Landesbeauftragte
für Datenschutz
und Akteneinsicht

Tätigkeitsbericht 2022
Datenschutz

Titelbild

Motiv: Hauptgebäude der Filmuniversität Babelsberg

Bildrechte: Filmuniversität Babelsberg KONRAD WOLF

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 2022

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 2022 ab.

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

Vorwort

Liebe Leserinnen, liebe Leser,

in diesem Tätigkeitsbericht möchte ich Sie über die wichtigsten Themen und Fälle informieren, mit denen meine Dienststelle im Jahr 2022 befasst war. Erneut hat die Anzahl der Beschwerden über Datenschutzverstöße zugenommen. Ob daraus zu schließen ist, dass solche Verstöße häufiger vorkommen oder die Brandenburgerinnen und Brandenburger in Fragen des Datenschutzes aufmerksamer geworden sind, lässt sich nicht ohne Weiteres beantworten. In jedem Fall kann ich über eine mangelnde Auswahl von Beiträgen für diesen Bericht nicht klagen.

Ein wesentlicher Schwerpunkt meiner Aufsichtstätigkeit war der Einsatz von Facebook-Fanpages durch öffentliche Stellen, aber auch durch Unternehmen. Der Europäische Gerichtshof hatte bereits vor mehreren Jahren festgestellt, dass Facebook und die jeweilige Stelle, die eine Fanpage verwendet, datenschutzrechtlich gemeinsam für deren Betrieb verantwortlich sind. Ich erläutere in diesem Bericht, welche Anforderungen an einen datenschutzkonformen Einsatz von Fanpages bestehen und lege dar, dass die betreffenden öffentlichen Stellen des Landes Brandenburg bislang nicht in der Lage waren, nachzuweisen, diese einzuhalten. Außerdem berichte ich über den Stand des Verfahrens, das meine Behörde mit der Landesregierung führt.

Aus Sicht des Datenschutzes sind die meisten Cookies, die beim Besuch von Webseiten auf den Rechnern der Nutzerinnen und Nutzer gesetzt werden, nicht nötig. Da diese Technologie aber insbesondere eine wirtschaftliche Auswertung des Nutzerverhaltens ermöglicht, ist ihr Einsatz weit verbreitet. Ergebnis sind die allgemein als lästig empfundenen Cookie-Banner, mit denen Webseitenbetreiberinnen und -betreiber die Einwilligung der Betroffenen einholen. Über die Art und Weise, wie dies geschieht, beschwerten sich zahlreiche Bürgerinnen und Bürger bei meiner Behörde. Dies nehme ich zum Anlass, die datenschutzrechtlichen Bedingungen für den Einsatz von Cookies in einem zweiten Schwerpunkt zu erläutern und über das

Vorgehen der brandenburgischen Datenschutzaufsichtsbehörde in den Beschwerdefällen zu berichten. Inzwischen ist das Aufkommen der Beschwerden so umfangreich, dass die Kapazitäten meiner Behörde nicht mehr ausreichen, um allen Anliegen in angemessener Zeit nachzugehen.

Die zahlreichen Meldungen von Datenschutzverletzungen über Cyberangriffe zeigen, dass es für verantwortliche Stellen immer wichtiger wird, rechtzeitig und umfassend Schutzvorkehrungen dagegen zu treffen. Um dies an einem konkreten Beispiel zu erläutern, stelle ich Ihnen den Fall einer Bank vor, deren gravierende Sicherheitsmängel durch den Hackerangriff auf eine Videokamera offengelegt wurden. Im Ergebnis habe ich ein Bußgeld gegen das Kreditinstitut verhängt.

