Absatz 1 DS-GVO angemessen zu erfüllen. Da zu erwarten war, dass das Unternehmen Auskunftsbegehren von Mitarbeiterinnen und Mitarbeitern systematisch in der vorliegenden Form beantwortete, haben wir es in einem weiteren Schreiben auf die unserer Ansicht

nach bestehenden Mängel hingewiesen. Insbesondere monierten wir, dass Daten(kategorien) nur exemplarisch aufgezählt wurden und betroffene Personen (hier: die Beschäftigten) nicht erkennen konnten, welche Kategorien von Daten für welche Zwecke verarbeitet, an welche Stellen die Daten weitergegeben und wie lange sie gespeichert werden. Insofern stellten wir fest, dass die Auskunft in struktureller Hinsicht nicht die gesetzlichen Anforderungen erfüllte, da keine Unterscheidung nach Verarbeitungssituationen oder -verfahren vorgenommen wurde. Sie genügte damit auch nicht den Ansprüchen von Artikel 12 Absatz 1 DS-GVO, der verlangt, dass betroffenen Personen die Informationen in präziser, transparenter und verständlicher Form zu übermitteln sind.

## Auskünfte an Betroffene müssen strukturiert sein

Offensichtlich war auch das Arbeitsgericht dieser Auffassung. Parallel zu unseren Aktivitäten verpflichtete es das Unternehmen u. a. dazu, die Auskunft an den Beschwerdeführer zu präzisieren und aufgeschlüsselt nach dem jeweiligen Verarbeitungsvorgang die o. g. Informationen wie Kategorien verarbeiteter Daten, Verarbeitungszwecke, Empfängerinnen und Empfänger sowie Aufbewahrungsfristen bereitzustellen.

Im Übrigen war auch die Aufforderung des Unternehmens an den Beschwerdeführer, er möge mitteilen, welche Daten in der Auskunft nach Artikel 15 Absatz 1 DS-GVO noch fehlen, aus datenschutzrechtlicher Sicht kritisch zu hinterfragen. Zwar verweist der Erwägungsgrund 63 der Datenschutz-Grundverordnung darauf, dass ein Verantwortlicher die Präzisierung des Auskunftsbegehrens verlangen kann, wenn er eine große Menge an Informationen über die betroffene Person verarbeitet. Er muss dabei aus unserer Sicht jedoch aktiv mitwirken und z. B. Verarbeitungskontexte oder -verfahren mitteilen, in denen personenbezogene Daten vorliegen können. Betroffene Personen wissen u. U. gar nicht, welche Daten zu welchen Zwecken vom Verantwortlichen verarbeitet werden, an wen diese Daten weitergegeben und wie lange sie gespeichert werden und können insofern eine Präzisierung manchmal gar nicht allein vornehmen.

# 7 Verlust von Akten – das Autodach ist keine sichere Datenablage

Im laufenden Berichtsjahr erreichten uns erneut viele Meldungen gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) zu Datenschutzverletzungen. Ein großer Teil der Meldungen hat technische Ursachen. Hierzu gehören z. B. Ransomware-Angriffe, bei denen gespeicherte Daten verschlüsselt und Lösegelder erpresst werden, oder unbefugte Zugriffe auf und Ausleitungen von personenbezogenen Daten an Kriminelle. Allerdings führt auch die Nichtbeachtung organisatorischer Regelungen immer wieder zu derartigen Vorfällen, etwa zum Diebstahl von IT-Geräten, dem Fehlversand von Unterlagen oder dem Verlust von Akten.

Eine Körperschaft öffentlichen Rechts hatte uns von Letzterem zu berichten. Sie meldete den Verlust einer Aktenmappe mit Daten eines Unternehmers. Der Inhalt war für die betroffene Person bedeutsam. Es handelte sich um eine vollständige Personalausweiskopie, Kontaktdaten und den Lebenslauf sowie Geschäftspläne, Vorhabensbeschreibungen und Planzahlen zur Neugründung eines Unternehmens. Eine derartige Mischung aus sensitiven Informationen in einer Akte erfordert bei Aufbewahrung und Transport normalerweise besondere Sorgfalt und Sicherheitsmaßnahmen im Rahmen von Artikel 32 Absatz 1 DS-GVO. Daher war es umso verwunderlicher, wie die Aktenmappe verloren ging: Der zuständige Beschäftigte des Verantwortlichen war im Außendienst unterwegs und nutzte einen Dienstwagen zum Transport der Unterlagen. Das Unglück geschah, als er in Ermangelung einer freien Hand die Aktenmappe auf das Autodach legte, um das Fahrzeug entriegeln zu können. Danach trat der Beschäftigte seinen Weg an. Die Dokumente lagen jedoch noch auf dem Autodach – zunächst jedenfalls. Während der darauffolgenden Fahrt nahmen der Pkw und die Aktenmappe allerdings verschiedene Wege. Am Zielort angekommen, bemerkte der Beschäftigte den Verlust und begab sich umgehend auf die Suche. Allerdings konnte er die Aktenmappe nicht wiederfinden.

Neben der besagten Meldung einer Datenschutzverletzung gemäß Artikel 33 DS-GVO bei uns informierte der Verantwortliche auch die betroffene Person gemäß Artikel 34 DS-GVO über den Verlust.

Er führte darüber hinaus intensive Sensibilisierungsmaßnahmen sowohl des Beschäftigten als auch der gesamten Belegschaft durch.

So bedauerlich der Vorfall ist, er zeigt auch einen wesentlichen Aspekt des technisch-organisatorischen Datenschutzes: Es reicht nicht aus, technische Sicherheitsmaßnahmen in den IT-Systemen umzusetzen und sich z. B. gegen Sicherheitslücken oder Angriffe von innerhalb oder außerhalb des Unternehmens bzw. der Behörde zu wappnen. Denn dabei wird allzu häufig außer Acht gelassen, dass der Mensch vor dem Bildschirm oder am Schreibtisch – oder in diesem Fall am Steuer des Pkw – Teil des Systems ist. Es bedarf stets zusätzlich auch organisatorischer Regelungen, einer kontinuierlichen Sensibilisierung aller Beschäftigten, der Einübung datenschutzgerechten Verhaltes und einer Kontrolle der Einhaltung der Regelungen.

Obwohl es sich bei diesem konkreten Vorfall offensichtlich um ein menschliches Versehen handelte, ist allen Verantwortlichen dringend zu empfehlen, die umgesetzten technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes regelmäßig zu überprüfen, zu bewerten und ihre Wirksamkeit zu evaluieren. Nur so können sie auch gegenüber uns als Aufsichtsbehörde nachweisen, alles getan zu haben, um Datenschutzverletzungen zu verhindern.

## 8 Geburtsdatum auf Dienstausweisen

Ein Mitarbeiter eines Jobcenters beschwerte sich darüber, dass sein Geburtsdatum auf dem Dienstausweis angegeben war. Er hielt dies zur Erfüllung seiner Amtspflichten und Legitimation gegenüber den Leistungsempfängerinnen und -empfängern für nicht erforderlich. Darüber hinaus sei dieses Datum geeignet, über eine Melderegisteranfrage Nachforschungen zu seiner Person anzustellen. Der Landkreis hatte die Erstellung der Dienstausweise per Dienstanweisung geregelt und sich dabei an die am 2. Juli 2009 erlassene „Richtlinie des Ministeriums des Innern über die Einführung einheitlicher Dienstausweise für die obersten Landesbehörden des Landes Brandenburg“ angelehnt. Mit Verweis auf die Richtlinie und ohne eigene Erforderlichkeitsprüfung verwehrte der Landkreis dem Beschwerdeführer, auf die Angabe des Geburtsdatums zu verzichten.

Sowohl die vorgenannte Richtlinie als auch die Dienstanweisung des Landkreises führen dazu, dass die Beschäftigten diese private Information bei Amtshandlungen offenbaren müssen, was aus Sicht der Landesbeauftragten nicht erforderlich ist.

Sinn und Zweck des Dienstausweises ist der Nachweis, dass es sich bei der Inhaberin oder dem Inhaber um eine Amtsperson handelt, die Aufgaben innerhalb ihrer Zuständigkeit wahrnimmt. Haben Dritte, wie z. B. Bürgerinnen und Bürger oder Unternehmen, Zweifel an der Inhaberschaft, ist über die Dienstausweisnummer jederzeit eine eindeutige Zuordnung zu der handelnden Person bei der Beschäftigungsbehörde möglich. Des Geburtsdatums auf dem Dienstausweis bedarf es hierfür nicht – unabhängig davon, ob die Amtsperson für eine Kommunal- oder die Landesverwaltung tätig wird.

Gegenüber dem Ministerium des Innern und für Kommunales haben wir daher angeregt, die Richtlinie aus dem Jahr 2009 zu überarbeiten und unseren Bedenken hinsichtlich der Erforderlichkeit des Geburtsdatums auf Dienstausweisen Rechnung zu tragen. Das Ministerium steht einer Änderung aufgeschlossen gegenüber; der Abstimmungsprozess mit den obersten Landesbehörden hierzu dauert jedoch noch an.

Den betroffenen Landkreis als datenschutzrechtlich Verantwortlichen haben wir aufgefordert, die Dienstanweisung entsprechend zu ändern und das Geburtsdatum auf dem Dienstausweis unkenntlich zu machen. Dieser Aufforderung kommt der Landkreis nach; die Dienstanweisung wird angepasst und die Ausweise werden ohne Geburtsdatum ausgestellt.

## 9 Unrechtmäßige Veröffentlichungen in Ratsinformationssystemen

Von mehreren Kommunen erhielten wir im Berichtszeitraum Meldungen gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) über eine unrechtmäßige Veröffentlichung personenbezogener Daten in Ratsinformationssystemen. Grundsätzlich wird ein solches System von der jeweiligen Kommunalverwaltung betrieben. Es dient

als Informationsquelle für Bürgerinnen und Bürger, aber auch für Gremienmitglieder, z. B. Gemeindevertreterinnen und -vertreter, über die in der Kommunalvertretung erfolgten Beratungen und Beschlüsse. Hierfür sollte es in einen öffentlichen Teil (für die interessierte Öffentlichkeit und ohne vertrauliche Unterlagen) und einen nicht öffentlichen Teil (für Gremienmitglieder und mit ggf. vertraulichen Unterlagen) unterteilt sein.

Allerdings kann es in bestimmten Fällen dazu kommen, dass Unterlagen, die eigentlich zur Erfüllung der Aufgaben der Kommunalvertreterinnen und -vertreter im Rahmen einer Gremiensitzung gedacht waren (z. B. Unterschriftenlisten von Bürgerbegehren), versehentlich im öffentlich zugänglichen Teil des Ratsinformationssystems publiziert werden, oder aber Dokumente hochgeladen werden, welche dort gar nicht erst hätten eingepflegt werden dürfen. Über ähnliche Fälle informierten wir bereits mehrmals in vorherigen Tätigkeitsberichten.[13] Wir nehmen die aktuellen Meldungen von Datenschutzverletzungen zum Anlass, nochmals auf mögliche Maßnahmen zur Verhinderung derartiger Vorfälle hinzuweisen.

Grundsätzlich muss vor dem Hochladen von Dokumenten in das Ratsinformationssystem geprüft werden, ob die hochzuladenden Dokumente personenbezogene oder personenbeziehbare Daten gemäß Artikel 4 Nummer 1 DS-GVO enthalten. Falls dies zutrifft, ist zu entscheiden, ob eine Rechtsgrundlage besteht, um die genannten Daten zu veröffentlichen. Dabei sollte die Verwaltung immer das Prinzip der Datenminimierung aus Artikel 5 Absatz 1 Buchstabe c DS-GVO berücksichtigen und nur die für den beabsichtigten Zweck unbedingt erforderlichen personenbezogenen Daten verarbeiten. Wir vertreten nach wie vor die Auffassung, dass insbesondere bei der Veröffentlichung von Beschlussvorlagen im Internet Vorsicht geboten ist. Das verwendete Formular sollte nur insoweit personenbezogene Daten enthalten, wie dies zur Vorbereitung auf die Sitzung und das Verständnis des Vorgangs erforderlich ist.

Zur Unterstützung der zuständigen Beschäftigten empfehlen wir, in Zusammenarbeit mit dem Datenschutzbeauftragten der Kom-

13 Tätigkeitsbericht 2016/2017, B 11.2, Tätigkeitsbericht Datenschutz 2019, A II 3, Tätigkeitsbericht Datenschutz 2020, A V 1.3.

munalverwaltung eine Checkliste zu erstellen oder zumindest eine Übersicht mit Kriterien, die für ein Hochladen von Dokumenten mit personenbezogenen Daten mindestens erfüllt sein müssen. Alternativ kann auch ein Prozess geschaffen werden, bei dem Dokumente vor dem Hochladen zusätzlich nachweislich (z. B. durch Unterschrift) von einer zweiten Person geprüft werden (Vier-Augen-Prinzip). Weiterhin sollten die Beschäftigten in regelmäßigen Schulungen nochmals auf die Notwendigkeit einer Prüfung der Unterlagen vor dem Hochladen hingewiesen und ihnen die o. g. Kriterien erläutert werden. Dabei sollte auch klar kommuniziert werden, dass die Beratung des Verantwortlichen gemäß Artikel 39 Absatz 1 DS-GVO eine wesentliche Aufgabe der bzw. des örtlichen Datenschutzbeauftragten und sie bzw. er im Zweifelsfall zu konsultieren ist.

**Vier Augen sehen mehr**

Falls es trotz der oben genannten Maßnahmen zu einer unzulässigen Veröffentlichung personenbezogener Daten im Ratsinformationssystem gekommen ist, müssen die betreffenden Dokumente unverzüglich entfernt werden. Es ist deshalb für die Administration der Inhalte stets eine Vertretung zu benennen, sodass die jeweilige Kommunalverwaltung entsprechend handeln kann. Weiterhin ist in diesem Fall zu prüfen, ob gemäß Artikel 33 DS-GVO eine Meldung an uns als zuständige Datenschutzaufsichtsbehörde abzugeben ist. Darüber hinaus empfehlen wir, eine Person zu benennen, die das Ratsinformationssystem regelmäßig stichprobenartig prüft, in der Vergangenheit eventuell unzulässig veröffentlichte Dokumente identifiziert und deren Löschung bzw. datenschutzgerechte Aufbereitung veranlasst.

## 10 Aufgedrängte Daten – Prüfpflichten öffentlicher Stellen vor der Datenübermittlung

Immer wieder kommt es vor, dass öffentliche Verwaltungen zusätzlichen Stellen Vorgangsinhalte zur Kenntnis geben. Diese Einbindung Dritter ist insbesondere bei der Nutzung von E-Mails mit wenigen Mausklicks, z. B. in Form der CC- oder BCC-Funktion, schnell mög-

lich. Soweit die ursprüngliche Korrespondenz personenbezogen ist, muss allerdings zunächst geprüft werden, ob und inwieweit die Voraussetzungen einer rechtmäßigen Übermittlung personenbezogener Daten an diese Stellen vorliegen.

Den Mitarbeiterinnen und Mitarbeitern der öffentlichen Verwaltung ist in aller Regel bewusst, dass für die Weiterleitung personenbezogener Daten in E-Mails eine Rechtsgrundlage erforderlich ist. Für öffentliche Stellen ist dies regelmäßig Artikel 6 Absatz 1 Satz 1 Buchstabe e Datenschutz-Grundverordnung (DS-GVO), entweder in Verbindung mit Artikel 6 Absatz 3 DS-GVO und einer spezialgesetzlichen Rechtsgrundlage oder mit § 5 Brandenburgisches Datenschutzgesetz (BbgDSG). Nicht immer scheint klar zu sein, dass in vielen Fällen ebenso zu prüfen ist, dass alle Empfängerinnen und Empfänger auch einen Rechtsgrund für den Erhalt der Daten besitzen, und dass es Konstellationen im Datenschutzrecht gibt, in denen die sendende Stelle selbst zu prüfen hat, ob dies der Fall ist.

## CC und BCC nicht ohne Rechtsgrundlage

Rechtliche Fehler entstehen beispielsweise, wenn die versendende Stelle die Reichweite ihrer Pflichten im Hinblick auf die Prüfung der Rechtmäßigkeit der Übermittlung verkennt oder die Erforderlichkeit einer Datenübermittlung lediglich annimmt, ohne sie ausreichend zu prüfen.

Viele Fälle im Berichtszeitraum betreffen das Auskunftsrecht der betroffenen Person nach Artikel 15 DS-GVO. Nach dieser Norm können betroffene Personen verlangen, dass ihnen eine Auskunft über ihre gespeicherten personenbezogenen Daten sowie über bestimmte, die Verarbeitung betreffende Informationen erteilt wird. Je nach Formulierung des Antrags kann dies sämtliche gespeicherten Daten betreffen oder auch nur einen Ausschnitt. Gemäß Absatz 3 der Vorschrift kann auch die Herausgabe von Kopien der Daten verlangt werden.

Die Landesbeauftragte prüft in diesen Fällen die Reichweite des Auskunftsanspruchs und den Umfang der herauszugebenden Daten. Dies soll auch die Antragstellerinnen und Antragsteller vor unrechtmäßigen (Teil-) Ablehnungen ihres Antrages schützen. Sie erlangt in

diesen Beratungsverfahren in der Regel keine Kenntnis über konkrete Daten der betroffenen Personen und dürfte dies mangels Erforderlichkeit in den meisten Fällen auch nicht. In Einzelfällen erbittet sie unter Umständen den Nachweis der fristgerechten Auskunftserteilung und geht ansonsten davon aus, dass der Verantwortliche gemäß den Hinweisen handelt.

Im Berichtszeitraum kam es in einem Fall dazu, dass eine Verwaltung uns die komplette Auskunft für einen Betroffenen nach Artikel 15 DS-GVO per E-Mail in Kopie zusandte. Dadurch erlangten wir Kenntnis des gesamten beauskunfteten Datensatzes. Nach Rücksprache stellte sich heraus, dass sich die versendende Stelle hierzu verpflichtet fühlte, da der Antragsteller ausdrücklich darum gebeten hatte, die Landesbeauftragte im Verfahren einzubinden. Das war in Form unserer beratenden Tätigkeit auch geschehen. Dass wir allerdings mehr als die Vollzugsnachricht erhielten, rügte der Betroffene umgehend.

Das Vorgehen der Behörde war rechtswidrig. Nach § 8 Satz 1 BbgDSG trägt die übermittelnde Stelle grundsätzlich die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten. Die Landesbeauftragte hatte nicht um die Übermittlung der beauskunfteten Daten selbst gebeten, sodass die Verwaltung deren Rechtmäßigkeit in allen Teilen selbst zu verantworten hatte. Sie musste eigenständig prüfen, ob die Datenweitergabe für die von uns tatsächlich erbetene Mitteilung, dass die Auskunft erteilt wurde, erforderlich war. Die Übersendung an uns war aber für die Durchführung dieser Auskunft nicht erforderlich. Daran änderte auch die Aufforderung des Antragstellers zur Einbindung der Landesbeauftragten nichts. Diese bezog sich erkennbar auf die rechtliche Unterstützung zur Durchsetzung des Auskunftsrechts, aber gerade nicht auf die Übermittlung der Inhaltsdaten. Daher ergab sich aus der Aufforderung auch keine ausdrückliche Einwilligung, uns den Einblick in personenbezogene Daten außerhalb des für eine Beratung Erforderlichen zu ermöglichen. Die Landesbeauftragte löschte im weiteren Verlauf die ihr übersandten Inhaltsdaten.