Hoffentlich zum letzten Mal hatte ich im Berichtsjahr mit den Auswirkungen der Eindämmung der Corona-Pandemie auf die Datenschutzrechte der Bürgerinnen und Bürgern zu tun. Dies betraf im Wesentlichen die Einführung der einrichtungsbezogenen Impfpflicht, die wir zum Anlass genommen haben, entsprechende Meldeportale zu prüfen. Im Zusammenhang mit der bereits länger zurückliegenden Verpflichtung zur Kontaktdatenerhebung berichte ich zudem über die Verhängung von Bußgeldern in zwei Fällen. Die Verstöße erwiesen sich hier als so gravierend, dass das in vielen anderen Fällen durch meine Behörde genutzte Sanktionsmittel der Verwarnung nicht mehr ausreichte.

Ein Thema, zu dem meine Behörde bisher vor allem beratend tätig war, ist der Einsatz der onlinebasierten Software Microsoft 365. Nach intensiver Befassung der Datenschützerinnen und Datenschützer und zahlreichen Gesprächen zwischen der Datenschutzkonferenz und dem Herstellerunternehmen liegen inzwischen Ergebnisse vor, die ich in meinem Bericht vorstelle. Verwaltungen oder Unternehmen, die beabsichtigen, die Software Microsoft 365 zu verwenden, können daran die Probleme erkennen, die durch ihren Einsatz für den Datenschutz entstehen.

Der Tätigkeitsbericht Datenschutz 2022 enthält noch viele weitere anschauliche Fälle – lesen Sie selbst. Ich wünsche Ihnen eine interessante Lektüre.

Dagmar Hartge

Teil A: Bericht nach Art. 59 Datenschutz-Grundverordnung

I Schwerpunkte

1 Betrieb von Facebook-Fanpages durch öffentliche Stellen

Seit mehreren Jahren beschäftigt sich die Landesbeauftragte mit der Vereinbarkeit des Betriebs von sogenannten Fanpages im sozialen Netzwerk Facebook mit dem Datenschutzrecht. Im Jahr 2018 hatten wir über die Vorabentscheidung des Europäischen Gerichtshofs[1] in dem Rechtsstreit der Wirtschaftsakademie Schleswig-Holstein gegen das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein berichtet. Wir wiesen besonders auf die gemeinsame datenschutzrechtliche Verantwortung nach Artikel 26 Datenschutz-Grundverordnung (DS-GVO) zwischen Fanpage-Betreiberinnen bzw. -Betreibern und dem Unternehmen Facebook hin und forderten die Verantwortlichen auf, die Rechtmäßigkeit des Betriebs von Fanpages zu überprüfen.[2]

Im Jahr 2019 begannen wir damit, Stellungnahmen oberster Landesbehörden sowie nachgeordneter Behörden und Einrichtungen der Landesverwaltung einzuholen, von denen bekannt war, dass sie eine solche Präsenz betreiben.[3] Ziel war es, den genannten Stellen die Gelegenheit zu geben, selbst zu prüfen, ob ihnen hinreichende Informationen vorliegen, um den rechtmäßigen Betrieb einer Fanpage sicherzustellen und im Rahmen der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DS-GVO den Nachweis der Rechtmäßigkeit erbringen zu können. Dabei machten wir auf bestehende Probleme aufmerksam, die es einer Fanpage-Betreiberin bzw. einem -Betreiber aus unserer Sicht nicht erlaubten, die Verantwortung für den rechtmäßigen Betrieb zu übernehmen – insbesondere wegen fehlender Informationen seitens des Facebook-Konzerns und mangelnder Transparenz der Datenverarbeitung. Die Antworten zeigten, dass weder die erforderlichen Kenntnisse über die beim Besuch einer Facebook- Fanpage stattfindenden Datenverarbeitungsvorgänge vorlagen, noch die Rechtmäßigkeit des Betriebs der Fanpages selbst nachgewiesen werden konnte. Stattdessen lag das Hauptargument für die Nutzung in vielen Fällen in der Relevanz der sozialen Netzwerke, an der der

1 Urteil des Europäischen Gerichtshofs vom 5. Juni 2018, C-210/16.
2 Tätigkeitsbericht Datenschutz 2018, A IV 1.
3 Tätigkeitsbericht Datenschutz 2019, A II 1.