Wir empfehlen allen öffentlichen Stellen, die im Zuge der Erfüllung ihrer Aufgaben unaufgefordert personenbezogene Daten übermit-

teln, für alle Empfängerinnen und Empfänger einzeln zu prüfen, ob dort nicht nur ein Interesse an den Daten besteht, sondern ob die Speicherung der Daten für legitime eigene Zwecke erforderlich ist. Gegebenenfalls kann dies durch Rücksprache verifiziert werden. Im Zweifel ist auf eine vorherige Übermittlung zu verzichten.

# V Ausgewählte Beratungen

# 1 Weitere Erörterungen zum Einsatz von Microsoft Online-Diensten

Mit Produkten und Diensten des Unternehmens Microsoft setzen sich die Datenschutzaufsichtsbehörden seit mehreren Jahren auseinander. Wegen ihrer großen Verbreitung sowohl im öffentlichen als auch im nicht öffentlichen Bereich erhalten alle deutschen Aufsichtsbehörden von den ihrer Aufsicht unterstehenden Stellen immer wieder Beratungsanfragen zum Datenschutz bei der Verwendung von Microsoft-Produkten und -Diensten. Sie stehen deshalb in engem Austausch über ihre Erkenntnisse und Aktivitäten. Zu beachten ist dabei, dass die Zuständigkeit für die Aufsicht über das Unternehmen Microsoft in Deutschland beim Bayerischen Landesamt für Datenschutzaufsicht und in Europa bei der irischen Data Protection Commission liegt, jeweils begründet durch den Unternehmenssitz.

Wie im letzten Tätigkeitsbericht[14] ausgeführt, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) im September 2020 eine Arbeitsgruppe unter Leitung des Bayerischen Landesamtes für Datenschutzaufsicht und unserer Behörde eingerichtet. Deren Aufgabe ist es, weitere Gespräche mit Microsoft hinsichtlich der erforderlichen Anpassungen der vertraglichen Unterlagen für die Nutzung von Online-Diensten des Unternehmens an die gesetzlichen Anforderungen der Datenschutz-Grundverordnung (DS-GVO) sowie zur Umsetzung des Schrems II-Urteils des Europäischen Gerichtshofs[15] zu führen. Grundlage bilden dabei die Ergebnisse des Arbeitskreises Verwaltung der Konferenz, der eine Reihe von Mängeln in den Dokumenten festgestellt hatte.

**Weiter Klärungsbedarf bei Microsoft Cloud Diensten**

Die neue Arbeitsgruppe nahm zum Ende des vorigen Berichtsjahres die Gespräche mit Microsoft auf und erörterte im Berichtszeitraum mit dem Unternehmen fortlaufend die aus Sicht der Datenschutzkonferenz bestehenden vertraglichen Unzulänglichkeiten sowie mögliche Anpassungen. Diskussionsgegenstand waren die so genannten Online Service Terms in Verbindung mit dem Data Protection Addendum.

14 Tätigkeitsbericht Datenschutz 2020, A V 1.5.
15 Tätigkeitsbericht Datenschutz 2020, A V 2.

Die vorgenannten Dokumente bilden die vertraglichen Regelungen für die Nutzung eines oder mehrerer cloudbasierter Online-Dienste. Neben den unter dem Namen „Microsoft 365“ angebotenen Diensten für klassische Büroanwendungen (MS Office, Word, Excel, ...) sind die Festlegungen auch Grundlage z. B. für die Nutzung der Azure Cloud oder des Videokonferenzsystems MS Teams.

Zwar gibt Microsoft an, die Unterlagen erfüllten die Anforderungen von Artikel 28 DS-GVO zur vertraglichen Regelung der Auftragsverarbeitung und berücksichtigten insbesondere die Mindestvertragsinhalte nach Absatz 3 der Vorschrift. Allerdings wird dabei immer wieder auch auf andere bestehende Dokumente zur Beschreibung der bereitgestellten Dienste sowie der technischen und organisatorischen Maßnahmen verwiesen. Ohnehin erschweren die komplexe Struktur sowie mannigfaltige Querverweise die Prüfung und das Verständnis des Vertragswerks. Verantwortliche, die vor dem Einsatz der Online-Dienste den Vertragsbedingungen zustimmen müssen, sind oftmals überfordert, eigene Prüfungen der Rechtskonformität vorzunehmen. Ein Gegenstand der Gespräche der Arbeitsgruppe mit Microsoft war deshalb auch, ob und ggf. wie Vereinfachungen und Verbesserungen der Transparenz erreicht werden können.

Weiterhin bildeten die Einbindung von Unterauftragnehmerinnen und Unterauftragnehmern und die proaktive Information der Auftrag gebenden Verantwortlichen hierzu sowie die Verarbeitung personenbezogener Daten durch Microsoft für eigene Geschäftszwecke Schwerpunkte der Diskussionen. Beispiele für Letztere sind die Umsetzung der Rechnungslegung, die Gewährleistung und der Schutz der IT-Sicherheit, die ständige Verbesserung und Weiterentwicklung der Online-Dienste sowie die Erfüllung rechtlicher Verpflichtungen – hier gegenüber Behörden in den USA. Bei der Verarbeitung für eigene Geschäftszwecke agiert Microsoft als Verantwortlicher gemäß Artikel 4 Nummer 7 DS-GVO; sie ist nicht von der (weisungsgebundenen) Auftragsverarbeitung nach Artikel 28 DS-GVO umfasst. Stellen, die die Online-Dienste nutzen, müssen somit eine eigene Rechtsgrundlage haben, um personenbezogene Daten zur Verarbeitung für Microsofts eigene Geschäftszwecke an das Unternehmen zu übermitteln.

Zwar erlaubt Artikel 6 Absatz 1 Satz 1 Buchstabe f DS-GVO, personenbezogene Daten zu verarbeiten (hier: zu übermitteln), wenn es zur Wahrung der Interessen des Verantwortlichen oder einer bzw. eines Dritten (hier: Microsoft) erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Allerdings muss diese Abwägung auch tatsächlich durchgeführt werden. Für öffentliche Stellen, die Online-Dienste von Microsoft zur Erfüllung ihrer Aufgaben einsetzen wollen, ist die Regelung wegen Artikel 6 Absatz 1, letzter Satz DS-GVO gar nicht anwendbar.

Ohnehin fehlt es nach unserer Auffassung auch nach den bisherigen Gesprächen an einer hinreichenden Konkretisierung der durch Microsoft für eigene Geschäftszwecke verarbeiteten personenbezogenen Daten. Diese werden nach Aussage des Unternehmens nicht eigenständig durch Kundinnen und Kunden der Online-Dienste bereitgestellt, sondern erst bei Nutzung der Dienste auf den technischen Einrichtungen Microsofts erzeugt. Zwar soll es sich vielfach um statistisch aggregierte Daten handeln, eine durch Microsoft realisierte so genannte Deidentifizierung schließt eine Personenbeziehbarkeit aber nicht aus.

Für die Arbeitsgruppe überraschend passte Microsoft die Online Service Terms und das Data Protection Addendum im September 2021 inhaltlich an. Die vorherigen Diskussionen mit den Datenschutzaufsichtsbehörden fanden hier jedoch keinen Eingang. Gleichwohl war zum Ende des Berichtszeitraums geplant, die Gespräche mit dem Unternehmen fortzuführen, insbesondere auch zu Fragen der Umsetzung des Schrems II-Urteils. Dabei wird das bereits angekündigte „EU Data Boundary Program“ von Microsoft zu thematisieren sein, bei dem das Unternehmen beabsichtigt, alle Daten von Kundinnen und Kunden der Online-Dienste, die das wünschen, ausschließlich innerhalb der Europäischen Union zu verarbeiten.

Die kritische datenschutzrechtliche Betrachtung der Microsoft Online-Dienste betraf auch deren Einsatz im schulischen Umfeld.[16] Zumindest für das Land Brandenburg steht mit der Schul-Cloud eine datenschutzgerechte Alternative zur Verfügung. Wegen der

16 Tätigkeitsbericht 2020, A IV 5.

andauernden Corona-Pandemie, einer immer wieder drohenden Schließung von Schulen mit der Notwendigkeit, Distanzunterricht durchzuführen, aber auch im Kontext einer stärkeren Digitalisierung des Schulunterrichts überhaupt befasst sich eine Arbeitsgruppe der Ständigen Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (Kultusministerkonferenz) mit datenschutzrechtlichen Fragen des Einsatzes von Microsoft Online-Diensten. Die Arbeitskreise Schulen und Bildungseinrichtungen sowie Datenschutz-/Medienkompetenz der Datenschutzkonferenz unter Leitung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit berät die entsprechende Arbeitsgruppe der Kultusministerkonferenz bei der Vorbereitung der Gespräche mit Microsoft zur Nutzung der Online-Dienste im schulischen Umfeld. Auch hier sind wir auf Grund unserer Rolle in den bisherigen Gesprächen mit Microsoft eingebunden.

## 2 Datenspenden für die medizinische Forschung

Das Forschen mit medizinischen Daten ist nicht nur aufgrund der aktuellen Corona-Pandemie ein viel diskutiertes Thema. Gerade hinsichtlich der Verarbeitung personenbezogener Gesundheitsdaten ergeben sich besonders hohe Anforderungen an die Gewährleistung des Datenschutzes und der Informationssicherheit. Es ist daher in diesem Bereich besonders wichtig, den Grundsatz „Data Protection by Design – Datenschutz durch Technikgestaltung“ aus Artikel 25 Datenschutz-Grundverordnung (DS-GVO) zu beachten. Dieser Grundsatz bedeutet im Wesentlichen, dass bereits bei der Planung und Konzeption der Verarbeitung personenbezogener Daten datenschutzrechtliche Aspekte berücksichtigt sowie technische und organisatorische Maßnahmen zur Beherrschung möglicher Risiken vorgesehen werden müssen. Ein gemeinnütziges Unternehmen, das großen Wert auf die Umsetzung des Grundsatzes „Data Protection by Design“ legt, wandte sich mit der Bitte um Beratung an uns. Ziel des Projektes war die Umsetzung einer sogenannten Datenspende betroffener Personen für die medizinische Forschung. Für den Begriff „Datenspende“ gibt es derzeit keine allgemein anerkannte, feststehende Definition. Er wird hier im Sinne einer eigenverant-

wortlichen Weitergabe oder Freigabe von medizinischen Daten betroffener Personen für Forschungszwecke verstanden.

Im Fokus des Projekts stand auch das Erreichen eines möglichst hohen Datenschutzstandards. Es baut auf einer Plattform auf, über die wir im letzten Tätigkeitsbericht informierten.[17] Auf dieser Plattform können die Nutzerinnen und Nutzer medizinische Daten wie zum Beispiel Symptomtagebücher bei bestimmten Erkrankungen verschlüsselt speichern. Zur Anwendung kommt hierbei ein Zero-Knowledge-Ansatz, der dafür sorgt, dass ausschließlich die jeweilige Nutzerin oder der jeweilige Nutzer in der Lage ist, die eigenen Daten zu entschlüsseln und einzusehen. Im Berichtszeitraum sollten sie zusätzlich die Möglichkeit erhalten, ihre innerhalb der Symptomtagebücher gesammelten Daten freiwillig für medizinische Forschungszwecke zur Verfügung zu stellen. Voraussetzung dafür ist, dass die Nutzerinnen und Nutzer ihre Einwilligung erteilen, die medizinischen Daten in einer (separaten) Forschungsdatenbank speichern zu lassen. Auf diese Forschungsdatenbank dürfen sodann nur ausgewählte Forschungsprojekte, welche durch eine Ethikkommission benannt werden, zugreifen. Interessant sind hierbei die für eine datenschutzgerechte Gestaltung gewählten Ansätze:

## Daten freiwillig für die Forschung weitergeben

Das erste Problem entstand beim Erteilen der Einwilligung in die Datenspende. Eine Einwilligung in eine Datenverarbeitung muss stets in informierter Weise erfolgen. Das bedeutet, die betroffene Person muss sich der Tragweite ihrer Einwilligung bewusst sein und insbesondere wissen, welche ihrer Daten von welchen Verantwortlichen für welche Zwecke verarbeitet werden. Allerdings war im vorliegenden Fall zum Zeitpunkt der Einwilligung in der Regel noch unklar, welche zukünftigen Forschungsvorhaben mit den Daten wissenschaftlich arbeiten werden. Bei der sogenannten „breiten Einwilligung“ (Erwägungsgrund 33 DS-GVO) war es uns daher wichtig, dass Vorkehrungen getroffen werden, durch die Nutzerinnen und Nutzer rechtzeitig und umfassend über zukünftige Forschungsvorhaben informiert werden. Nur so besteht für sie die Möglichkeit, ihre Entscheidung ggf. zu revidieren und die Einwilligung zu widerrufen.

17 Tätigkeitsbericht Datenschutz 2020, A I 4.

Eine weitere wichtige Anforderung ergab sich daraus, dass die Daten in der Forschungsdatenbank möglichst keine Rückschlüsse auf die Identitäten der spendenden Personen zulassen sollen. Andererseits bestand das Ziel des Projekts darin, auch Langzeitstudien mit den gespendeten Daten zu ermöglichen. Hierfür war es wichtig, aktuelle Datensätze einer konkreten Person den bereits bestehenden Datensätzen dieser Person in der Forschungsdatenbank zuzuordnen. Eine Zuordnung ist darüber hinaus auch erforderlich, um die Rechte der betroffenen Personen wie zum Beispiel das Recht auf Vergessenwerden oder den Widerruf der Einwilligung innerhalb der Forschungsdatenbank umsetzen zu können. Die konkrete Realisierung dieser Anforderungen erfolgt im vorliegenden Fall mit einem ausgefeilten kryptografischen Konzept, welches letztendlich ausschließlich der Daten spendenden Person erlaubt, die Zuordnung ihrer Datensätze in der Forschungsdatenbank zur eigenen Identität herzustellen.

Allerdings ist es bei Langzeitstudien oder bei seltenen Krankheitsbildern nicht ausgeschlossen, dass durch die Verknüpfung und Verdichtung von Daten oder durch extrem seltene Beobachtungen eine Reidentifizierung konkreter Personen (z. B. mit Zusatzinformationen) doch möglich wird. Eine Idee im vorliegenden Projekt sieht vor, dass die Datensätze in der Forschungsdatenbank ständig auf ihre Reidentifizierbarkeit überprüft und notfalls leicht abgeändert werden. Dies kann jedoch die Qualität der Daten und indirekt die Forschungsergebnisse beeinflussen. Somit gilt es, einen Mittelweg zu finden. Da das Erkennen einer wahrscheinlichen Reidentifizierbarkeit ein sehr komplexes Problem ist und stark von der Struktur der Datensätze abhängt, entschied sich das Unternehmen, die regelmäßige Prüfung zunächst nur für Daten mit einfacher Struktur (wie zum Beispiel Symptomtagebücher) durchzuführen. Die Lösung dieses Problems für komplexe Datenstrukturen ist ein aktuelles Forschungsthema.

## 3 Schulung zur datenschutzgerechten Wahlwerbung

Kandidatinnen und Kandidaten sowie Parteien und politische Vereinigungen müssen z. B. im Wahlkampf oder bei der Öffentlichkeitsarbeit einige Vorkehrungen treffen, um alle Datenschutzvorschriften einzuhalten. Dies dient sowohl der Wahrung des Rechts der Bürge-

rinnen und Bürger auf informationelle Selbstbestimmung als auch der Integrität der Wahlen.

## Kein Freibrief im Wahlkampf

Im Vorfeld der Wahlen zum 20. Deutschen Bundestag am 26. September 2021 hat die Landesbeauftragte Vertreterinnen und Vertreter der in Brandenburg zur Wahl stehenden Parteien zu einer Schulung in Form einer Videokonferenz eingeladen. Zu Beginn der Veranstaltung führten wir kurz in die Grundzüge des relevanten Datenschutzrechts ein und erörterten die Bedeutung des nach Artikel 9 Datenschutz-Grundverordnung (DS-GVO) besonders schutzbedürftigen Datums der „politischen Meinung“. Der Schwerpunkt der Schulung lag in der Darstellung praxisnaher Fallvarianten aus unserer aufsichtsrechtlichen Tätigkeit. Insbesondere haben wir mit den Teilnehmerinnen und Teilnehmern besprochen, wie sie in datenschutzkonformer Weise die Kontaktdaten der Wahlberechtigten zum Zweck der Wahlwerbung erhalten können. Eine besondere Bedeutung kommt in diesem Zusammenhang der Vorschrift des § 50 Bundesmeldegesetz (BMG) zu. Danach dürfen die Meldebehörden den Parteien zu diesem Zweck während der Dauer von sechs Monaten vor der Wahl Auskünfte aus dem Melderegister erteilen. Davon sind unter anderem die vollständigen Namen und die Anschriften der Wahlberechtigten umfasst. Ausdrücklich hingewiesen haben wir auf deren Widerspruchsrecht gegenüber den Meldebehörden nach § 50 Absatz 5 BMG sowie auf die in Absatz 1 Satz 3 der Vorschrift verankerte, für die Parteien verbindliche Löschfrist von einem Monat nach der Wahl.

Ein weiterer Schwerpunkt der Schulung lag auf den datenschutzrechtlichen Herausforderungen bei der Nutzung von sozialen Netzwerken, Messengerdiensten oder Videokonferenzsystemen im Wahlkampf. Beispielsweise war zu klären, was es bedeutet, für eine Präsenz in einem sozialen Netzwerk gemeinsam mit der Betreiberin oder dem Betreiber der Plattform im Sinne des Artikels 26 DS-GVO datenschutzrechtlich verantwortlich zu sein. Kann eine solche gemeinsame Verantwortung überhaupt übernommen werden, wenn die Plattform nur unzureichende Informationen über die Verarbeitung personenbezogener Daten zur Verfügung stellt? Inwieweit steht das Schrems II-Urteil des Europäischen Gerichtshofs der

Nutzung von Plattformen mit Sitz in den Vereinigten Staaten von Amerika entgegen? Nach welchen Kriterien wird ein datenschutzkonformes Videokonferenzsystem ausgesucht? Welches Recht gilt für die Veröffentlichung von Abbildungen von Personen im Internet: Datenschutz- oder Kunsturheberrecht? Antworten auf diese Fragen finden sich teilweise bereits in verschiedenen Veröffentlichungen der Landesbeauftragten.[18]

Angesichts der positiven Resonanz der Teilnehmerinnen und Teilnehmer haben wir angeboten, unsere Beratung der Kandidatinnen und Kandidaten sowie der Parteien auch künftig mit dem Ziel fortzusetzen, einen rechtskonformen Umgang mit personenbezogenen Daten im Wahlkampf sicherzustellen.

Im Berichtszeitraum haben sich nur wenige Bürgerinnen und Bürger über die Verwendung ihrer Daten durch Parteien im Wahlkampf bei uns beschwert oder hierzu Fragen gestellt. In der Regel konnten wir diese mit Hinweisen auf die genannten Vorschriften des § 50 BMG beantworten. Insbesondere haben wir die Betroffenen über ihr Widerspruchsrecht gegenüber der Meldebehörde sowie über ihr Recht auf Auskunft zur Herkunft ihrer personenbezogenen Daten gegenüber den Parteien nach Artikel 15 DS-GVO informiert.

## 4 Betreiberwechsel bei der Schul-Cloud Brandenburg

Die Schul-Cloud des Potsdamer Hasso-Plattner-Instituts (HPI) hatte sich während der Corona-Pandemie im Land Brandenburg und darüber hinaus als wichtiges Werkzeug für die digitale Unterstützung des häuslichen Lernens und des Wechselunterrichts etabliert.[19] Mit dem Ende des vom Bundesministerium für Bildung und Forschung geförderten Forschungsprojekts wurde im Berichtsjahr auch der vom HPI durchgeführte Pilotbetrieb der Plattform eingestellt. Da wegen der weiter andauernden Pandemie und aufgrund genereller Digita-

18 Tätigkeitsbericht Datenschutz 2020, I 6 (Videokonferenzsysteme) und V 2 (Schrems II-Urteil) sowie Handreichung „Verarbeitung personenbezogener Daten bei Fotografien – Rechtliche Anforderungen unter der DS-GVO".

19 Tätigkeitsbericht 2016/2017, B 13.1.1, Tätigkeitsbericht Datenschutz 2019, A II 2 sowie Tätigkeitsbericht Datenschutz 2020, A IV 4.

lisierungsbestrebungen im Schulbereich eine derartige Plattform dauerhaft benötigt wird, war zu klären, ob und wie der Betrieb und die Weiterentwicklung trotz des Projektendes gewährleistet werden können.

Vor diesem Hintergrund schlossen die Länder Brandenburg, Niedersachsen und Thüringen im Juli 2021 ein Verwaltungsabkommen, in dem sie länderübergreifend den weiteren Betrieb sowie die bedarfsorientierte Fortentwicklung und Anpassung der Schul-Cloud als digitale Lehr- und Lernplattform vereinbarten. Die drei genannten Bundesländer beauftragten die Dataport, eine Anstalt des öffentlichen Rechts, als Rechenzentrumsdienstleister mit dem Cloud Hosting sowie dem inhaltlichen, organisatorischen und technischen Betrieb einschließlich der Weiterentwicklung der Schul-Cloud. Dataport übernahm auch einen Teil der Beschäftigten des HPI, die sich zuvor um die Schul-Cloud gekümmert hatten.

## Schul-Cloud weiter im Einsatz

In Brandenburg agiert das Ministerium für Bildung, Jugend und Sport seit dem 1. August 2021 als Betreiber der „Schul-Cloud Brandenburg“ und bietet allen Schulen deren Nutzung an (wie zuvor das HPI). Daneben erbringt das Landesinstitut für Schule und Medien Berlin-Brandenburg im Auftrag des Ministeriums Unterstützungsleistungen bei Anfragen von Lehrkräften oder Schülerinnen und Schülern im Zusammenhang mit der Nutzung der Schul-Cloud (1st Level Support). Aus datenschutzrechtlicher Sicht bestehen somit mehrere Auftragsverarbeitungsverhältnisse nach Artikel 28 Datenschutz-Grundverordnung (DS-GVO): Die Schulen, die die Schul-Cloud nutzen, sind Verantwortliche im Sinne von Artikel 4 Nummer 7 DS-GVO für die Verarbeitung der personenbezogenen Daten auf der Plattform und gleichzeitig Auftraggeberinnen einer Auftragsverarbeitung, nämlich des Betriebs der Schul-Cloud. Auftragnehmer ist in diesem Kontext das Ministerium, das wiederum zwei Unterauftragnehmer vertraglich gebunden hat – zum einen Dataport als Rechenzentrumsdienstleister für das Cloud Hosting und die Weiterentwicklung des Angebots und zum anderen das Landesinstitut für den 1st Level Support.

Das neue Betriebsmodell erforderte zunächst eine Anpassung des Auftragsverarbeitungsvertrages, den die Schulen nun nicht mehr

mit dem HPI, sondern mit dem Bildungsministerium als Betreiber der Schul-Cloud zu schließen haben. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten beider Seiten. Er wird ergänzt durch eine Reihe von Anlagen wie z. B. ein Muster für das Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DS-GVO, das die Schulen vorhalten müssen, sowie Beschreibungen der technischen und organisatorischen Maßnahmen nach Artikel 32 DS-GVO. Das Ministerium legte uns einen Vertragsentwurf vor, den wir kurzfristig prüften.

Aufgrund der Doppelfunktion des Bildungsministeriums, einerseits als oberste Schulaufsichtsbehörde zu agieren und gleichzeitig andererseits die Schul-Cloud Brandenburg zu betreiben und somit Dienstleister für die Schulen zu sein, war uns wichtig, dass in allen mit dem Ministerium abgeschlossenen Verträgen eine klare organisatorische Trennung zwischen beiden Aufgabenbereichen vorgeschrieben ist. Auf diese Weise soll eine Interessenkollision und Vermischung der Tätigkeiten vermieden werden. Im Übrigen ist es Schulen auch nur durch diese Trennung möglich, die Auftragsdurchführung beim Ministerium als Betreiber der Schul-Cloud gemäß Artikel 28 Absatz 3 Buchstabe h DS-GVO zu kontrollieren, da sie ansonsten als beaufsichtigte Stelle ihre eigene Aufsicht überprüfen würden.

Zur Vermeidung des aufwändigen Austauschs der Verträge mit jeder Schule haben wir dem Ministerium aus Praktikabilitätsgründen vorgeschlagen, einen einseitigen Vordruck für die Schulen unter Angabe des konkret bezeichneten Vertrages einschließlich eines Links zur aktuell gültigen Fassung zu erstellen. Jede Schulleiterin bzw. jeder Schulleiter bestätigt auf diesem Formblatt mit der Unterschrift den Vertragsabschluss und sendet es anschließend an das Bildungsministerium zurück.

Bei dem Muster zum Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO fielen uns teilweise sehr unspezifische Angaben auf. Dies betraf insbesondere die Fristen zur Löschung der Daten. Wir haben dem Ministerium empfohlen, die Schulen beim Erstellen eines Löschkonzeptes zu unterstützen und dabei die zum Teil bestehenden, speziellen landesrechtlichen Regelungen zur Dauer

der Verarbeitung aus § 12 Absatz 1 Datenschutzverordnung Schulwesen zu berücksichtigen und zu konkretisieren.

Hinsichtlich der von den Schulen zu ergreifenden technischen und organisatorischen Maßnahmen gemäß Artikel 32 DS-GVO wiesen wir darauf hin, dass aus unserer Sicht zusätzliche Schulungen und Sensibilisierungen der Lehrkräfte erforderlich sind, vor allem zu Passwortrichtlinien und der Umsetzung von Zugriffsbeschränkungen. Gleiches gilt auch für diejenigen Beschäftigten in Schulen, die die Administration der schulbezogenen Bereiche der Schul-Cloud vornehmen. Weiterhin erinnerten wir an die Fortschreibung der bereits bestehenden Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO, die wir wegen des großen Umfangs an personenbezogenen Daten von Kindern, die unter besonderem Schutz der Datenschutz-Grundverordnung stehen, und der Möglichkeit der Profilbildung in der Schul-Cloud für erforderlich erachten. Hier muss das Ministerium voraussichtlich wesentliche Unterstützung leisten.

Bereits die Präambel des Auftragsverarbeitungsvertrages zwischen den Schulen als Auftraggeberinnen und dem Bildungsministerium als Auftragnehmer und Betreiber der Schul-Cloud Brandenburg weist darauf hin, dass das Hosting der Lehr- und Lernplattform bei Dataport als Unterauftragnehmer stattfindet. Auch für dieses Unterauftragsverhältnis besteht ein Vertrag gemäß Artikel 28 DS-GVO. Vertragspartner sind auf der einen Seite als Auftraggeber die drei Bundesländer, die die Schul-Cloud weiter betreiben, und auf der anderen Seite Dataport als Auftragnehmer.

Allerdings gibt es in diesem Vertrag eine landesspezifische Abweichungsklausel für Brandenburg. Sie hängt mit unterschiedlichen Auffassungen der Länder zur Rolle des jeweiligen Ministeriums zusammen: Während Niedersachsen und Thüringen davon ausgehen, dass dort die Ministerien selbst Verantwortliche im Sinne von Artikel 4 Nummer 7 DS-GVO für die Datenverarbeitung in der Schul-Cloud sind, besteht in Brandenburg zwischen dem Ministerium und unserer Behörde Konsens, dass nur die Schulen die Rolle der Verantwortlichen im Sinne der genannten Vorschrift einnehmen können. Zwischen Bildungsministerium und Dataport besteht insofern lediglich ein Unterauftragsverhältnis. Aus den unterschiedlichen Auffas-

sungen resultieren entsprechende Änderungen im Vertragstext, die nur für Brandenburg gelten. Bei einer nochmaligen detaillierten Prüfung des Vertragstextes, die aufgrund der kurzfristigen Beteiligung unserer Behörde vor Vertragsabschluss nicht möglich war, stellten wir fest, dass trotz der oben genannten Abweichungsklausel an weiteren Stellen terminologische Unstimmigkeiten zur Bezeichnung der Rolle des brandenburgischen Bildungsministeriums auftreten. Aus Gründen der Rechtssicherheit regten wir eine dementsprechende Nachbesserung an.

## 5 Beitritt des Landes Brandenburg zum Pilotprojekt „Digitales Lernen unterwegs“

Seit 2020 erproben sieben Bundesländer unter Federführung von Nordrhein-Westfalen in dem Pilotprojekt „DigLu – Digitales Lernen unterwegs“ den Einsatz einer länderübergreifenden digitalen Infrastruktur zur Unterstützung der Bildung von Kindern beruflich Reisender. Das Projekt ist Bestandteil der Strategie „Bildung in der digitalen Welt“ der Ständigen Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland und wird aus Mitteln der Verwaltungsvereinbarung DigitalPakt Schule gefördert. Zielgruppe sind insbesondere Kinder von beruflich Reisenden, z. B. aus Schausteller-, Markthändler- oder Zirkusfamilien. Sie wechseln teilweise wöchentlich und oft über die Grenzen von Bundesländern hinweg die Schule. Hierdurch entstehen große Herausforderungen nicht nur für die Kinder selbst und ihre Eltern, sondern auch für die jeweiligen Schulen und die dortigen Lehrkräfte. Eine kontinuierliche Begleitung der Schullaufbahn, eine angemessene pädagogische Betreuung und eine zielgerichtete, individuelle Förderung waren bislang kaum umsetzbar. Das Projekt DigLu soll in einer digitalen Infrastruktur die Kontinuität des Lernens sichern, die Dokumentation der Lernentwicklung und der Leistungsbewertung gewährleisten und eine ortsunabhängige Nutzung vielfältiger Lehr- und Lernmaterialien ermöglichen.

Mittlerweile haben alle Bundesländer ihren Beitritt zum Projekt erklärt. Das Land Brandenburg wird sich ab dem 1. Februar 2022 mit zunächst 27 Kindern beruflich Reisender beteiligen, deren Stammschulen (also die Schulen am melderechtlichen Wohnsitz der Eltern)

sich in Brandenburg befinden. Vor diesem Hintergrund hat uns das Ministerium für Bildung, Jugend und Sport im Berichtszeitraum eine Vielzahl von Projektunterlagen zur datenschutzrechtlichen Prüfung zur Verfügung gestellt. Das Konzept sieht vor, dass die jeweiligen Bildungs- bzw. Kultusministerien zusammen mit den jeweiligen Stammschulen als gemeinsam Verantwortlicher im Sinne von Artikel 26 Datenschutz-Grundverordnung (DS-GVO) agieren. In dieser Konstellation soll ein Unternehmen mit Sitz in Deutschland als Auftragsverarbeiter gemäß Artikel 28 DS-GVO vertraglich gebunden werden, das den eigentlichen technischen Betrieb sicherstellt.

Im Mittelpunkt des Projekts steht die Ablösung des analogen durch ein digitales Schultagebuch. In diesem werden von der jeweiligen Stammschule erstellte, individuelle Lernpläne für die Schülerin bzw. den Schüler in den Fächern Deutsch, Mathematik, einer Fremdsprache und ggf. weiteren Fächern aufgenommen und den so genannten Stützpunktschulen, an denen das Kind im Verlauf der Reise zeitweise lernt, bereitgestellt. Die Lehrkräfte an den Stützpunktschulen dokumentieren im Schultagebuch die Schulbesuchstage, den Lernstand und die Lernfortschritte des jeweiligen Kindes. Für das Projekt DigLu ist lediglich die Verarbeitung eines Teils der Schüler- bzw. Elternstammdaten notwendig. Sie sind Bestandteil des digitalen Schultagebuchs. Die gesamte Schülerakte verbleibt genauso an der Stammschule, wie dort auch weiterhin die Führung des Klassenbuchs und die Notengebung erfolgen.

Das uns vom Ministerium übergebene Muster einer Einwilligungserklärung enthält Hinweise auf freiwillig auszufüllende Freitextfelder, mit denen sowohl die jeweilige Schülerin bzw. der jeweilige Schüler als auch die Eltern zusätzliche Daten in der DigLu-Umgebung hinterlegen können. Exemplarisch werden Profilbilder und eigene Angaben zu Lernschwierigkeiten oder zu Lebensumständen, die das Lernen beeinflussen, genannt. Wir haben das Ministerium auf die Gefahr hingewiesen, dass auf diese Weise mehr persönliche Daten als nötig preisgegeben werden. Darüber hinaus können diese Daten auch besonders sensitiv sein, etwa wenn es sich um Informationen zu gesundheitlichen Einschränkungen oder familiären Problemen handelt.

Das im Projekt DigLu entwickelte Datenschutzkonzept sieht bisher keine Datenschutz-Folgenabschätzung gemäß Artikel 35 DS-GVO vor, da das federführende nordrhein-westfälische Ministerium für Schule und Bildung das mit der Datenverarbeitung verbundene Risiko für die Rechte und Freiheiten der betroffenen Personen nicht als hoch eingestuft hat. Auch das brandenburgische Bildungsministerium war sich zunächst unsicher, ob nicht aufgrund der geringen Anzahl der am Projekt teilnehmenden Schülerinnen und Schüler, deren Stammschulen sich in Brandenburg befinden, auf eine Datenschutz-Folgenabschätzung verzichtet werden kann.

Aus unserer Sicht muss allerdings spätestens mit der Aufnahme des Routinebetriebs der IT-Systeme im DigLu-Projekt eine solche Datenschutz-Folgenabschätzung vorliegen. Dies ergibt sich zum einen aus den Empfehlungen des Europäischen Datenschutzausschusses, eines Zusammenschlusses der Datenschutzaufsichtsbehörden in Europa, die dieser von seinem Vorgängergremium übernommen hatte. Im Rahmen von Leitlinien[20] wurden bereits 2017 Kriterien erarbeitet, die Verantwortliche bei der Bewertung des Risikos einer Verarbeitung personenbezogener Daten und der Entscheidung über die Erforderlichkeit einer Datenschutz-Folgenabschätzung unterstützen. Im vorliegenden Kontext sind mehrere dieser Kriterien erfüllt, womit das Gesamtrisiko der Datenverarbeitung voraussichtlich als hoch zu bewerten ist:

- Minderjährige Schülerinnen und Schüler gehören zu den besonders schutzwürdigen betroffenen Personen. Dies ergibt sich beispielsweise aus Erwägungsgrund 75 DS-GVO. Die Verarbeitung ihrer Daten ist in der Regel mit einem hohen Risiko verbunden.

- Die Daten der Schülerinnen und Schüler enthalten z. B. Leistungsbewertungen und Aussagen zum Lernfortschritt, aus denen Schul- bzw. Zeugnisnoten abgeleitet werden.

- Die Verarbeitung kann vertrauliche oder höchstpersönliche Daten der Schülerinnen und Schüler umfassen, wie z. B. Gesund-

20 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“ (WP 248 rev.01), angenommen am 4. Oktober 2017, abrufbar in unserem Internetangebot.

heitsdaten, Daten zum Förder- und Unterstützungsbedarf, zu Lernschwierigkeiten und zu Lebensumständen oder Meinungen, die sie in Chats austauschen.

- Die Datenverarbeitung bezieht sich spätestens mit Aufnahme des Regelbetriebs auf eine große Anzahl betroffener Personen. Neben den Schülerinnen und Schülern sind dies auch Eltern sowie Lehrkräfte.

Zum anderen existieren vergleichbare Lösungen wie die Schul-Cloud Brandenburg[21] mit ähnlichen Kategorien von personenbezogenen Daten, teilweise ähnlichen Verarbeitungszwecken und ebenfalls einer großen Zahl betroffener Personen. Für dieses vergleichbare System steht bereits fest, dass von der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen ausgeht, sodass eine Datenschutz-Folgenabschätzung durchgeführt wurde.

Wir haben das Thema auch in dem zuständigen Arbeitskreis der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder angesprochen und sind dort auf Zustimmung gestoßen. Vor dem Hintergrund, dass mittlerweile alle Bundesländer dem DigLu-Projekt beigetreten sind, erscheint die länderübergreifende Durchführung einer Datenschutz-Folgenabschätzung sinnvoll. Wir gehen davon aus, dass die gegenwärtige Erprobungsphase des Projekts von den Verantwortlichen auch zu diesem Zweck genutzt wird.

## 6 Recherche in sozialen Netzwerken durch Ausländerbehörden?

Soziale Netzwerke stellen eine schier unerschöpfliche Quelle für personenbezogene Daten ihrer Mitglieder dar. Teilweise möchten auch öffentliche Stellen diese nutzen. Das Ministerium des Innern und für Kommunales bat uns daher um Auskunft, inwieweit eine Recherche durch die Ausländerbehörden in sozialen Netzwerken, insbesondere auf Facebook, zur Identitätsfeststellung, rechtmäßig ist. Es teilte mit, dass die eindeutige Feststellung der Identität einer ausländischen

21 Siehe A V 4.

Person für die Ausländerbehörden nicht nur, aber insbesondere auch zur Durchführung aufenthaltsbeendender Maßnahmen zwingend erforderlich sei, da eine ungeklärte Identität die zwangsweise Durchsetzung einer vollziehbaren Ausreisepflicht selbst bei Personen, die die öffentliche Sicherheit und Ordnung nachhaltig gefährden, unmöglich mache. Dies führe dazu, dass Personen, die eine zumutbare Mitwirkung an der Identitätserklärung absichtlich verweigern und bewusst falsche Angaben machen, bessergestellt seien, als diejenigen Personen, die ihren Pflichten nachkommen und dann in ihre Heimatländer (teilweise zwangsweise) zurückgeführt werden. Um dem entgegenzuwirken, sei die Identitätsklärung von herausragender Bedeutung.