Staat partizipieren müsse, und der einfachen Erreichbarkeit von Bürgerinnen und Bürgern über diesen Kommunikationskanal.

Aus verschiedenen Gründen ruhten die Verfahren sodann für einige Zeit. Zum einen waren gerichtliche Entscheidungen[4] zur Umsetzung des genannten Urteils des Europäischen Gerichtshofs abzuwarten. Hierbei setzte jedes Gericht etwas andere Schwerpunkte und betonte unterschiedliche Nuancen in der Auslegung der europäischen Vorgaben, die für das Vorgehen der Datenschutzaufsichtsbehörden bedeutsam waren. Zum anderen war eine zwischenzeitlich ergangene weitere Entscheidung des Europäischen Gerichtshofs[5] zur gemeinsamen Verantwortlichkeit zu berücksichtigen.

Im November 2021 beauftragte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) eine Arbeitsgruppe damit, die Rechtsprechung auszuwerten und eine einheitliche Rechtsauffassung der Aufsichtsbehörden über die Rechtmäßigkeit des Fanpage-Betriebs zu erarbeiten. Dabei sollte auch geprüft werden, welche Auswirkungen das am 1. Dezember 2021 in Kraft getretene Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)[6] hatte. Ergebnis der Arbeitsgruppe, an der sich auch unsere Behörde beteiligte, war ein Kurzgutachten, das die Konferenz im März 2022 zur Kenntnis nahm und dessen Bewertungen sie teilte. Das Gutachten wurde ergänzt durch ein Merkblatt mit den wichtigsten Feststellungen in Form von FAQs (Frequently Asked Questions). Beide Dokumente sind auf unseren Internetseiten veröffentlicht.

Ebenfalls im März 2022 fasste die Konferenz den Beschluss, dass die Aufsichtsbehörden in ihrem Zuständigkeitsbereich den Betrieb von Facebook-Fanpages durch Landes- bzw. Bundesbehörden überprüfen und darauf hinwirken, diese Fanpages zu deaktivieren, falls die jeweils Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können. Dieser Nachweis betrifft insbesondere

4 Z. B. Urteil des Oberverwaltungsgerichts Schleswig-Holstein vom 25. November 2021, 4 LB 20/13.
5 Urteil des Europäischen Gerichtshofs vom 29. Juli 2019, C-40/17.
6 Siehe A I 2.

- den Abschluss einer Vereinbarung nach Artikel 26 DS-GVO über die gemeinsame Verantwortlichkeit mit Facebook,

- ausreichende Informationen gemäß Artikel 13 DS-GVO gegenüber den Nutzerinnen und Nutzern von Fanpages über die gemeinsamen Datenverarbeitungen,

- die Zulässigkeit zur Speicherung von Informationen in der Endeinrichtung der Nutzerin bzw. des Nutzers und der Zugriff auf diese Informationen gemäß § 25 TTDSG sowie

- die Zulässigkeit der Übertragung personenbezogener Daten in den Zugriffsbereich von Behörden in Drittstaaten ohne angemessenes Datenschutzniveau.

Zur Umsetzung dieses Beschlusses wandten wir uns im April 2022 erneut an die Ministerien sowie die nachgeordneten Behörden und Einrichtungen der Landesverwaltung, von denen bekannt war, dass sie eine Facebook-Fanpage betreiben, und forderten sie auf, den Nachweis der Rechtmäßigkeit dieser Datenverarbeitung zu erbringen. Auf die oben genannten Unterlagen wiesen wir dabei hin. Um sicherzustellen, dass das Verfahren einheitlich durchgeführt und Ergebnisse bei allen Fanpage-Betreiberinnen und -Betreibern der Landesverwaltung gleich umgesetzt werden, sowie zur Vereinfachung der Kommunikation stimmten wir zu, dass die Staatskanzlei stellvertretend für alle zu unserer Aufforderung Stellung nimmt. Nach entsprechenden Gesprächen und mehreren Verlängerungen der Antwortfrist erreichte uns im August 2022 ein Schreiben, in dem die Staatskanzlei ihren Rechtsstandpunkt vortrug.