Eine allgemeingültige Antwort zur Rechtmäßigkeit einer solchen Datenerhebung zur Identitätsfeststellung mittels sozialer Netzwerke konnten wir nicht geben, da es sich um Grundrechtseingriffe und somit Einzelfallentscheidungen handelt, die eine Verhältnismäßigkeitsprüfung am konkreten Fall benötigen. Die Anforderungen an eine solche Entscheidung haben wir in unserer Stellungnahme an das Ministerium wie folgt dargelegt:

- Grundsätzlich dürfen Behörden Informationen aus öffentlich zugänglichen Quellen beschaffen. Ob ein soziales Netzwerk als öffentlich zugängliche Quelle angesehen werden kann, hängt nicht zuletzt davon ab, ob es über einen geschützten Bereich verfügt, der es den Nutzerinnen und Nutzern ermöglicht, auszuwählen, wer welchen Inhalt einsehen kann. Nur soweit und solange der Zugang zu personenbezogenen Daten nicht an besondere Voraussetzungen, z. B. eine Gruppenzugehörigkeit geknüpft ist, handelt es sich um öffentlich zugängliche Quellen.

- Wenn eine Behörde personenbezogene Daten in sozialen Netzwerken verarbeitet, etwa durch eine Suchanfrage, ist sie hierfür Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DS-GVO) und darf dabei nur ein eigenes behördliches Nutzerkonto verwenden (soweit die Erstellung eines solchen behördlichen Kontos nach den Nutzungsbedingungen des sozialen Netzwerkes zulässig ist).

- Jede Verarbeitung personenbezogener Daten durch eine Behörde bedarf einer Rechtsgrundlage. Für behördliche Recherchen in sozialen Netzwerken zum Zweck der Identitätsfeststellung kommen Artikel 6 Absatz 1 Satz 1 Buchstaben c oder e, Absatz 2 und Absatz 3 Buchstabe b DS-GVO in Verbindung mit spezialgesetzlichen Vorschriften infrage. Ausländerbehörden sind gemäß §§ 86 ff. Aufenthaltsgesetz (AufenthG) befugt, die zur Aufgabenwahrnehmung erforderlichen Datenverarbeitungsvorgänge vorzunehmen. Hierbei dürfen sie gemäß § 49 AufenthG identitätsfeststellende Maßnahmen und sogar körperliche Eingriffe durchführen, soweit dies erforderlich ist.

- Grundsätzlich muss der Verantwortliche betroffene Personen gemäß Artikel 14 Absätze 1 und 2 DS-GVO informieren, wenn er personenbezogene Daten bei Dritten erhebt. Er muss Auskunft darüber geben, aus welcher öffentlich zugänglichen Quelle die Daten stammen, das heißt hier, in welchem sozialen Netzwerk sie erhoben wurden. Dies kann entweder im Vorfeld der Erhebung in Kombination mit den Hinweisen nach Artikel 13 Absätze 1 und 2 DS-GVO erfolgen oder gemäß Artikel 14 Absatz 3 Buchstabe a DS-GVO spätestens einen Monat nach der Datenerhebung.

Hinsichtlich der konkreten Anfrage des Ministeriums des Innern und für Kommunales waren jedoch auch die folgenden Punkte bei der Informationsgewinnung in den sozialen Netzwerken zu bedenken:

Prinzipiell ist eine Überprüfung der Authentizität und des Wahrheitsgehalts von Angaben in sozialen Netzwerken nicht möglich. So können Profile zu unbeteiligten Personen mit demselben Namen oder zu Personen führen, die unter falschem Namen auftreten. Angaben aus sozialen Netzwerken werden zudem nicht regulär verifiziert, sodass auch die Einhaltung des Grundsatzes der Richtigkeit der Daten aus Artikel 5 Absatz 1 Buchstabe d DS-GVO nicht gesichert ist.

Die Behörde müsste in der Regel auch eine Vielzahl von Profilen durchsuchen, um die jeweilige Person ausfindig zu machen. Somit wären Unbeteiligte durch die Recherche betroffen. Weiterhin würde sie durch das Durchsuchen der Profile eine Fülle an Informationen zu den betroffenen Personen erhalten, welche nicht für die Aufga-

benwahrnehmung notwendig sind. Wir haben erhebliche Zweifel, dass solche Recherchemaßnahmen dem Grundsatz der Datenminimierung aus Artikel 5 Absatz 1 Buchstabe c DS-GVO gerecht werden – selbst wenn es sich um Plattformen handelt, die ihren Sitz in der Europäischen Union oder einem Land haben, das einem Angemessenheitsbeschluss der Europäischen Kommission unterfällt. Im Fall des Netzwerkes Facebook oder anderer Plattformen mit Hauptsitz in den USA ist eine Nutzung für behördliche Recherchezwecke aus folgenden Gründen ohnehin ausgeschlossen:

## Soziale Netzwerke für Recherchen tabu

Durch die Benutzung eines sozialen Netzwerks werden Daten zu Interaktionen – etwa IP-Adresse, Zeitpunkt und -dauer sowie der Standort des genutzten Kontos, aber auch die getätigten Suchanfragen und Durchsuchungen von Profilen – durch das jeweilige Netzwerk erfasst und gespeichert. Die recherchierenden Behörden sind deshalb als verantwortliche Stellen verpflichtet, für geeignete Garantien zu sorgen, die einen angemessenen Schutz der personenbezogenen Daten bei ihrer Verarbeitung im und durch das soziale Netzwerk gewährleisten. Im Ergebnis des Schrems II-Urteils des Europäischen Gerichtshofs erfordert dies regelmäßig zusätzliche vertragliche, organisatorische und technische Maßnahmen, die gegenüber der Betreiberin oder dem Betreiber des Netzwerkes durchzusetzen sind.[22] Ob dies gelingt, dürfte fraglich sein.

Führt eine Ausländerbehörde Ordnungswidrigkeitenverfahren durch, wendet sie die entsprechenden Vorschriften aus dem Teil III des Bundesdatenschutzgesetzes (BDSG) an. Diese enthalten ähnliche Anforderungen, z. B. § 47 BDSG zu den Grundsätzen der Verarbeitung personenbezogener Daten, §§ 55, 56 BDSG zur Information betroffener Personen und §§ 78 ff. BDSG zu Datenübermittlung an Drittstaaten.

In Rücksprache mit den anderen Datenschutzaufsichtsbehörden des Bundes und der Länder zur erarbeiteten Rechtsauffassung teilten wir dem Ministerium des Innern und für Kommunales unsere grund-

22 Siehe A III 1.

sätzlichen Zweifel zur rechtmäßigen Durchführung der angefragten Recherchemaßnahme mit.

## 7 Zensus 2022 – Beratung und Kontrolle der Erhebungsstelle Berlin

Der Zensus ist eine für alle Mitgliedstaaten der Europäischen Union verpflichtende statistische Erhebung umfassender Daten über die Bevölkerung und die Wohnungssituation im Abstand von zehn Jahren.[23] In erster Linie werden hierfür vorhandene Daten aus Verwaltungsregistern genutzt und durch eine Stichprobe ergänzt. Die Erhebung findet jeweils zu einem bestimmten Stichtag statt. In Deutschland wurde der Zensus aufgrund der Corona-Pandemie um ein Jahr verschoben. Das Gesetz zur Verschiebung des Zensus legt als neuen Stichtag den 15. Mai 2022 fest.

Wie bereits beim letzten Zensus im Jahr 2011 begleiten wir die Vorbereitung und Durchführung des Zensus 2022 durch das Amt für Statistik Berlin-Brandenburg. Dazu zählt unter anderem die Kontrolle ausgewählter Erhebungsstellen, bei denen die Daten gesammelt und für die weitere statistische Aufbereitung verarbeitet werden. Den Anfang machten wir bereits im August 2021 mit der zentralen Erhebungsstelle für das Land Berlin, die ihren Sitz in der Bundeshauptstadt hat. Für diese und den zentralen Service des Zensus 2022 mietete das Amt ein separates Gebäude an, das gemäß den Erfordernissen der Sicherheit und statistischen Abschottung baulich angepasst wurde.

Die Leitung und Beschäftigte des Projektes Zensus 2022 gaben uns einen Einblick über den bisherigen Stand der Vorbereitungen und die weiteren Schritte der anstehenden Erhebungsphase. Das konstruktive Gespräch wurde genutzt, Probleme, die beim letzten Zensus auftraten, anzusprechen, um sie bei dieser Erhebung bereits im Vorfeld zu beheben. Im Verlauf des anschließenden Rundgangs konnten wir die getroffenen Sicherheitsmaßnahmen zur baulichen Abschottung

23 Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen (Amtsblatt der Europäischen Union L 218/14 vom 13. August 2008).

der Erhebungsstelle in Augenschein nehmen und Hinweise zu ergänzenden organisatorischen Maßnahmen geben.

Für das Jahr 2022 sind auch Kontrollen in den brandenburgischen Erhebungsstellen geplant.

## 8 Arbeit von Gemeindevertretungen unter Corona-Bedingungen

Die Corona-Pandemie hat auch im Berichtsjahr viele öffentliche Veranstaltungen sowie die Teilnahme an öffentlichen Sitzungen von Kommunalvertretungen verhindert. Ist die Öffentlichkeit solcher Sitzungen oder gar deren gesamte Durchführung beeinträchtigt, geht dies unmittelbar zu Lasten der Demokratie. Beschlüsse, die in öffentlicher Sitzung zu treffen sind, können sogar unwirksam sein, wenn sie unzulässigerweise unter Ausschluss der Öffentlichkeit gefasst werden.

**Öffentlichkeit während der Pandemie**

Bereits während der ersten Kontaktbeschränkungen im Jahr 2020 war es aufgrund des Infektionsschutzes in den meisten Fällen nicht mehr möglich, Publikum in angemessenem Umfang in die Sitzungssäle einzulassen. Teilweise waren auch die Präsenzsitzungen selbst undurchführbar.

Der Gesetzgeber reagierte hierauf mit der Schaffung des Brandenburgischen kommunalen Notlagegesetzes,[24] welches dem Ministerium des Innern und für Kommunales ermöglichte, durch Rechtsverordnung unter anderem abweichende Regeln zur Präsenz von Mitgliedern kommunaler Vertretungen und zur Herstellung der Sitzungsöffentlichkeit zu treffen. Von dieser Verordnungsermächtigung machte das Ministerium durch Erlass der Brandenburgischen Kommunalen Notlagenverordnung (BbgKomNotV)[25] Gebrauch.

24 Gesetz zur Sicherstellung der Handlungsfähigkeit der brandenburgischen Kommunen in außergewöhnlicher Notlage (BbgKomNotG) vom 15. April 2020, GVBl. I, Nr. 14.

25 Verordnung zur Aufrechterhaltung der Handlungsfähigkeit der kommunalen Organe in außergewöhnlicher Notlage (BbgKomNotV) vom 17. April 2020, GVBl. II, Nr. 19.

Diese bis zu ihrem Auslaufen am 30. Juni 2021 in Kraft befindliche Regelung führte neben der nunmehr Präsenzsitzung genannten Sitzungsform am üblichen Sitzungsort (§ 5 BbgKomNotV) die Form der Video- und die Audiositzung ein (§§ 6, 7 BbgKomNotV), bei denen Gemeindevertreterinnen und Gemeindevertreter jeweils von anderen Orten aus über Video- oder Telefonkonferenzsysteme teilnehmen. In allen genannten Sitzungsformen war die Zulassung von Publikum im Sitzungssaal nicht mehr die Voraussetzung für die Herstellung der Sitzungsöffentlichkeit. Dem Publikum sollte stattdessen „mindestens“ eine Verfolgung der Sitzung in Ton und gegebenenfalls Bild in einem anderen zugewiesenen Raum ermöglicht werden.

Im Zusammenhang mit diesen Regelungen erreichten uns im Berichtszeitraum deutlich mehr Anfragen – vornehmlich von Mitgliedern von Kommunalvertretungen und örtlichen Datenschutzbeauftragten – als im Jahr 2020. Dies erklären wir uns damit, dass sich der Bekanntheitsgrad dieser Regelungen – trotz eines entsprechenden Rundschreibens des Ministeriums des Innern und für Kommunales – vermutlich zunächst auf die Verwaltungsleitungen beschränkt hatte.

Wie auch in der Vergangenheit bezogen sich mehrere Beschwerden auf die fehlende individuelle Möglichkeit, das Gefilmtwerden bei Videositzungen abzulehnen. Bereits in Fällen, in denen Gemeindevertretungen sich nach § 36 Absatz 3 Kommunalverfassung des Landes Brandenburg (BbgKVerf) freiwillig entschließen, Videositzungen durchzuführen, besteht die Möglichkeit, das Gefilmtwerden durch individuellen Widerspruch zu vermeiden, nur so lange, bis die Gemeindevertretung einen Passus in ihre Geschäftsordnung aufnimmt, der Bildaufnahmen für zulässig erklärt. Besteht eine solche Geschäftsordnungsregelung, sind individuelle Ablehnungen des Gefilmtwerdens durch Inhaberinnen und Inhaber von Ämtern und Mandaten unbeachtlich.

Die Brandenburgische kommunale Notlagenverordnung war da eindeutiger: § 9 Absatz 3 BbgKomNotV, der sich auf alle Formen der Sitzung bezog, regelte ausdrücklich, dass § 36 Absatz 3 BbgKVerf nicht anzuwenden war. Dies folgte daraus, dass in den Fällen von § 36 Absatz 3 BbgKVerf die Gemeindevertretung über eine freiwillige Einführung der Bildaufzeichung bzw. -übertragung neben

einer bestehenden Sitzungsöffentlichkeit entscheidet, während die Sitzungsöffentlichkeit unter Pandemiebedingungen überhaupt erst hergestellt werden musste. Die Herstellung der Öffentlichkeit der Sitzung erfolgte per Norm; die Nutzung der Videotechnologie ergänzte nicht nur die Öffentlichkeit vor Ort, sondern ersetzte sie.

Ein weiterer Themenkomplex von Anfragen ergab sich weniger aus einer Änderung der Rechtslage, sondern vielmehr aus der ziemlich raschen Einführung von Videokonferenzsystemen in Kommunen. Er betraf die Sicherheit der personenbezogenen Daten während und nach der Übertragung. Zum einen war es vorgekommen, dass Dritte Videos, die per Livestream oder als archivierte Daten vorhanden waren, mitgeschnitten bzw. heruntergeladen und verändert hatten (z. B. durch kritische Kommentare in Wort und Schrift). Zum anderen stellte sich die Frage, welche datenschutzrechtlichen Maßnahmen die Kommunalverwaltung bei selbst angefertigten Audio- und Videoübertragungen beziehungsweise -aufzeichnungen zu beachten hat und wie weit die datenschutzrechtliche Verantwortlichkeit für die Livebilder beziehungsweise die archivierten Versionen reicht. Dazu haben wir wie folgt beraten:

- Es sind datenschutzgerechte Plattformen auszuwählen, das heißt solche, die die Gewähr insbesondere der Integrität der Daten für die Dauer der Ausstrahlung und möglichen Speicherung bieten. Zu vermeiden sind Plattformen, bei denen es zu einer Übermittlung der Daten in Staaten kommt, deren Datenschutzniveau unangemessen niedrig ist (z. B. Vereinigte Staaten von Amerika[26]), was insbesondere für die Nutzung von Facebook gilt. Bei einem Hosting auf Facebook ist eine etwa beabsichtigte Wahrung der Öffentlichkeit der Sitzung darüber hinaus schon deswegen gefährdet, weil es an der Verfolgung einer Sitzung Interessierten nicht zugemutet werden kann, sich zu diesem Zweck auf Facebook zu begeben. Im Zweifel sollte ein Hosting bei der Gemeinde oder auf Basis einer ordnungsgemäßen Auftragsverarbeitung in der Europäischen Union stattfinden.

26 Zu dem hier relevanten Schrems II-Urteil des Europäischen Gerichtshofs siehe Tätigkeitsbericht Datenschutz 2020, A V 2.

- Bei Präsenzsitzungen sind die für § 36 Absatz 3 BbgKVerf geltenden Schutzmaßnahmen (z. B. Kameraeinstellung, Platzierung Anwesender) gegenüber Personen einzuhalten, die nicht der Kommunalvertretung angehören. Pausen sind in keinem Sitzungsformat zu übertragen. Die Übertragung der nicht öffentlichen Teile der Sitzung ist in allen Formaten selbstverständlich zu unterlassen.

- Soweit Personen an Sitzungen von ihrem Wohnsitz aus teilnehmen, müssen sie selbst dafür Sorge tragen, ihre Umgebung so einzurichten, dass keine Rückschlüsse auf ihren Standort oder persönliche Lebensumstände gezogen werden können, falls sie das nicht wünschen.

- Die Kommunalverwaltung ist, soweit bei der Erhebung und Übertragung bzw. Speicherung der personenbezogenen Daten die rechtlichen Anforderungen der Datensicherheit eingehalten wurden, für die nachträgliche Veränderung der Videos durch Dritte auf deren Rechnern datenschutzrechtlich regelmäßig nicht verantwortlich, etwaige Ansprüche sind den Dritten gegenüber geltend zu machen.