Neben dem weiter bestehenden Argument, dass der Staat sich aus sozial relevanten Teilen des Internets nicht zurückziehen dürfe und seine Öffentlichkeitsarbeit auch dort betreiben müsse, wurden wir darüber informiert, dass das Unternehmen Facebook bereits im Juni dieses Jahres die sogenannte Insights-Funktion für die von der Staatskanzlei betriebene Fanpage abgeschaltet habe. Diese Funktion ermöglicht einer Fanpage-Betreiberin bzw. einem -Betreiber, verschiedene Statistiken und Analysen zu den Besuchen der Fanpage zu erhalten, um z. B. das Angebot zu optimieren. Die Auswertungen

basieren dabei natürlich auf der Verarbeitung personenbezogener Daten der Fanpage-Besucherinnen und -Besucher, welche durch Facebook vorgenommen wird – und zwar sowohl für beim sozialen Netzwerk angemeldete Personen als auch für solche, die dort kein Konto haben. Die Staatskanzlei war der Auffassung, dass mit Abschaltung der Insights-Funktion keine gemeinsame datenschutzrechtliche Verantwortung mehr vorliege, sondern Facebook allein für die Erfüllung der gesetzlichen Anforderungen zuständig sei.

Eine ähnliche Antwort mit gleichen Argumenten erhielten auch einige unserer Kolleginnen und Kollegen der anderen Datenschutzaufsichtsbehörden. Es war insofern folgerichtig, dass die von der Datenschutzkonferenz eingesetzte Arbeitsgruppe – weiterhin unter unserer Beteiligung – sich hiermit befasste, die Stellungnahmen prüfte und eine einheitliche Bewertung vornahm. Diese floss in eine Fortschreibung des Kurzgutachtens und des Merkblatts ein, welche im November 2022 von der Konferenz zustimmend angenommen wurden.

Aus inhaltlicher Sicht ist festzuhalten, dass die von der Staatskanzlei vorgebrachten Argumente zu keiner anderen datenschutzrechtlichen Bewertung führen. Sie trägt auch bei Abschaltung der Insights-Funktion eine Mitverantwortung im Sinne von Artikel 26 DS-GVO für den Betrieb der Facebook-Fanpage und die damit verbundene Verarbeitung personenbezogener Daten. Denn erst durch die Einrichtung der Fanpage wurde Facebook ermöglicht, personenbezogene Daten über die Interaktionen der Besucherinnen und Besucher zu erheben und auszuwerten. Eine solche Datenverarbeitung würde es ohne die Fanpage nicht geben. Damit werden nicht nur eigene Zwecke der Staatskanzlei, sondern auch die des Unternehmens gefördert. Nach der oben erwähnten Rechtsprechung des Europäischen Gerichtshofs reicht es für die Annahme einer gemeinsamen datenschutzrechtlichen Verantwortung aus, wenn beide Seiten von den Datenverarbeitungsvorgängen profitieren. Das ist hier der Fall, da die Staatskanzlei die Reichweite ihrer Öffentlichkeitsarbeit durch die Fanpage erhöhen und Facebook wiederum eine genauere und differenziertere Bildung

Datenverarbeitung bei Facebook weiter intransparent

von (Interessens-) Profilen der Besucherinnen und Besucher vornehmen kann.

Im Ergebnis konnten unsere Bedenken hinsichtlich der Rechtmäßigkeit des Fanpage-Betriebes nicht ausgeräumt werden. Wir werden nunmehr prüfen, ob eine Untersagungsverfügung nach Artikel 58 Absatz 2 Buchstabe f DS-GVO zu erlassen ist. Diese Entscheidung wird in enger Abstimmung mit anderen Aufsichtsbehörden erfolgen. Es ist zu hoffen, dass die staatlichen Stellen ihrer Vorbildfunktion gerecht werden und Wege finden, ihr legitimes Informationsinteresse nicht auf Kosten unwägbarer Datenschutzrisiken für interessierte Bürgerinnen und Bürger auszuüben.