Da die Notlagenregelungen zum 30. Juni 2021 außer Kraft traten, beeilte sich das zuständige Ministerium, die Übernahme von Vorschriften, die sich aus Sicht der Landesregierung bewährt hatten, in die Kommunalverfassung vorzubereiten. Die Landesbeauftragte wurde vor Erlass der Rechtsvorschriften wegen deren Datenschutzbezugs angehört. Anregungen aus unserer Stellungnahme hat das Ministerium in erfreulichem Umfang aufgenommen. Unter anderem gelang es, klarzustellen, dass

- die rechtliche Verantwortlichkeit für die Einhaltung der Nichtöffentlichkeit von Videositzungen gemäß dem neu eingefügten § 34 Absatz 1a BbgKVerf grundsätzlich bei der Kommunalverwaltung bleibt, auch wenn die Teilnehmenden durch geeignete Maßnahmen selbst dafür zu sorgen haben, dass die Sitzungsinhalte keiner anderen Person, die sich in der Umgebung aufhält, zur Kenntnis gelangen und

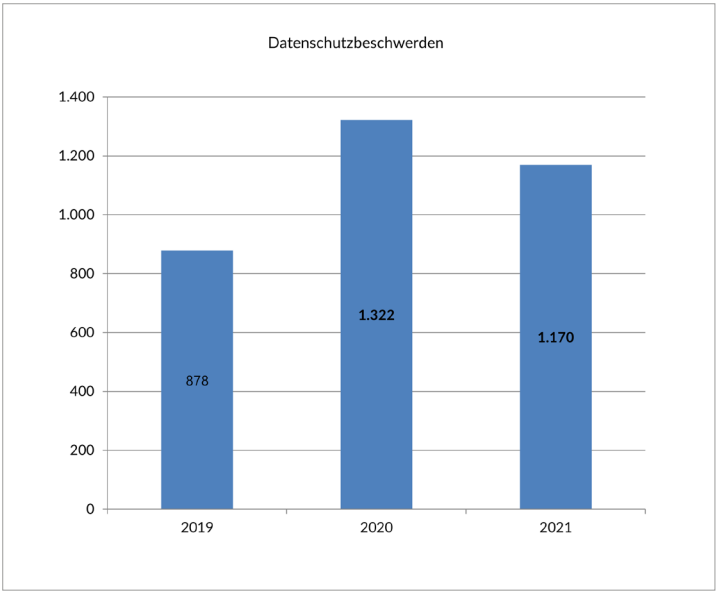
- der zunächst vorgesehene Vorrang der Videositzung vor der Audiositzung nicht als Regel formuliert wird, sodass eine Entscheidung für die Videositzung mit den Erfordernissen der Sitzungsumstände zu begründen ist. Wir hatten die pauschale Bevorzugung der Videositzung kritisiert, weil diese einen wesentlich tieferen Eingriff in das Recht auf Datenschutz darstellt und einer Begründung aus den Umständen nach dem Verhältnismäßigkeitsgrundsatz (Erforderlichkeitsprinzip) bedarf.

Die Änderungen der Kommunalverfassung des Landes Brandenburg traten zum 1. Juli 2021 in Kraft. Sie tragen in dieser schwierigen Zeit dazu bei, demokratische Transparenz in einer Form aufrechtzuerhalten, die die Datenschutzinteressen der Beteiligten nicht außer Acht lässt.

# VI Zahlen und Fakten

# 1 Beschwerden

Im Berichtszeitraum gingen bei der Landesbeauftragten – neben einer Vielzahl telefonischer – 1.170 schriftliche Beschwerden gemäß Artikel 77 Datenschutz-Grundverordnung ein. Diese wurden von Personen eingereicht, die der Ansicht waren, dass die Verarbeitung ihrer personenbezogenen Daten sie in ihren Rechten verletzt und gegen das Datenschutzrecht verstößt. Zwar bedeutet das einen Rückgang der eingereichten Beschwerden im Vergleich zum Vorjahr. Der erhebliche Anstieg der Beschwerden im Jahr 2020 ist aber insbesondere auf Datenverarbeitungen im Zusammenhang mit der Corona-Pandemie zurückzuführen, z. B. die Erhebung von Kontaktdaten, der Umgang mit Corona-Gästelisten, die verstärkte Einführung von Heimarbeit und die Nutzung von Videokonferenzsystemen in großem Umfang



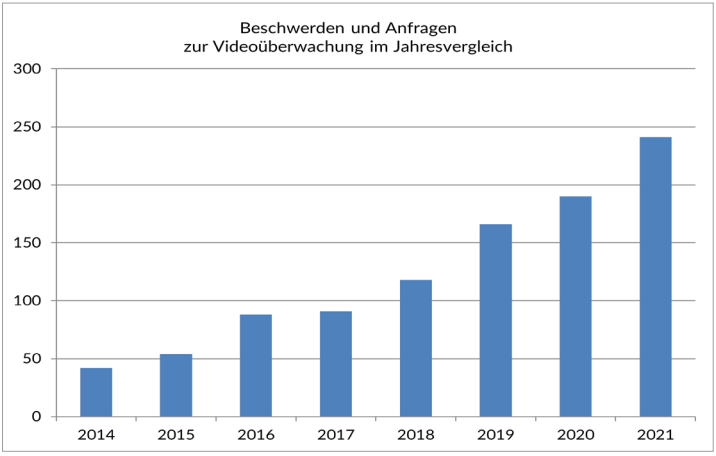
## 2 Beratungen

Neben der Bearbeitung von Beschwerden berät die Landesbeauftragte auch zu Datenschutzfragen. Im Berichtsjahr unterstützte sie in 555 Fällen betroffene Personen, Verantwortliche im öffentlichen wie nicht öffentlichen Bereich sowie die Landesregierung bei Rechtsetzungsverfahren. Auch hier lässt sich ein zahlenmäßiger Rückgang beobachten, dem höhere Anforderungen und eine gestiegene Komplexität im Einzelfall entgegenstehen. Einzelne Beratungen beinhalten die umfassende Begleitung von Projekten, z. B. bei der Realisierung von Vorhaben zur Umsetzung des Onlinezugangsgesetzes. Zudem ist es gelungen, zahlreiche telefonische Anfragen mündlich zu beantworten, ohne dass dies Eingang in die Statistik gefunden hätte.

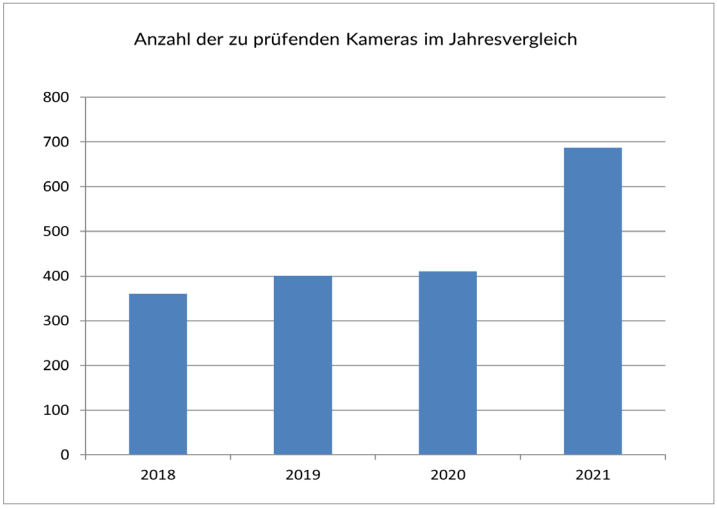
## 3 Videoüberwachung: Beschwerden und Anfragen

Seit Jahren verzeichnet die Landesbeauftragte eine Zunahme von Beschwerden und schriftlichen Anfragen zur Videoüberwachung durch Privatpersonen, Unternehmen und öffentliche Stellen. Richteten sich die Beschwerden lange Zeit noch überwiegend gegen Videoüberwachungen aus der Nachbarschaft, so stehen nun solche Kameras vermehrt im Fokus, die den öffentlichen Raum miterfassen. So wenden sich die Beschwerdeführerinnen und Beschwerdeführer an uns, weil sie sich durch Videokameras beispielsweise in der Sauna, im Schwimmbad, an Schiffsanlegestellen, in Pflegeheimen, auf Parkplätzen, Gehwegen und Straßen beobachtet fühlen und dies nicht hinnehmen möchten.

Im Berichtszeitraum erreichten uns insgesamt 241 Beschwerden und Anfragen. Dies stellt eine signifikante Steigerung im Vergleich zu den Vorjahreszeiträumen mit 190 Beschwerden und Anfragen im Jahr 2020 und 166 im Jahr 2019 dar. Die zahlreichen telefonischen Auskünfte haben wir nicht statistisch erfasst.




Mit jeder Videoüberwachung ist in der Regel der Einsatz mehrerer Kameras verbunden. Insofern waren im Jahr 2018 insgesamt 360 Videokameras, im Folgejahr 401, im Jahr 2020 411 und im Berichtszeitraum 687 Kameras auf ihre rechtliche Zulässigkeit und auf technisch-organisatorische Maßnahmen zu überprüfen. Dies bedeutet einen enormen Arbeitsaufwand, der mit den zur Verfügung stehenden personellen Ressourcen kaum zu bewältigen ist.



# 4 Meldungen von Datenschutzverletzungen

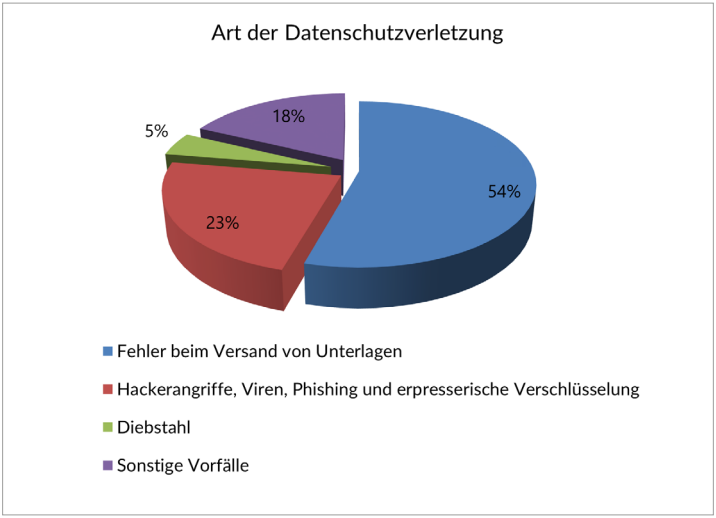
Artikel 33 Datenschutz-Grundverordnung verpflichtet Verantwortliche, eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihnen die Verletzung bekannt wurde, an die zuständige Datenschutzaufsichtsbehörde zu melden. Die Meldepflicht entfällt nur, wenn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

Im Berichtszeitraum erhielt die Landesbeauftragte insgesamt 510 Meldungen von Datenschutzverletzungen. Die gemeldeten Datenschutzverletzungen geschahen sowohl im öffentlichen (219 Meldungen) als auch im nicht öffentlichen Bereich (291 Meldungen).

Über die Hälfte aller Meldungen betraf den Fehlversand von Unterlagen (insgesamt 277 Fälle). Hiervon umfasst sind sowohl Fehlkuvertierungen von Briefpost, versehentlicher E-Mail-Versand an einen offenen Verteilerkreis, Namensverwechslungen oder die Beifügung von Unterlagen unbeteiligter Dritter. So verschickte beispielsweise eine Krankenkasse Abrechnungsunterlagen zu ärztlichen Behandlungen an den Namensvetter eines Versicherten.

Ein erheblicher Anteil der Meldungen (119 Meldungen) betraf Datenschutzverletzungen, die auf technischen Mängeln beruhen und insofern Virenbefall, Phishing, Hackerangriffe, unberechtigte Zugriffe Dritter und erpresserische Verschlüsselungen von Datensätzen ermöglichen. Hieran wird deutlich, dass Verantwortliche dem Einsatz und der Aktualisierung der technischen und organisatorischen Datenschutzmaßnahmen verstärkt Aufmerksamkeit widmen müssen. Ein Abhandenkommen physischer Datenträger, etwa Diebstähle durch Einbrüche in Räume des Verantwortlichen oder durch den Verlust auf dem Postweg, wurde der Landesbeauftragten in 23 Fällen gemeldet.

Die verbliebenen Fälle (91 Meldungen) verteilten sich auf verschiedene Gebiete des Umgangs mit personenbezogenen Daten.




# 5 Abhilfemaßnahmen

## 5.1 Warnungen, Verwarnungen, Anweisungen und Anordnungen

Gemäß Artikel 58 Absatz 2 Datenschutz-Grundverordnung sind die Aufsichtsbehörden befugt, gegen Verantwortliche vorzugehen, die entweder bereits gegen datenschutzrechtliche Vorschriften verstoßen haben oder die unmittelbar davor stehen, datenschutzrechtliche Bestimmungen nicht einzuhalten. Die Befugnisse umfassen u. a. die Möglichkeit, Warnungen, Verwarnungen, Anweisungen und Anordnungen auszusprechen. Insbesondere das Instrument der Warnung hat präventiven Charakter, da diese Maßnahme bereits im Vorfeld eines möglichen Datenschutzverstoßes genutzt werden kann. In diesem Fall ist der Rechtsverstoß noch nicht geschehen, würde aber verwirklicht, wenn der Verantwortliche mit seinem Handeln unverändert fortfährt. Im Gegensatz dazu rügt eine Verwarnung einen

zurückliegenden Datenschutzverstoß. Mit einer Anweisung oder Anordnung werden Verantwortliche zum konkreten Tun oder Unterlassen verpflichtet.

Eine Abhilfemaßnahme fasst dabei häufig mehrere Einzelfälle oder Verstöße zusammen. So kann beispielsweise bei einem großflächigen Areal mit einer großen Anzahl von Kameraüberwachungseinrichtungen eine Vielzahl unterschiedlich zu bewertender Überwachungsszenarien vorliegen. Das bedeutet für den Fall, dass die Bewertung des Betriebs mehrerer Kameras in einer Maßnahme zusammengefasst wird, trotzdem jeweils die Zulässigkeit jeder einzelnen Kameranutzung für sich geprüft und rechtlich beurteilt werden muss. Die bloße Zahl der Maßnahmen spiegelt daher nur teilweise die tatsächlich vorgefundenen Umstände wider.

Die Landesbeauftragte sprach im Berichtszeitraum 8 Verwarnungen und eine Anordnung aus.

## 5.2 Geldbußen

Im Berichtszeitraum wurden der Bußgeldstelle der Landesbeauftragten 57 Sachverhalte wegen Verstößen gegen datenschutzrechtliche Vorgaben zur Kenntnis gegeben. Die Verfahren wurden zu einem großen Anteil, nämlich in 46 Fällen, von den zuständigen Polizeibehörden oder Staatsanwaltschaften an die Bußgeldstelle weitergeleitet. 9 Sachverhalte haben aufsichtsbehördlich tätige Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten an die Bußgeldstelle abgegeben. Die beiden übrigen Fälle waren Abgaben anderer Aufsichtsbehörden mangels eigener dort bestehender Zuständigkeit.

Insgesamt 66 Verfahren, die sich sowohl gegen nicht öffentliche Stellen als auch gegen Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen richteten, hat die Bußgeldstelle im Berichtszeitraum abgeschlossen. Etwas weniger als die Hälfte dieser Verfahren war im Vorjahr eröffnet worden.

In 23 Fällen verhängte die Landesbeauftragte wegen der festgestellten datenschutzrechtlichen Verstöße ein Bußgeld. Die Gesamtsumme der festgesetzten Bußgelder betrug 13.430 Euro. In den übrigen

Fällen wurde entweder kein Ordnungswidrigkeitenverfahren eingeleitet, das Verfahren eingestellt oder mangels Zuständigkeit an die entsprechende Verfolgungsbehörde abgebeben.

## 6 Europäische Verfahren

Die Artikel 60 ff. Datenschutz-Grundverordnung (DS-GVO) sehen vor, dass bei grenzüberschreitender Datenverarbeitung eine europaweite Zusammenarbeit der Datenschutzaufsichtsbehörden erfolgen muss. Eine solche grenzüberschreitende Verarbeitung liegt zum Beispiel dann vor, wenn der Verantwortliche personenbezogene Daten von betroffenen Personen aus mehreren Mitgliedsstaaten verarbeitet oder verarbeiten lässt. Um die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden zu erleichtern, erfolgt der gegenseitige Austausch elektronisch über das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission. In diesem Rahmen hat die Landesbeauftragte in 1.404 Fällen geprüft, ob und welche Maßnahmen zu treffen sind:

In 561 Fällen, die von anderen europäischen Aufsichtsbehörden gemeldet worden, prüften wir allgemein, ob eine Zuständigkeit der Landesbeauftragten als federführende oder betroffene Aufsichtsbehörde in Betracht kommt und entsprechende Verfahrensschritte ergriffen werden müssen. Die Federführung orientiert sich dabei an der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen in der EU. Eine Betroffenheit ist demgegenüber dann gegebenen, wenn die gemeldete Verarbeitungstätigkeit durch die jeweiligen Unternehmen erhebliche Auswirkungen auf Bürgerinnen und Bürger im Land Brandenburg haben könnte oder die verantwortliche Stelle ihre Niederlassung im Zuständigkeitsbereich der Landesbeauftragten hat.

Eine Federführung der Landesbeauftragten haben wir in drei Fällen angenommen. Eine Betroffenheit der Landesbeauftragten ergab sich in 42 Fällen. In den übrigen Fällen haben wir nach Durchsicht entschieden, uns nicht an dem weiteren Verfahren zu beteiligen, da die Verantwortlichen keine Niederlassung in Brandenburg hatten und

keine Auswirkungen auf Brandenburgerinnen und Brandenburger festzustellen war.

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

In 831 Fällen beteiligten wir uns an Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII Datenschutz-Grundverordnung, etwa im Rahmen gegenseitiger Amtshilfe oder bei der Vorbereitung einer Stellungnahme des Europäischen Datenschutzausschusses. Davon gehen 11 auf die Initiative der Landesbeauftragten zurück.

Im Berichtszeitraum wurden 336 Kooperationsverfahren nach Artikel 60 DS-GVO (One-Stop-Shop-Verfahren) durch einen Beschluss der jeweils zuständigen, federführenden Aufsichtsbehörde abgeschlossen. 22 dieser Beschlüsse beruhen auf Prüfungen anderer deutscher Aufsichtsbehörden, einer geht auf die Landesbeauftragte zurück.

# 7 Förmliche Begleitung von Rechtsetzungsvorhaben

Aus den zahlreichen Beratungen ist die Begleitung legislativer Maßnahmen durch die Landesbeauftragte besonders hervorzuheben. Im Rahmen der insgesamt 555 Beratungen nahmen wir 37 Mal zu Gesetzen, Verordnungen, Satzungen oder Verwaltungsvorschriften Stellung. Bei im laufenden Jahr immer wieder anzupassenden Regelungen, etwa im Zusammenhang mit der Corona-Pandemie, erfolgte die Beratung gleich mehrfach, obwohl sie in der Statistik insgesamt nur einmal gewertet wurde.

Die rechtliche Grundlage zur Beteiligung der Landesbeauftragten folgt aus § 18 Absatz 5 Satz 1 Brandenburgisches Datenschutzgesetz. Danach ist sie vor dem Erlass von Rechts- und Verwaltungsvor-

schriften, die die Verarbeitung personenbezogener Daten betreffen, zu hören. Auch die Datenschutz-Grundverordnung überträgt in Artikel 57 Absatz 1 Buchstabe c den Aufsichtsbehörden eine Beratungsfunktion bei legislativen Maßnahmen.

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

# 1 Automatische Kennzeichenerfassung: Neue Rechtslage

Der in Brandenburg seit längerem schwelende Streit, ob das von der Polizei im sogenannten Aufzeichnungsmodus eingesetzte Kennzeichenerfassungssystem KESY als „technisches Mittel“ auf § 100h Strafprozessordnung gestützt werden kann, wurde im Januar 2021 durch einen Gesetzentwurf der Bundesregierung zur Fortentwicklung der Strafprozessordnung[27] zunächst beendet. Die Landesbeauftragte hatte entgegen der polizeilichen Praxis die genannte Vorschrift nicht als tragfähige Rechtsgrundlage für eine Speicherung unbegrenzt vieler Kennzeichen von miterfassten, aber unbeteiligten Dritten angesehen.[28] Der Gesetzentwurf stellte klar, dass unter Berücksichtigung der verfassungsgerichtlichen Rechtsprechung eine spezielle Ermächtigungsgrundlage für den Einsatz von automatischen Kennzeichenerfassungssystemen zu strafprozessualen Zwecken geschaffen werden muss. Durch den neu in die Strafprozessordnung eingefügten § 163g wurden die verdeckte, örtlich begrenzte und vorübergehende automatische Kennzeichenerhebung sowie ein Kennzeichenabgleich erlaubt. Voraussetzung ist, dass die Maßnahme von der Staatsanwaltschaft angeordnet, begründet und die ermittlungsrelevanten Kennzeichen genau bezeichnet werden. Alle erfassten Kennzeichen sind jedoch unverzüglich mit den zuvor in eine Fahndungsdatei eingepflegten Kennzeichen von Kraftfahrzeugen eines Beschuldigten oder mit diesem in Verbindung stehenden Personen automatisiert abzugleichen. Eine Speicherung erfolgt nur, wenn eine Übereinstimmung von gespeicherten und erfassten Kennzeichen zu einem Treffer führt und eine manuelle Nachprüfung diesen bestätigt. Alle anderen Kennzeichen müssen sofort und spurenlos gelöscht werden. Diese Verfahrensweise entspricht dem bisher in Brandenburg ebenfalls praktizierten Fahndungsmodus, der eine erheblich geringere Eingriffstiefe für das Recht auf informationelle Selbstbestimmung von Unbeteiligten aufweist. Die ganz überwiegende Zahl der Kennzeichen wird lediglich für den kurzen Moment des Abgleichs verarbeitet und, wenn kein Treffer vorliegt, unwiederbringlich gelöscht. Diese Kennzeichen stehen damit für

27 Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 22. Januar 2021, (Bundesrats-Drucksache 57/21).

28 Tätigkeitsbericht Datenschutz 2020, B 2.3.

weitere, auch rückwirkende Ermittlungen der Polizei nicht zur Verfügung. Mit dem Inkrafttreten des Gesetzes[29] zum 1. Juli 2021 blieb daher für den sogenannten Aufzeichnungsmodus kein Raum mehr. Die brandenburgische Polizei teilte uns folgerichtig mit, dass sie KESY seit diesem Zeitpunkt nicht mehr in diesem Modus nutzt.

Trotz dieser deutlichen Entscheidung des Bundesgesetzgebers, erklärte der brandenburgische Minister des Innern und für Kommunales bereits Mitte Juli 2021, dass die Pläne für den Einsatz von automatischen Kennzeichenerfassungssystemen im Aufzeichnungsmodus weiterverfolgt würden. Der Verlust des Aufzeichnungsmodus sei eine erhebliche Einschränkung für die wirksame Bekämpfung von grenzüberschreitenden Serientäterinnen und Serientätern. Der Innenminister kündigte daher an, im Brandenburgischen Polizeigesetz, das bisher nur den Betrieb von KESY im Fahndungsmodus vorsieht, eine der früheren Ermittlungspraxis entsprechende Befugnis zu schaffen.

# 2 Ausgewählte Fälle

## 2.1 Einstellung im Strafverfahren: Erforderliche Angaben bei Zahlungsauflage

Die Staatsanwaltschaft Potsdam hatte gegen die Beschwerdeführerin ein Strafverfahren geführt, das gegen eine Geldauflage gemäß § 153a Strafprozessordnung vorläufig eingestellt wurde. Um diese Auflage zu erfüllen, sollte sie einen Betrag an einen gemeinnützigen Verein überweisen und als Verwendungszweck die Formulierung „Auflage in dem Verfahren gegen … “ ergänzt um ihren vollständigen Namen eintragen. Sodann sollte sie den Nachweis der Überweisung gegenüber der Staatsanwaltschaft belegen. Die Beschwerdeführerin wehrte sich dagegen, dass dem Verein als Empfänger der Zahlung bei Befolgung dieser Vorgabe bekannt würde, dass gegen sie ein Ermittlungsverfahren geführt wurde. Zunächst erschien es uns unter dem Gesichtspunkt des Grundsatzes der Datensparsamkeit nicht einsich-

29 Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25. Juni 2021, BGBl. I 2021 Nr. 37, S. 2099.

tig, weshalb im Verwendungszweck eine namentliche Erwähnung der Betroffenen erforderlich sein sollte.

Unsere Nachfrage bei der Staatsanwaltschaft brachte jedoch die Erkenntnis, dass ohne Namensangabe eine datenschutzrechtlich nicht minder bedenkliche Situation entstehen kann. In den nicht seltenen Fällen, dass eine dritte Person die Geldauflage an die gemeinnützige Einrichtung überweist, besteht nämlich die Gefahr, dass die Zahlungsempfängerin oder der Zahlungsempfänger irrtümlich davon ausgeht, dass die überweisende Person gleichzeitig im Verfahren beschuldigt ist. Auch gegenüber dem Kreditinstitut, das die Überweisung ausführt, könnte diese Person als einer Straftat beschuldigt angesehen werden. Daneben ist es aus praktischen Gründen regelmäßig erforderlich, den Namen der oder des Beschuldigten zu nennen, damit eine eindeutige Zuordnung erfolgen kann. Zum einen ist die alleinige Angabe eines Aktenzeichens fehleranfällig, weil es immer wieder vorkommt, dass die gemeinnützige Einrichtung ein falsches Aktenzeichen bei der Rückmeldung der Auflagenerfüllung übermittelt. Zum anderen ist eine eindeutige Zuordnung einer Zahlung insbesondere in den Fällen erschwert oder unmöglich, in denen unter einem Aktenzeichen ein Verfahren gegen mehrere Beschuldigte geführt und Geldauflagen in gleicher Höhe verhängt oder Teilzahlungen geleistet werden. Beide Konstellationen bergen die Gefahr in sich, dass auch gegen eine oder einen Beschuldigten, die oder der die Auflage erfüllt hat, das Ermittlungsverfahren fortgesetzt wird.

Neben diesen Argumenten überzeugte uns die Tatsache, dass bei allen Überweisungen auf dem Kontoauszug der Zahlungsempfängerinnen oder Zahlungsempfänger auch der Name der Kontoinhaberin oder des Kontoinhabers offenbart wird, sodass zumindest in den Fällen, in denen Personenidentität besteht, kein verbesserter Schutz erreicht wird.

Da im konkreten Fall der gemeinnützige Verein als Zahlungsempfänger die personenbezogenen Daten der Beschwerdeführerin und die Information zum Grund der Zahlung nur zweckgebunden verarbeiten durfte, hielten wir unter Abwägung aller genannten Gesichtspunkte die Vorgabe, Verwendungszweck und Namen auf der Überweisung anzugeben, für zulässig.

## 2.2 Meldungen von Datenschutzverletzungen durch die Polizei

Wenn die Polizei in ihren eigenen Reihen eine Verletzung des Schutzes personenbezogener Daten bemerkt, muss sie diese unter bestimmten Voraussetzungen der Landesbeauftragten melden. Da sie eine Doppelfunktion erfüllt, also sowohl repressiv zur Strafverfolgung als auch präventiv zur Gefahrenabwehr tätig wird, richtet sich die Meldepflicht einer Datenschutzverletzung nach verschiedenen Normen, je nachdem, welchem Zweck die Datenverarbeitung bei der Polizei dient. Bei repressivem Tätigwerden bestimmt sich die Meldepflicht in der Regel nach § 500 Strafprozessordnung (StPO) i. V. m. § 65 Bundesdatenschutzgesetz (BDSG), bei präventivem Tätigwerden nach § 29 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG).

§ 65 Absatz 1 Satz 1 BDSG besagt, dass der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Bundesbeauftragten – in diesem Fall wegen § 500 Absatz 2 StPO der oder dem Landesbeauftragten – zu melden hat, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat.

Nach § 29 Absatz 1 BbgPJMDSG meldet der Verantwortliche eine Verletzung der Sicherheit personenbezogener Daten unverzüglich der oder dem Landesbeauftragten, es sei denn, es ist absehbar, dass die Verletzung nicht zu einer Beeinträchtigung der Rechtsgüter der betroffenen Person führt. Erfolgt die Meldung nicht innerhalb von 72 Stunden, so ist die Verzögerung zu begründen.

Im Berichtszeitraum gab es seitens der Polizei bei einigen Fallgruppen Abstimmungsbedarf über die Voraussetzungen einer Meldepflicht. Einige Beispiele stellen wir in den nachfolgenden Abschnitten vor:

### 2.2.1 Unbefugte Zugriffe auf Daten durch Bedienstete der Polizei

Die Polizei benutzt ihre polizeilichen Auskunfts- und Vorgangsbearbeitungssysteme zur Erfüllung der polizeilichen Aufgaben sowohl im repressiven als auch im präventiven Bereich. Immer wieder erhalten wir Kenntnis davon, dass diese Systeme zweckwidrig, etwa aus privaten Motiven wie Neugier, verwendet werden.[30] Fraglich war daher, ob ein unbefugter Abruf personenbezogener Daten durch Polizeibeamte eine meldepflichtige Datenschutzverletzung darstellt.

**Auch Polizei muss Datenschutzverletzungen melden**

Im repressiven Bereich wird eine Verletzung des Schutzes personenbezogener Daten nach § 46 Nummer 10 BDSG als eine Verletzung der Sicherheit definiert, die zur unbeabsichtigten oder unberechtigten Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten geführt hat. Durch diese Definition wird klargestellt, dass mit der Verletzung des Schutzes personenbezogener Daten nicht die rechtliche Zulässigkeit der Datenverarbeitung gemeint ist, sondern die Datensicherheit. Diese kann nur durch technische und organisatorische Maßnahmen erreicht werden. Mit anderen Worten: Nicht jede unberechtigte Datenverarbeitung ist auch eine Datenschutzverletzung. Eine Datenschutzverletzung kann nur dann vorliegen, wenn es überhaupt technische und organisatorische Maßnahmen gegeben hätte, deren Ergreifen die Datenschutzverletzung hätte verhindern können. Die Besonderheit unbefugter Abrufe liegt darin, dass Polizeibeamte auf die Systeme zu dienstlichen Zwecken zugreifen dürfen und ein Abruf zu privaten Zwecken kaum verhindert werden kann. Darin unterscheidet sich dieser unberechtigte Datenzugriff von dem krimineller Personen von außen. Sie können im besten Fall durch ausreichende technische und organisatorische Maßnahmen davon abgehalten werden, in die Systeme einzudringen und einen unbefugten Datenzugriff vorzunehmen. Dies ist bei Polizeibeamten, die die Systeme zu dienstlichen Zwecken nutzen dürfen, sich dann aber bewusst nicht an datenschutzrechtliche Vorgaben halten, unmöglich.

30 Siehe A II 4.4.

In der so erfolgenden Kenntnisnahme personenbezogener Daten zu außerdienstlichen Zwecken liegt ein unbefugter Zugang im Sinne des § 46 Nummer 10 BDSG, sodass eine Verletzung der Sicherheit gegeben ist. Allein die Tatsache, dass die betroffene Person im Zusammenhang mit repressiven Maßnahmen der Verfolgung von Straftaten bzw. Ordnungswidrigkeiten in den polizeilichen Systemen gespeichert ist, ist ein sensibles personenbezogenes Datum. Daher bringt ein unbefugter Abruf dieser Daten eine Gefahr für die Rechtsgüter dieser Person mit sich. Hierbei sind insbesondere Rufschädigung, Verlust der Kontrolle über diese Daten sowie private und wirtschaftliche Schäden denkbar.

Eine Meldung der Datenschutzverletzung durch die Polizei an uns als Aufsichtsbehörde ist damit ab Kenntnisnahme des unbefugten Datenabrufs nach § 500 StPO i. V. m. § 65 BDSG verpflichtend.

Im präventiven Bereich ist eine Verletzung der Sicherheit personenbezogener Daten gemäß § 2 Nummer 13 BbgPJMDSG als eine Verletzung der Sicherheit definiert, die zur unbeabsichtigten oder unbefugten Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat.

In der Wortwahl der Norm scheint auf den ersten Blick ein deutlicher Unterschied zur Meldepflicht im repressiven Bereich zu bestehen. Denn statt von einer Verletzung des Schutzes personenbezogener Daten wird im präventiven Bereich von einer Verletzung der Sicherheit personenbezogener Daten gesprochen. Die Gesetzesbegründung[31] zu § 2 Nummer 13 BbgPJMDSG offenbart aber, dass die Norm inhaltlich den in der EU-Richtlinie 2016/680 (sogenannte JI-Richtlinie) genannten Begriff der „Verletzung des Schutzes personenbezogener Daten“ übernehmen soll. Somit stellt ein unbefugter Datenzugriff durch Polizeikräfte auch bei präventivem Handeln der Polizei grundsätzlich eine meldepflichtige Datenschutzverletzung dar.

31 Landtags-Drucksache 6/10692.

### 2.2.2 Meldepflicht der Zentralen Bußgeldstelle

Die Verfolgung verkehrsrechtlicher Ordnungswidrigkeiten obliegt in Brandenburg der beim Zentraldienst der Polizei angesiedelten Zentralen Bußgeldstelle. Da es sich bei dieser Aufgabe um eine repressive Tätigkeit handelt, richtet sich die Pflicht zur Meldung von Datenschutzverletzungen nach § 46 Absatz 1 OWiG i. V. m. § 500 StPO i. V. m. § 65 BDSG.

Exemplarisch für eine solche Datenschutzverletzung war beispielsweise der Fall, in dem sich ein Bürger darüber beschwerte, dass die Zentrale Bußgeldstelle seinen Führerschein mit dem einer anderen Person vertauscht hatte. Als nach Ablauf seines Fahrverbotes die Führerscheine postalisch an die jeweiligen Berechtigten zurückgesandt werden sollten, erhielt der Beschwerdeführer den Führerschein der anderen Person. Dies stellt eine typische Verletzung des Schutzes personenbezogener Daten dar. Den betroffenen Personen kann die Gefahr des Missbrauchs ihres Führerscheins drohen, insbesondere wenn sie sich ähnlich sehen. Damit ist in der Regel eine Beeinträchtigung ihrer Rechtsgüter gegeben, die eine Meldepflicht der Bußgeldstelle an die Datenschutzaufsichtsbehörde nach sich zieht. Darüber hinaus muss sie in solchen Fällen grundsätzlich auch die jeweils anderen von der Datenschutzverletzung betroffenen Personen benachrichtigen. Diese Verpflichtung bewirkt, dass Letztere ggf. Schutzmaßnahmen treffen können, um einen Missbrauch ihrer Daten zu verhindern.

In einem anderen Fall, der eine Meldung der Verletzung des Schutzes personenbezogener Daten erforderte, ging es um das Foto einer Person, die auf der Rückbank eines Fahrzeugs saß, das in einer Geschwindigkeitskontrolle geblitzt wurde. Die Halterin des Fahrzeugs, die nicht die Fahrerin war, bekam das Foto daraufhin zugesandt. Es gelangte auch der Mitfahrerin zur Kenntnis, die sich auf dem Foto wiedererkannte und bei uns beschwerte. Die Zentrale Bußgeldstelle hatte das Bild nicht teilweise geschwärzt, weil es nach ihrer Einschätzung nicht von ausreichend guter Qualität gewesen sei, um die Gesichtsstrukturen der Beschwerdeführerin zu erkennen.

Wir wiesen die Behörde darauf hin, dass ein Personenbezug auch dann gegeben ist, wenn die Identifikation der betroffenen Person unter zumutbarem Aufwand möglich ist. Im vorliegenden Fall war die Beschwerdeführerin zwar mit einer Person unterwegs, die nicht die Halterin des Fahrzeugs war. Allerdings ist davon auszugehen, dass die Halterin weiß, wem sie das Fahrzeug zum fraglichen Zeitpunkt überlassen hatte. Selbst wenn sie die Beschwerdeführerin auf dem Foto nicht selbst identifiziert haben sollte, war es ihr mutmaßlich mit sehr geringem Aufwand möglich, die fraglichen Informationen über die Beschwerdeführerin durch Befragen der Person, die das Fahrzeug geführt hat, herauszubekommen.

Da es für die Verfolgung der Ordnungswidrigkeit gegen die Halterin bzw. die Fahrerin nicht erforderlich war, dass die Beschwerdeführerin auf der Rückbank erkennbar ist, war die Datenübermittlung durch die Zentrale Bußgeldstelle an die Halterin des Fahrzeugs unbefugt. Aus der Abbildung ging hervor, dass sich die Beschwerdeführerin zu einem bestimmten Zeitpunkt im Wagen der Halterin aufgehalten hatte und in eine bestimmte Richtung unterwegs war. Die Beschwerdeführerin war in ihrer Privatsphäre betroffen. In Anbetracht des Schutzniveaus hätte die Behörde das Bild entsprechend schwärzen müssen.

Keine meldepflichtige Datenschutzverletzung lag hingegen im folgenden Fall vor: Der Fahrer eines Fahrzeugs, das wegen einer Geschwindigkeitsübertretung geblitzt worden war, beschwerte sich darüber, dass auf dem Foto auf der Gegenfahrbahn ein Lieferwagen mit der Aufschrift einer Küchenfirma erkennbar war. Das Nichtschwärzen des Firmenaufdrucks stellte in seinen Augen einen Datenschutzverstoß der Bußgeldstelle dar. Nach unserer Einschätzung geht aus dem Foto zwar hervor, dass der Lieferwagen mit diesem Aufdruck zu einer bestimmten Uhrzeit in eine bestimmte Richtung gefahren ist. Im Gegensatz zu einem Kennzeichen ließ das Foto jedoch nicht darauf schließen, auf wen das Fahrzeug zugelassen war und ob die Zulassung mit einer Privatadresse erfolgte. Auch ließ sich nicht erkennen, wer das Fahrzeug führte. Insofern konnten lediglich unternehmensbezogene Daten, die gerade zu Werbezwecken veröffentlicht wurden, zur Kenntnis genommen werden. Es handelt sich also um offenkundige Daten, die einen größtmöglichen Adressa-

tenkreis erreichen sollen. Insofern unterliegen diese Daten – selbst wenn sie Angaben zu natürlichen Personen wie der Inhaberin oder dem Inhaber eines Unternehmens enthalten – einem allenfalls sehr geringen Schutzbedarf. Eine Meldepflicht bestand daher mangels Datenschutzverletzung nicht.