2 Cookies und Tracking im Internet

2.1 Orientierungshilfe für Anbieterinnen und Anbieter von Telemedien

Cookies und ähnliche Technologien erlauben Anbieterinnen und Anbietern von Webseiten, Internetdiensten oder Apps, Daten auf den Geräten der Nutzerinnen und Nutzer abzulegen und von dort auszulesen. Werden hierbei eindeutige Kennungen verwendet, ist eine Zuordnung der Daten zu natürlichen Personen und die Auswertung ihrer Interessen sowie ihres individuellen Verhaltens im Internet möglich – oftmals auch über die Grenzen von Webseiten, Diensten oder Apps hinweg.

Sogenannte Cookie-Banner sind für Nutzerinnen und Nutzer häufig ein Hinweis auf den Einsatz der beschriebenen Technologien. Sie sollen – in der Regel bevor sie den Dienst oder die App in Anspruch nehmen – eine Einwilligung erteilen, dass Anbieterinnen und Anbieter Cookies o. Ä. verwenden dürfen. Dabei sind aus der rechtlichen Perspektive zwei Sachverhalte zu unterscheiden: zum einen die Speicherung der Daten im und das Auslesen aus dem Endgerät und zum anderen das (Weiter-) Verarbeiten, Nutzen, Auswerten, Übermitteln dieser Informationen durch Anbieterinnen und Anbieter bzw. durch Dritte. Als Endgerät (oder Endeinrichtung) werden in diesem Kontext

alle direkt oder indirekt an öffentliche Kommunikationsnetze (wie das Internet) angeschlossenen Geräte aufgefasst, also z. B. Laptops, Tablets und Mobiltelefone, aber auch mit dem Internet verbundene Smarthome-Geräte wie Fernseher, Küchengeräte, Alarmanlagen oder Steuergeräte.

Auch hinsichtlich der datenschutzrechtlichen Anforderungen sind zwei unterschiedliche Vorschriften zu beachten: Während die (Weiter-) Verarbeitung der Informationen aus Cookies und vergleichbaren, in der Endeinrichtung gespeicherten Daten nach den Regelungen der Datenschutz-Grundverordnung (DS-GVO) zu beurteilen ist, gelten für die vorgelagerten technischen Prozesse, insbesondere das Setzen von Cookies, die Vorgaben der EU-Richtlinie 2002/58/EG in der durch die Richtlinie 2009/136/EG geänderten Fassung (ePrivacy-Richtlinie). Zur Umsetzung dieser europäischen Richtlinie in nationales Recht trat in Deutschland am 1. Dezember 2021 das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)[7] in Kraft. Es führt die bisher getrennten datenschutzrechtlichen Regelungen aus dem Telekommunikationsgesetz und dem Telemediengesetz zusammen. Ziel des Gesetzgebers war der Abbau von Rechtsunsicherheiten, die sich aus der Abgrenzung der datenschutzrechtlichen Vorschriften in den beiden genannten Gesetzen zu denjenigen in der Datenschutz-Grundverordnung ergeben hatten.

Neue gesetzliche Regelungen zu Cookies beachten!

Das Telekommunikation-Telemedien-Datenschutz-Gesetz gilt für Anbieterinnen und Anbieter von Telekommunikationsdiensten unabhängig davon, ob es sich um klassische, nummerngebundene Telefonie oder hiervon unabhängige Dienste wie beispielsweise Webmail- oder Messenger-Dienste handelt. Es gilt weiter für Anbieterinnen und Anbieter von Telemediendiensten, also elektronischer Informations- und Kommunikationsdienste, die nicht bereits Telekommunikationsdienste oder klassischer Rundfunk sind. Hierunter fallen beispielsweise Webseiten- und andere Internetangebote wie Video-Streaming oder Online-Shops.