# 3 Ausgewählte Beratungen

## 3.1 Pilotprojekt zum Einsatz von Bodycams

In den letzten Jahren hat sich die Palette der Einsatzmittel der Polizei erweitert. So ist in § 31a Absatz 2 Brandenburgisches Polizeigesetz geregelt worden, dass die Polizei zur Erfüllung ihrer Aufgaben bei Personen- oder Fahrzeugkontrollen körpernah getragene, üblicherweise an der Uniform befestigte kleine Kameras zur Herstellung von Video- und Tonaufzeichnungen einsetzen darf. Allerdings müssen zuvor Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine Gefahr für Leib, Leben oder Freiheit erforderlich ist. Der wesentliche Zweck des Einsatzes dieser Kameras – die Abwendung möglicher Gefahren – basiert auf der Grundannahme eines Deeskalationseffekts bei potenziell gewaltgeneigten Personen. Diese Annahme ist aus unserer Sicht jedoch noch nicht ausreichend unabhängig und wissenschaftlich fundiert nachgewiesen.

Bereits in unserem vorletzten Tätigkeitsbericht[32] informierten wir über Planungen eines Pilotprojektes zum Einsatz von Körperkameras (Bodycams) bei der Polizei Brandenburg. Ein Schwerpunkt unserer Projektbegleitung lag auf den erforderlichen technischen und organisatorischen Maßnahmen, die ergriffen werden müssen, um einen sicheren und datenschutzgerechten Betrieb der Bodycams zu gewährleisten. Insbesondere haben wir die Notwendigkeit einer sorgfältigen Datenschutz-Folgenabschätzung gemäß § 21 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) betont. Im Oktober 2019 übergab uns die Polizei hierzu eine Reihe von Unterlagen, die aus unserer Sicht

32 Tätigkeitsbericht Datenschutz 2019, B 4.

jedoch nicht den datenschutzrechtlichen Anforderungen genügten und dadurch nicht belegen konnten, dass die durch einen Bodycam-Einsatz ausgelösten Risiken für die Rechte und Freiheiten der betroffenen Personen in ausreichendem Maß durch technische und organisatorische Maßnahmen eingedämmt und beherrscht werden. Dies teilten wir der Polizei im Februar 2020 in einer detaillierten Stellungnahme mit.

Ende 2020 leitete das Ministerium des Innern und für Kommunales die rechtliche Abstimmung mit uns zu dem Entwurf einer Verwaltungsvorschrift für den Einsatz von Bodycams ein. Eine überarbeitete Datenschutz-Folgenabschätzung wurde jedoch nicht vorgelegt. Als das Polizeipräsidium uns im Sommer 2021 mit dem Wunsch kontaktierte, das Pilotprojekt baldmöglichst starten zu wollen, sahen wir uns veranlasst, erneut an die fehlenden, aus Datenschutzsicht aber essenziell notwendigen Unterlagen zur Folgenabschätzung zu erinnern.

Schließlich erhielten wir hierzu ein umfassend überarbeitetes Dokument, das eine erheblich verbesserte Qualität aufwies. Die Datenschutz-Folgenabschätzung war nun systematisch und methodisch sinnvoll durchgeführt worden. Insbesondere wurden umfassend mögliche Risikoszenarien erhoben und zusätzliche technische und organisatorische Maßnahmen entwickelt, um erkannte Risiken zu minimieren. Wir waren mit der vorgelegten Risikoanalyse grundsätzlich einverstanden.

Allerdings sahen wir ein großes Problem bei der Behandlung der Herstellerinnen und Hersteller von Kameras, deren eigene Interessen und Zugriffsmöglichkeiten bzw. der Rechtsrahmen, in dem sie sich selbst bewegen, von der Polizei noch nicht ausreichend berücksichtigt wurden. Dies gilt insbesondere für Unternehmen aus Drittstaaten wie z. B. den USA ohne effektiv umsetzbare Möglichkeiten, den Zugriff auf personenbezogene Daten und damit die Möglichkeit einer Datenübertragung in das Drittland datenschutzrechtlich abzusichern. Wir haben der Polizei daher dringend empfohlen, beim Einkauf der Bodycams auf diese

**Datenschutz schon bei Beschaffung beachten**

Aspekte zu achten und einen unzulässigen Datenzugriff durch entsprechende Maßnahmen von vornherein nachprüfbar zu verhindern.

Aber auch bei europäischen Herstellerinnen oder Herstellern von Kameras sehen wir es als zwingend erforderlich an, im Vorfeld klare Vereinbarungen zur Wartung und zum Service im Rahmen der datenschutzrechtlichen Vorgaben des § 27 BbgPJMDSG abzuschließen. Diese Vorgaben sind auch dann zu beachten, wenn eine Verarbeitung personenbezogener Daten durch die Unternehmen zwar nicht beabsichtigt ist, aber ggf. nicht verhindert werden kann.

Schließlich haben wir die Polizei noch darauf hingewiesen, dass die in der Datenschutz-Folgenabschätzung erarbeiteten Maßnahmen auch umgesetzt werden müssen. Nur dann können datenschutzrechtliche Risiken auf ein ausreichend geringes Maß reduziert werden, um das Pilotprojekt verantwortungsvoll durchzuführen.

Das geplante Projekt soll umfassend von der Hochschule der Polizei des Landes Brandenburg begleitet und wissenschaftlich ausgewertet werden. Wir hoffen, dass sich dadurch die derzeit noch nicht ausreichende Datenlage zur Evaluierung der postulierten Deeskalationseffekte verbessern lässt.

Wir haben die Polizei gebeten, uns über den Fortgang des Projekts weiter auf dem Laufenden zu halten.

### 3.2 Rahmensicherheitskonzept der Polizei

Damit die Informationssicherheit bei der Verarbeitung personenbezogener Daten durch die Polizei gewährleistet ist, müssen die Verantwortlichen ein Konzept nach der Methodik des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entwickeln und umsetzen. Bei einem sehr großen Informationsverbund wie dem der Polizei Brandenburg ist es sinnvoll und angemessen, ein Rahmenkonzept für die Basis-Infrastruktur mit übergreifenden, verfahrensunabhängigen IT-Sicherheitsmaßnahmen zu erstellen und darauf die jeweiligen Teil-Sicherheitskonzepte für die einzelnen automatisierten Verfahren aufzubauen. Die Entwicklung des Rah-

mensicherheitskonzeptes wies jedoch über Jahre hinweg erhebliche Defizite auf. Bis zum Ende des Berichtszeitraumes haben sich erfreulicherweise inzwischen sowohl die Realisierungsplanung als auch der Umsetzungsstand insbesondere der als hoch-prioritär erkannten technischen und organisatorischen Maßnahmen deutlich verbessert.

Noch im Jahr 2019 mussten wir aufgrund der lange andauernden Mängel beim Sicherheitskonzept eine Beanstandung gegenüber dem verantwortlichen Innenminister aussprechen.[33] Dieser versicherte daraufhin, dass Datenschutz und Informationssicherheit bei der Polizei höchste Priorität hätten und er sich mit Nachdruck für die Fertigstellung der erforderlichen Dokumente einsetzen werde. Einige Monate später wurden uns umfassende Unterlagen zum Rahmensicherheitskonzept übergeben. Nach deren Prüfung kamen wir jedoch zu dem Ergebnis, dass das Konzept in allen Teilen stark verbesserungswürdig war. Insbesondere zeigte sich, dass erforderliche Basismaßnahmen nicht in ausreichendem Maß umgesetzt wurden. Auch die weitere Planung ihrer Realisierung war aus unserer Sicht unzureichend, da vielfach keine sinnvollen Terminsetzungen, Zuständigkeiten für die Umsetzung und begründete Priorisierungen erkennbar waren. Wir hielten eine Besprechung unserer Prüfergebnisse für dringend angezeigt; wegen pandemiebedingter Einschränkungen einigten wir uns schließlich auf einen schriftlichen Austausch zum aktuellen, mittlerweile weiterentwickelten Stand des Konzeptes. Dieses war allerdings aus unserer Sicht wiederum nicht hinreichend, da nur geringe Fortschritte zu erkennen und die zuvor bemängelten Punkte im Wesentlichen nach wie vor vorhanden waren. Insbesondere der Umsetzungsstand der technischen und organisatorischen Maßnahmen ließ weiterhin zu wünschen übrig.

Schließlich gelang im Sommer 2021 ein persönliches Treffen mit den Verantwortlichen, in dem wir uns den aktuellen Stand erläutern ließen und unsere Erwartungen hinsichtlich des Fortgangs der Arbeiten am Rahmensicherheitskonzept formulierten. Wir verwiesen erneut darauf, dass ein Realisierungsplan mit nach Prioritäten geordneten umzusetzenden Maßnahmen, konkreten Umsetzungsterminen und Umsetzungsverantwortlichen erstellt werden sollte. Dieser Plan sollte laufend zur Termin- und Umsetzungskontrolle verwendet und

33 Tätigkeitsbericht Datenschutz 2019, B 2.

ggf. fortgeschrieben werden. Gleiches gilt auch für andere Teile des Sicherheitskonzeptes, falls während der Abarbeitung des Plans Mängel, Lücken oder veränderte Rahmenbedingungen erkannt werden.

Gegen Ende des Berichtszeitraums ist uns ein weiterentwickelter Realisierungsplan übergeben worden, bei dem sich bereits deutliche Fortschritte hinsichtlich der Priorisierungen erkennen lassen. Zu dem aus unserer Sicht kritischen Punkt der termingerechten Umsetzung der Maßnahmen, hat uns die Polizei nun nachvollziehbar darlegen können, dass alle Maßnahmen der höchsten Prioritätsstufe bezogen auf die betrachteten IT-Verbünde termintreu umgesetzt werden. Hinsichtlich der Steuerung der Maßnahmenplanung und -umsetzung durch die Verantwortlichen für die nächsten Meilensteine sehen wir ebenfalls eine positive Entwicklung. Eine große Herausforderung bleibt für die Polizei jedoch die Gewährleistung ausreichender personeller Ressourcen zur kontinuierlichen Weiterführung des Informationssicherheitsprozesses. Hier sehen wir auch eine klare Verantwortlichkeit der Leitungsebene, die die erforderlichen Rahmenbedingungen für eine verlässliche, sichere und datenschutzgerechte Informationsverarbeitung bei der Polizei in Brandenburg sicherstellen muss.

**Was lange währt, scheint gut zu werden**

Zu einem ordnungsgemäßen IT-Sicherheitskonzept gehört auch, dass sämtliche Auftrags- und Unterauftragsverhältnisse zu Dienstleistern mit vertraglichen Vereinbarungen beschrieben und technisch-organisatorisch abgesichert sind. Zu den Auftragnehmern der Polizei zählen beispielsweise die Landes-IT-Dienstleister. Die vorhandene Vertragslage war allerdings bislang unzureichend, sodass grundlegende Nacharbeiten erforderlich waren. Diese sind bereits in Angriff genommen worden, zum Ende des Berichtszeitraums aber noch nicht abgeschlossen.

Eine spezielle Problematik hat sich im Kontext der als Teil eines IT-Sicherheitskonzeptes nach BSI-Standard bei erhöhtem Schutzbedarf erforderlichen zusätzlichen Risikoanalyse ergeben. Die von den Verantwortlichen vorgesehenen Maßnahmen zur Risikobehandlung basierten im Wesentlichen darauf, die Restrisiken durch einen Risikotransfer hin zu den ohnehin per Auftragsverarbeitung verpflich-

teten IT-Dienstleistern zu verschieben. Wir bezweifeln jedoch, dass diese Übertragung der Risiken zu einer besseren Risikominimierung führt und haben daher das Bundesamt für Sicherheit in der Informationstechnik um eine Stellungnahme hierzu gebeten. Hinsichtlich der Interpretation der nun vorliegenden Antwort des Bundesamtes besteht derzeit allerdings noch ein Dissens mit den Verantwortlichen, sodass weitere Gespräche zu diesem Themenkomplex erforderlich sind.

## 3.3 Aufgaben und Tätigkeiten des Zentrums zur polizeilichen Telekommunikationsüberwachung

Das gemeinsame Kompetenz- und Dienstleistungszentrum auf dem Gebiet der polizeilichen Telekommunikationsüberwachung (GKDZ) der Polizeien der fünf Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen wurde als rechtsfähige Anstalt des öffentlichen Rechts am 11. Januar 2018 gegründet. Hauptsitz der Anstalt ist Leipzig. Der Gründung waren jahrelange Verhandlungen der beteiligten Trägerländer über einen Staatsvertrag (GKDZ-StV) vorausgegangen. Dieser legt die Rechtsform, Finanzierung, Aufgaben, Organe und Aufsicht sowie datenschutzrechtliche Rahmenbedingungen des GKDZ fest.[34]

Zwischenzeitlich wurden das Zentrum auf dem Areal der Bereitschaftspolizei Sachsen aufgebaut, diverse Hard- und Software beschafft und erste Stellenbesetzungsverfahren durchgeführt. Im Mai 2018 wurde ein Datenschutzbeauftragter für das GKDZ benannt. Das sächsische Staatsministerium des Innern stellte im Februar 2019 im Beisein von Vertretern der Datenschutzaufsichtsbehörden der beteiligten Länder Anforderungen aus den rechtlich relevanten Normen für die Telekommunikationsüberwachung und Maßnahmen zur technisch organisatorischen Umsetzung des Zentrums (Feinplanung) vor. Hieraus ergab sich weiterer Erörterungsbedarf. Die Landesdatenschutzbeauftragten legten im November 2019 und Oktober 2020 gemeinsame Stellungnahmen zur Feinplanung vor, die u. a. Fragen des Aufgabenspektrums des GKDZ, der Betroffenenrechte, der

34 Tätigkeitsbericht 2016/2017, B 12.1.

Datenanreicherung und -ausleitung im GKDZ, der IT-Technikgestaltung, Berechtigungsmodelle und Zugriffsprotokollierung berührten.

Das gemeinsame Kompetenz- und Dienstleistungszentrum wird im Wege der Auftragsverarbeitung Daten aus polizeilichen Telekommunikationsüberwachungsmaßnahmen nach den Vorgaben der jeweiligen Landespolizeigesetze, der Umsetzungsgesetze der EU-Richtlinie 2016/680 (sogenannte JI-Richtlinie) sowie der Strafprozessordnung (StPO) für die Trägerländer verarbeiten. Verantwortliche der Datenverarbeitung im Sinne dieser Gesetze bleiben die Polizeien und Staatsanwaltschaften der Länder.

Eine der Differenzen, die bisher ungelöst blieb, ist die Frage nach dem Umfang der Aufgaben des GKDZ. Diese werden durch die Aufgabenzuweisung des Staatsvertrags beschrieben, der verbindlichen Gesetzescharakter hat. § 4 Abs. 1 Satz 2 und 3 GKDZ-StV lauten: „Die Trägerländer benutzen die Anstalt im Wege der Auftragsverarbeitung für Daten aus der polizeilichen Telekommunikationsüberwachung nach den jeweiligen Landespolizeigesetzen sowie nach den §§ 100a ff. Strafprozessordnung (Kernaufgabe). Telekommunikationsüberwachung ist die Verarbeitung von Nutzungs-, Inhalts-, Verkehrs-, Bestands- und Standortdaten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sowie des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“

Der Verweis auf „§§ 100a ff.“ könnte als Einfallstor für eine weite Auslegung herangezogen werden. Die Abkürzung „ff.“ steht für folgend bzw. auf den nächsten Seiten. In juristischen Texten wird sie regelmäßig für alle einem Paragraphen nachfolgende Normen eingesetzt. Bei gleicher Zahlenbenennung betrifft dies die durch kleine Buchstaben eingefügten Regelungen. In den Paragraphen 100a bis 100k StPO sind verschiedene verdeckte Datenerhebungsbefugnisse geregelt, die Eingriffe in das Post- und Fernmeldegeheimnis, das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und das Recht auf Unverletzlichkeit der Wohnung erlauben. Neben dem klassischen Abhören des Inhalts, also der Sprache und Töne – auch der Internet-Telefonie – und Bestandsdatenauskünften, fallen beispielsweise auch die Online-Durchsuchung, die

akustische Wohnraumüberwachung, die Observation durch Bildaufnahmen oder mittels technischer Mittel außerhalb des Wohnraums oder die Erhebung von Nutzungsdaten bei Telemediendiensten, aber auch Verfahrensregelungen und die Regelung zum Schutz des Kernbereichs privater Lebensgestaltung in diese Auflistung.

Aus der in § 4 des Staatsvertrags niedergelegten Definition ergibt sich aus unserer Sicht jedoch eine eindeutige Beschränkung der Datenverarbeitungsbefugnisse ausschließlich auf Daten im Zusammenhang mit Telekommunikationsvorgängen bzw. Telekommunikationsüberwachung. Wird dazu in ein informationstechnisches System eingegriffen, sind die zu verarbeitenden Daten auf den laufenden Übertragungsvorgang zu begrenzen. Unter Telekommunikationsdaten fallen weder Daten, die aus Online-Durchsuchungen informationstechnischer Systeme oder aus der akustischen Überwachung von Personen stammen, noch sonstige von Gefahrenabwehr- oder Strafverfolgungsbehörden sichergestellte oder beschlagnahmte Kommunikationsdaten in Papierform. Auch unter dem Gesichtspunkt, dass neuartige technologische Entwicklungen bei der Telekommunikation im Staatsvertrag mitberücksichtigt werden sollten, verbietet sich bei öffentlich-rechtlichem und hoheitlichem Handeln eine erweiternde Auslegung des Begriffs Telekommunikation. Der in gesetzlichen Definitionen, Rechtsprechung und im allgemeinen Verständnis begrenzte Begriff steht auch im Einklang mit der rechtspolitischen Diskussion um die Einrichtung des GKDZ. Bei dieser wurde stets darauf hingewiesen, dass über das Zentrum nur Telekommunikationsüberwachung abgewickelt werden soll.

## Gesetze zur TK-Überwachung eng auslegen

Wir haben – in Übereinstimmung mit den übrigen Aufsichtsbehörden – unsere Forderung, die Aufgaben des GKDZ auf Daten der Telekommunikation im oben genannten Sinne zu begrenzen, gegenüber dem Ministerium des Inneren und für Kommunales und dem GKDZ deutlich gemacht. Wie diese sich hinsichtlich des Aufgabenspektrums endgültig positionieren, ist bisher nicht bekannt.

Diese Frage muss abschließend geklärt werden, bis die vor der Inbetriebnahme des GKDZ geplante Testphase anläuft. Es war geplant, dass der Probebetrieb bis zum Ende des Berichtszeitraums möglich

sein sollte. Der Wirkbetrieb, der ursprünglich für 2019 anvisiert war, verzögert sich wegen der komplexen Gestaltung des Großprojekts und aufgrund des umfangreichen Abstimmungsprozesses zwischen fünf Bundesländern weiter.

## 4 Zahlen und Fakten

Im Berichtszeitraum war im Vergleich zum Vorjahr ein Anstieg von über 70 % an Beschwerden betroffener Personen über Datenverarbeitungsvorgänge bei Polizei und Staatsanwaltschaft zu verzeichnen. Insgesamt erreichten uns 31 Beschwerden, die sich ganz überwiegend auf die Polizeibehörden des Landes bezogen und nur vereinzelt staatsanwaltliches Handeln betrafen. Auffällig war die Häufung von Eingaben gegen die Datenverarbeitung durch die Zentrale Bußgeldstelle der Polizei in Verwarnungsverfahren wegen Geschwindigkeitsübertretungen. Die Beschwerden richteten sich gegen Ermittlungen (Bildaufnahmen) zur Aufklärung der Fahrereigenschaft, in diesem Zusammenhang bestehende Abfragebefugnisse in Registern als auch versehentliche Fehlübermittlungen an Unbeteiligte.