7 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 4 des Gesetzes vom 12. August 2021 (BGBl. I S. 3544; 2022 I 1045) geändert worden ist.

Der räumliche Anwendungsbereich des Gesetzes bestimmt sich ähnlich wie derjenige der Datenschutz-Grundverordnung nach dem sogenannten Marktortprinzip. Dem Gesetz unterliegen alle Unternehmen und Personen, die in seinem Geltungsbereich eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen. Es ist somit nicht erforderlich, dass der Hauptsitz des Verantwortlichen in Deutschland bzw. in der Europäischen Union liegt oder dort auch nur eine Niederlassung existiert.

Das Telekommunikation-Telemedien-Datenschutz-Gesetz regelt einerseits den Datenschutz und Schutz der Privatsphäre in der Telekommunikation. Hierzu wurden die entsprechenden Vorschriften des alten Telekommunikationsgesetzes in die §§ 3 bis 18 TTDSG überführt. Diese betreffen insbesondere die Vertraulichkeit der Kommunikation, die Wahrung des Fernmeldegeheimnisses oder die Verhinderung des Missbrauchs von Telekommunikationsanlagen und -diensten. Andererseits enthält das Gesetz in den §§ 19 ff. Vorgaben zum Telemediendatenschutz z. B. zur Umsetzung technischer und organisatorischer Vorkehrungen, zum Schutz personenbezogener Daten Minderjähriger oder zu Auskunftsverfahren aus Bestandsdaten. Vollständig neu gefasst wurden die Regelungen zur Speicherung von Informationen (wie Cookies) in Endeinrichtungen der Nutzerinnen und Nutzer und zum Zugriff auf diese Informationen sowie zu Diensten für die Verwaltung von Einwilligungen in Bezug auf die Cookie-Setzung und -Nutzung.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hat bereits im Dezember 2021 die „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien“ bereitgestellt. Sie enthält Hinweise und Hilfestellungen zur Anwendung des neuen Gesetzes. Im Berichtszeitraum gab die Konferenz Vertreterinnen und Vertretern aus Politik, Wirtschaft, Wissenschaft, Gesellschaft und Verwaltung im Rahmen eines Konsultationsverfahrens Gelegenheit, zu der Orientierungshilfe Stellung zu nehmen. Die zahlreichen Kommentare wurden im Rahmen eines Konsultationsberichts ausgewertet und die Orientierungshilfe fortgeschrieben. Die neue Version 1.1 liegt seit

Dezember 2022 vor; sie ist, wie der Konsultationsbericht auch, in unserem Internetangebot veröffentlicht.

Die wesentlichen Punkte der Orientierungshilfe sind:

- Die Speicherung von Informationen in der Endeinrichtung einer Nutzerin oder eines Nutzers sowie der Zugriff auf diese Informationen richten sich ausschließlich nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz. Es kommt nicht darauf an, ob die Informationen einen Personenbezug aufweisen, denn § 25 TTDSG fordert in diesen Situationen bis auf wenige Ausnahmen grundsätzlich immer die Einwilligung der Endnutzerin bzw. des Endnutzers. Während die genannte Vorschrift für das Setzen und Auslesen von Cookies und ähnlichen Technologien relevant ist, muss der Verantwortliche für die anschließende Verarbeitung der daraus erhobenen personenbezogenen Daten die Bestimmungen der Datenschutz-Grundverordnung beachten. Die beiden Phasen der Datenverarbeitung unterliegen somit unterschiedlichen rechtlichen Regelungen.

- Die Anforderungen an eine wirksame Einwilligung in diesem Kontext entsprechen denen der Datenschutz-Grundverordnung. Dazu zählen unter anderem die Informiertheit, die Freiwilligkeit und das Erfordernis einer unmissverständlichen, bestätigenden Handlung im konkreten Einzelfall. Die Nutzerin bzw. der Nutzer ist im Rahmen der Anwendungsbereiche des Telekommunikation-Telemedien-Datenschutz-Gesetzes und der Datenschutz-Grundverordnung ggf. separat über die jeweiligen Datenverarbeitungsvorgänge zu unterrichten, d. h. sowohl über das Setzen und Auslesen von Cookies o. Ä. als auch über eine etwaige danach erfolgende Verarbeitung personenbezogener Daten.

- Cookie-Banner zum Einholen der Einwilligung der Nutzerin oder des Nutzers sowie zu deren Information über Datenverarbeitungen müssen gleichwertige Handlungsmöglichkeiten aufweisen. So kann die Einwilligung zum Beispiel unwirksam sein, wenn nicht zwei Handlungsoptionen zur Verfügung stehen, die gleich schnell zur Nutzung des eigentlichen Dienstes führen. Die Nutzerin bzw. der Nutzer muss eine Einwilligung genauso einfach er-

teilen wie ablehnen können. Ein Cookie-Banner, welches einerseits die Schaltfläche „Alles Akzeptieren“ anzeigt, andererseits aber nur eine Schaltfläche mit Bezeichnungen wie „Einstellungen“ oder „Weitere Informationen“ enthält, um nach mehreren zusätzlichen Interaktionen das Setzen oder Auslesen von Cookies abzulehnen, ist mangels gleichwertiger Alternativen nicht ausreichend.

- Unzulässig ist es auch, wenn für den Widerruf einer Einwilligung zunächst die Datenschutzerklärung aufgerufen und dann in dieser zu der richtigen Stelle gescrollt werden muss. Ein solcher Suchvorgang als Zwischenschritt erschwert Nutzerinnen und Nutzern das Ausüben ihrer Rechte und ist nicht mit den gesetzlichen Vorgaben vereinbar. Erforderlich ist beispielsweise ein stets sichtbarer Direktlink oder ein im Dienst integriertes, mit den relevanten Einstellungsmöglichkeiten unmittelbar verknüpftes Bildsymbol.

- Zudem ist zu beachten, dass mit der Einbindung von Inhalten oder Diensten Dritter auf Webseiten regelmäßig eine Offenlegung personenbezogener Daten an die Betreiberinnen und Betreiber des jeweiligen Drittservers verbunden ist. Für diese Datenverarbeitung ist eine Rechtsgrundlage gemäß Artikel 6 Absatz 1 DS-GVO erforderlich. Typische Beispiele für solche Drittinhalte oder -dienste sind Werbeanzeigen, Schriftarten, Skripte, Stadtpläne, Videos, Fotos oder Inhalte von Social Media-Diensten. Für einen etwaigen Transfer personenbezogener Daten in Länder mit einem nicht angemessenen Datenschutzniveau (wie beispielsweise in die USA) sind von den jeweiligen Verantwortlichen weitere Prüfungen anzustellen und ggf. Maßnahmen zu ergreifen.

Die Orientierungshilfe formuliert hohe Anforderungen an Anbieterinnen und Anbieter von Telemedien. Deren Beachtung ist zur Einhaltung der gesetzlichen Vorgaben und zum Schutz der betroffenen Personen hinsichtlich ihrer Rechte und Freiheiten erforderlich. Sie bilden gleichzeitig den Maßstab unserer Beratungs- und Aufsichtstätigkeit.

2.2 Umgang mit Beschwerden über Cookies und Tracking

Die Landesbeauftragte erhielt im Berichtsjahr eine Vielzahl an Beschwerden zu den Themen Tracking, Einsatz von Cookies und Einbindung der Dienstleistungen von Drittanbieterinnen und Drittanbietern auf Webseiten. Erstaunlicherweise war die Anzahl der an uns in diesem Kontext gestellten Beratungsanfragen im Vergleich zur Anzahl der Beschwerden äußerst gering.