Zugleich wurden wie im Vorjahr mündlich und schriftlich zeitintensive Beratungen für die Polizeibehörden durchgeführt. Hier sind als wesentliche Schwerpunkte zu nennen: die Begleitung zur Vervollständigung des Rahmensicherheitskonzepts der Polizei sowie des Projekts zur Einführung von Körperkameras (Bodycams). Zugleich haben wir anhand von mehreren Einzelfällen gegenüber der Polizei präzisiert, wann Verhaltensweisen eine Verletzung der Sicherheit bzw. des Schutzes personenbezogener Daten (im präventiven wie repressiven Bereich) darstellen und gemäß der gesetzlichen Regelungen eine Meldepflicht gegenüber der Landesbeauftragten auslösen. Erfreulich war, dass die Polizei Datenschutzverletzungen häufiger fristgerecht und detailliert meldete.

Vor-Ort-Besuche und -Gespräche konnten bedingt durch die gebotene Kontaktvermeidung wegen der bestehenden Pandemielage nur sehr eingeschränkt durchgeführt werden. Wir nahmen jedoch zwei Vor-Ort-Kontrollen (eine unangekündigte und eine geplante) bei Po-

lizeibehörden vor. Die Auswertung dieser Prüfungen ist noch nicht abgeschlossen.

Im Berichtszeitraum hat die Landesbeauftragte gegenüber Polizei und Staatsanwaltschaft weder Warnungen oder Beanstandungen nach Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz ausgesprochen noch von Abhilfebefugnissen auf der Grundlage der Datenschutz-Grundverordnung Gebrauch gemacht.

# Teil C: Die Dienststelle

# 1 Öffentlichkeitsarbeit

Üblicherweise führt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder anlässlich des Europäischen Datenschutztages eine zentrale Veranstaltung durch. Im Berichtsjahr fand pandemiebedingt eine Videoübertragung statt, zu der am 28. Januar 2021 – dem 40. Jahrestag der Datenschutzkonvention 108 des Europarats – Vertreterinnen und Vertreter aus Politik, Justiz und Verwaltung zusammenkamen, um sich über die Herausforderungen des internationalen Datentransfers auszutauschen. Mehr als 900 Teilnehmerinnen und Teilnehmer hatten sich dafür angemeldet. Die digitale Tagung wurde vom Bundesministerium des Innern, für Bau und Heimat sowie von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder unter dem Vorsitz des Sächsischen Datenschutzbeauftragten ausgerichtet.

Ziel des Safer Internet Day ist es, für Online-Sicherheit zu sensibilisieren und die Medienkompetenz zu stärken. Unter der Überschrift „Gemeinsam für ein besseres Internet“ haben Schülerinnen und Schüler des Strittmatter-Gymnasiums Gransee dazu kurze Videos geschaffen, die gerade junge Menschen zum Nachdenken anregen sollen. Drei Spielszenen vermittelten anhand anschaulicher Beispiele, welche digitalen Spuren wir hinterlassen und welche Datenschutzrisiken daraus entstehen können. Die Jugendlichen haben aber auch deutlich herausgearbeitet, was junge Menschen tun können, um sich sicher im Netz zu bewegen. Das am 9. Februar 2021 der Öffentlichkeit vorgestellte Projekt wurde von der Landesbeauftragten sowie vom Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz, der DigitalAgentur Brandenburg, der Medienanstalt Berlin-Brandenburg und dem Medieninnovationszentrum Babelsberg unterstützt. Die Videos sind auf der Homepage des Ministeriums abrufbar.

Der Bedarf an Informationen über den Datenschutz im Zusammenhang mit der fortbestehenden Pandemie hat auch im Berichtszeitraum nicht nachgelassen. Die bereits im Vorjahr veröffentlichten Antworten auf häufig gestellte Fragen zur Erhebung der Kontaktdaten sowie das entsprechende Musterformular haben wir regelmäßig

der jeweils geltenden Rechtslage angepasst. Diese und weitere Informationen stehen unter der Schwerpunktrubrik zum Datenschutz während der Corona-Pandemie in unserem Internetangebot zur Verfügung.

Eine weitere Schwerpunktrubrik befasst sich mit dem internationalen Datenverkehr. Dort haben wir im Berichtsjahr verschiedene Informationen zur Übermittlung personenbezogener Daten an Drittländer bzw. in das Vereinigte Königreich von Großbritannien und Nordirland nach dessen Ausscheiden aus der Europäischen Union angeboten.

Zwei Handreichungen der Landesbeauftragten sollen es Verantwortlichen erleichtern, die Anforderungen der Datenschutz-Grundverordnung zu erfüllen. Mit den Ausführungen zur Meldung von Datenschutzverletzungen erläutern wir, was im Falle einer Verletzung des vorgeschriebenen Schutzes personenbezogener Daten zu beachten ist, und zwar in Bezug auf die interne Dokumentation des Vorfalls, seine Meldung an uns als Aufsichtsbehörde sowie die gegebenenfalls erforderliche Benachrichtigung der von der Datenschutzverletzung betroffenen Personen. In Form von Antworten auf häufig gestellte Fragen fasst die Handreichung zu den rechtlichen Anforderungen an Datenschutzbeauftragte die wichtigsten Gesichtspunkte rund um die Benennung und Aufgaben von Datenschutzbeauftragten zusammen. Sie berücksichtigt die Rechtslage nach der Datenschutz-Grundverordnung, dem Bundesdatenschutzgesetz und dem Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz. Beide Handreichungen sind in unserem Internetangebot abrufbar.

In Zusammenarbeit mit den übrigen Mitgliedern der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat die Landesbeauftragte mehrere Orientierungshilfen und Anwendungshinweise veröffentlicht. Im Berichtszeitraum handelte es sich dabei um die Orientierungshilfen zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, zum Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurants- und Geschäftsbesuchen zur Verhinderung der Verbreitung von COVID-19 sowie

für Anbieterinnen und Anbieter von Telemedien. Darüber hinaus hat die Konferenz Anwendungshinweise zu den Anforderungen an datenschutzrechtliche Zertifizierungsprogramme sowie eine Anwendungshilfe zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie herausgegeben. Auch diese Dokumente halten wir in unserem Internetangebot zum Abruf bereit.

Regelmäßig veröffentlicht die Landesbeauftragte auch die vom Europäischen Datenschutzausschuss herausgegebenen Leitlinien in ihrem Internetangebot. Im Jahr 2021 befassten diese sich mit den Beschränkungen unter Artikel 23 Datenschutz-Grundverordnung, mit virtuellen Sprachassistenten, mit Konzepten zu Verantwortlichen und Auftragsverarbeitern in der Datenschutz-Grundverordnung, mit der gezielten Ansprache von Nutzerinnen und Nutzern sozialer Medien, mit dem maßgeblichen und begründeten Einspruch im Sinne der Datenschutz-Grundverordnung, mit der Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen sowie mit Beispielen für Meldungen von Datenschutzverletzungen.

## 2 Pressearbeit

Am 9. Februar 2021 veröffentlichte die Landesbeauftragte eine gemeinsame Presseinformation mit dem Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz anlässlich des Safer Internet Day. Ziel dieses weltweit begangenen Tages ist es, für Online-Sicherheit zu sensibilisieren und Medienkompetenz zu stärken. Konkret stellte die Presseinformation kurze Erklär-Videos von Schülerinnen und Schülern des Strittmatter-Gymnasiums Gransee vor. Das Projekt war vom Ministerium, der DigitalAgentur Brandenburg, der Medienanstalt Berlin-Brandenburg, dem Medieninnovationszentrum Babelsberg und der Landesbeauftragten unterstützt worden.

Die Einführung der Luca App in Brandenburg kommentierten wir in einer Aussendung vom 31. März 2021. Die Landesbeauftragte äußerte sich grundsätzlich positiv darüber, die bisherige Zettelwirtschaft bei der pandemiebedingten Kontaktnachverfolgung durch ein digitales Verfahren zu ersetzen. Gleichzeitig skizzierte sie die Vor-

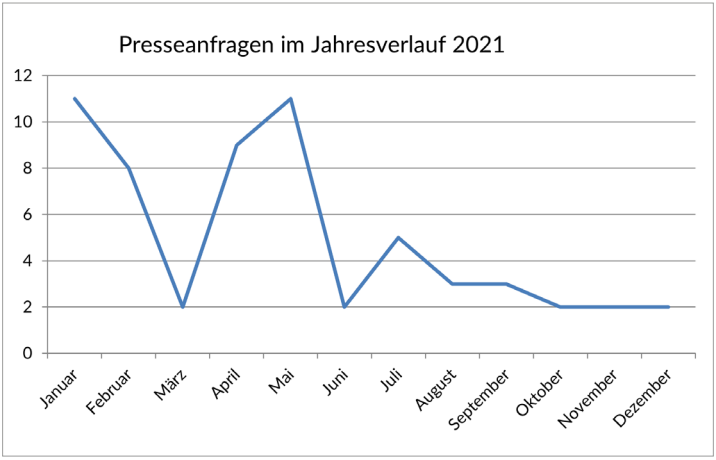
aussetzungen, die für einen datenschutzgerechten Betrieb des Systems erforderlich sind.

Ihren Tätigkeitsbericht Datenschutz 2020 übergab die Landesbeauftragte der Präsidentin des Landtages Brandenburg am 3. Mai 2021 – im Gegensatz zum Vorjahr wieder im Rahmen einer (hybriden) Pressekonferenz. Auf die wichtigsten Entwicklungen ihrer Aufsichtstätigkeit während des Berichtsjahres wies sie in einer ausführlichen Presseinformation am selben Tage hin.

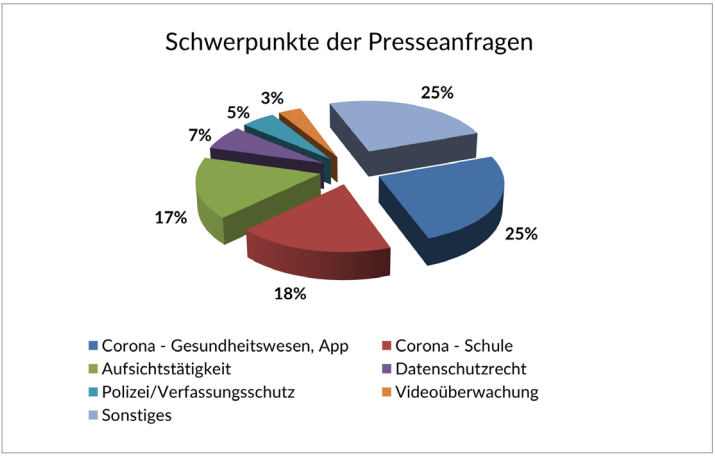
Am 1. Juni 2021 nahmen wir eine durch mehrere deutsche Aufsichtsbehörden koordinierte Prüfung internationaler Datentransfers zum Anlass für eine weitere Presseinformation. Hintergrund war die Rechtsprechung des Europäischen Gerichtshofes, der die strengen Voraussetzungen für die Übermittlung personenbezogener Daten in die Vereinigten Staaten von Amerika und andere Drittstaaten ohne angemessenes Datenschutzniveau festgestellt hatte. Die für die Prüfung verwendeten Fragenkataloge haben wir ebenfalls veröffentlicht.

Gegenstand einer Mitteilung vom 30. Juni 2021 war eine ebenfalls zwischen den Aufsichtsbehörden abgestimmte, länderübergreifende Prüfung des Umgangs von Medienunternehmen mit Einwilligungen der Nutzerinnen und Nutzer auf ihren Webseiten. Auf den geprüften Seiten wurden eine sehr hohe Anzahl von Cookies verwendet bzw. Drittdienste eingebunden, die überwiegend dem Nutzertracking und der Werbefinanzierung dienen. Die beteiligten Datenschutzbehörden wirkten auf die Unternehmen in ihrem Zuständigkeitsbereich ein, um datenschutzkonforme Zustände herzustellen.

Während wir im Vorjahr 84 Medienanfragen verzeichneten, reduzierte sich die Zahl im Berichtszeitraum auf 60. Zeitlich betrachtet konzentrierten sich die Anfragen auf die beiden ersten Monate sowie auf den Mai 2021, während Journalistinnen und Journalisten in der zweiten Jahreshälfte kaum Auskünfte der Landesbeauftragten erfragten.




Der größte Anteil der Presseanfragen bezog sich auf Datenschutzthemen im Zusammenhang mit der Corona-Pandemie. Eindeutig im Vordergrund standen dabei das schulische Distanzlernen sowie der Einsatz des Luca-Systems in der Gesundheitsverwaltung. Konkrete Datenschutzvorkommnisse bei öffentlichen und privaten Stellen aus unterschiedlichen Branchen waren Anlass für Anfragen in 22 % der Fälle. 17 % der anfragenden Medien interessierten sich für die Aufsichtstätigkeit der Landesbeauftragten, also beispielsweise für statistische Angaben zu verhängten Bußgeldern oder zu anderen Sanktionen. Dies entspricht dem Vorjahreswert. In sieben Prozent der Anfragen erkundigten sie sich nach einer generellen datenschutzrechtlichen Einschätzung. Polizeiliche Belange oder die Videoüberwachung waren im Vergleich zum vorangegangenen Berichtszeitraum kaum noch von Interesse. Auf dem Gebiet der Datenverarbeitung durch die Polizei Brandenburg erklärt sich dies durch die Beendigung der anlasslosen automatisierten Kennzeichenerfassung, die zuvor zu einem großen Anteil der Anfragen geführt hatte. Wie bereits im Vorjahr interessierten sich die Medien mit etwa der Hälfte der Anfragen für die Datenverarbeitung durch öffentliche Stellen und mit knapp einem Drittel für jene durch private Unternehmen.




Die Verteilung der anfragenden Medien hat sich im Vergleich zum Vorjahr nur insoweit signifikant geändert, als sich der Anteil der Anfragen von Fernsehjournalistinnen und Fernsehjournalisten auf 12 % halbiert hat. Mit 53 % hat der Printbereich – also Zeitungen oder Zeitschriften – etwa fünf Prozentpunkte hinzugewonnen. Im Großen und Ganzen gleich geblieben ist die regionale Verbreitung der Medien – etwas mehr als ein Drittel der Anfragen stammt aus anderen Bundesländern oder von überregional tätigen Journalistinnen und Journalisten, fünf Prozent der Anfragen von internationalen Medien und knapp 60 % aus den Ländern Brandenburg oder Berlin.

## 3 Personal und Organisation der Dienststelle

Im Berichtszeitraum konnte ich zwei neue Stellen, die der Landtag Brandenburg für den Haushalt 2021 bewilligt hatte, erfolgreich besetzen und so die Arbeitsgebiete Akteneinsichts- sowie Datenschutzrecht stärken. Nachbesetzt wurde auch die Stelle einer Mitarbeiterin der Verwaltung, die zum Ende des Vorjahres in den Ruhestand gegangen war.

Leider musste die Behörde auch zwei Weggänge verkraften. Jeweils ein Mitarbeiter aus dem technischen und dem juristischen Bereich wechselte in die Privatwirtschaft. Bereits absehbar ist, dass ein wei-

terer Mitarbeiter des Bereichs Technik und Organisation eine Stelle in der Landesverwaltung antritt. Dadurch entstehen erhebliche Lücken, die es zusätzlich erschweren, die gesetzlich vorgesehenen Aufgaben zu erfüllen.

Die Nachbesetzung der Stellen gestaltet sich insbesondere im Bereich Technik und Organisation aufgrund des andauernden Fachkräftemangels weiterhin sehr schwierig. Dies wirkt sich erheblich auf unsere Beratungstätigkeit im Bereich Digitalisierung aus. Auch wenn es gelingt, eine freie Stelle nach mehreren Anläufen zu besetzen, müssen in der Übergangszeit die jeweiligen Aufgaben von den anderen, meist ohnehin überlasteten Beschäftigten meiner Dienststelle miterledigt werden. So konnte im vorliegenden Fall die Vakanz im technischen Bereich erst nach über einem halben Jahr beseitigt werden. Die freie Stelle im juristischen Bereich konnte zeitnah hausintern wiederbesetzt werden. Außerdem ist es gelungen, die dadurch freigewordene, mit Sachgrund befristete Stelle mit einer juristischen Referentin zu besetzen.

Für das Jahr 2022 hat uns der Landtag erfreulicherweise die dringend benötigte Stelle für eine IT-Systemkoordinatorin bzw. einen IT-Systemkoordinator bewilligt. Obwohl sich die Dienststelle um eine rasche Besetzung bemüht hatte, musste ein erstes Ausschreibungsverfahren allerdings ohne Ergebnis beendet werden.

Wie auch schon in den vergangenen Jahren ist die Erfüllung der Aufgaben meiner Behörde mit dem vorhandenen Personal nur mit erheblichen Schwierigkeiten möglich. Hierzu trägt die pandemische Lage nicht unwesentlich bei. Die Beratungen der Landesregierung, der Kommunen und der nicht öffentlichen Stellen fanden, wenngleich unter veränderten Bedingungen, weiterhin in großer Zahl und zum Teil in großem Umfang statt. Außerdem sind meine Mitarbeiterinnen und Mitarbeiter einer erheblich gestiegenen Menge gemeldeter Datenschutzverletzungen nachgegangen. Deutlich zugenommen haben Beschwerden Betroffener über die Datenverarbeitung einiger großer Unternehmen. Auch Betreiberinnen und Betreiber von Videoüberwachungskameras stehen vermehrt im Fokus. Insgesamt sind hinsichtlich der Beratungs- und Beschwerdefälle deren zunehmende Komplexität und die Schwierigkeiten bei der Aufklärung der Daten-

verarbeitungsvorgänge ein Hauptgrund für lange Bearbeitungszeiten. Zunehmend beschweren sich Betroffene und Ratsuchende auch hierüber. Eine Verkürzung ist mit dem vorhandenen Personal jedoch ohne erhebliche Qualitätseinbußen nicht möglich.

Die räumliche Situation der Dienststelle hat sich mit dem dargestellten Personalzuwachs weiter verschlechtert. Bisherige Besprechungs- und Funktionsräume mussten zu Büros umgebaut werden. Nachdem der Umzug der Behörde in die Landeshauptstadt Potsdam aus Kostengründen geplatzt ist, hoffe ich nun auf eine zeitnahe Anmietung eines barrierefreien Besprechungsraums in einem anderen Gebäude auf der Liegenschaft in Kleinmachnow. Das Problem der mangelnden Barrierefreiheit der übrigen Räume – insbesondere der Büros – besteht unverändert fort.

## 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**