In den meisten Beschwerdefällen wurden die Ausgestaltung des Cookie-Banners, das Fehlen, die Platzierung oder die grafische Gestaltung von Auswahlmöglichkeiten zum Festlegen der Präferenzen, die mangelnde Transparenz der Verarbeitung von Nutzerdaten sowie fehlende, unvollständige bzw. unübersichtliche Datenschutzerklärungen moniert. Zum Teil enthielten die Beschwerden auch rechtliche Hinweise, in denen die Beschwerde führenden Personen die Rechtsgrundlage für eine Verarbeitung ihrer Daten durch Drittdienstleisterinnen bzw. -dienstleister oder die Zulässigkeit von Datenübermittlungen in Staaten außerhalb der Europäischen Union bezweifelten. Im Fokus standen dabei Cookies und Dienste des Konzerns Google – wie beispielsweise der Einsatz von Google Analytics oder die Einbindung von Google Fonts über die Server des Konzerns. Ein großer Teil der Beschwerden richtete sich gegen Webseiten kleinerer Unternehmen oder Blogs von Einzelpersonen.

Da auch der Landesbeauftragten die datenschutzrechtliche Komplexität des Themas und die in den letzten Jahren herrschende Rechtsunsicherheit bewusst war, verfolgte sie zunächst das Ziel, die jeweils Verantwortlichen zu beraten und mögliche Rechtsverstöße durch Hinweise und Empfehlungen zu beenden. Nach Eingang einer entsprechenden Beschwerde und Verifizierung des Beschwerdeinhalts versandten wir an die jeweiligen Betreiberinnen und Betreiber der Webseiten in der Regel ein Informationsschreiben, in dem wir unsere datenschutzrechtliche Einschätzung bezüglich der in den Internetpräsenzen vorhandenen Mängel, insbesondere bei der Verwendung von Cookies, der Ausgestaltung des Cookie-Banners oder der Einbindung von Drittdiensten, mitteilten. Außerdem übermittelten wir den Verantwortlichen ein technisches Prüfprotokoll, in dem wir die konkreten datenschutzrechtlichen Missstände dokumentierten.

Durch unsere rechtlichen und technischen Hinweise und Empfehlungen beabsichtigten wir, die jeweils Verantwortlichen zur Herstellung eines datenschutzkonformen Zustands ihrer Webseiten zu bewegen. Bislang gelang dies in der Regel auch, wie wir durch Nachprüfungen feststellen konnten. Insofern war die Landesbeauftragte im Berichtszeitraum auch nicht gezwungen, förmliche Verwaltungsverfahren zur Anordnung oder Untersagung im Sinne des Artikels 58 Absatz 2 Buchstabe d bzw. f Datenschutz-Grundverordnung einzuleiten, um gegenüber Verantwortlichen die Einhaltung der gesetzlichen Vorschriften durchzusetzen. Allerdings schließen wir derartige Maßnahmen für die Zukunft nicht aus, sollten Webseitenbetreiberinnen und -betreiber festgestellte Mängel nicht abstellen. Darüber hinaus ermöglicht uns die Datenschutz-Grundverordnung, rechtswidriges Verhalten in der Vergangenheit zusätzlich mit einer Verwarnung oder einer Geldbuße zu ahnden.

II Datenschutzverstöße: Maßnahmen und Sanktionen

1 Nutzung privater E-Mail-Adressen Beschäftigter für geschäftliche Zwecke

Durch die Beschwerde eines Betroffenen erfuhren wir davon, dass ein brandenburgisches Unternehmen über mehrere Jahre hinweg die privaten E-Mail-Adressen der Beschäftigten für geschäftliche Zwecke nutzte. Die Firma erbringt mit einer dreistelligen Anzahl von Außendienstmitarbeiterinnen und -mitarbeitern deutschlandweit Reparatur- und andere Kundendienstleistungen.

Zunächst waren die Beschäftigten im Außendienst über viele Jahre selbstständig tätig. In diesem Zusammenhang entschieden sie auch eigenverantwortlich über die durch sie verwendeten Mittel der Kommunikation. Seit 2015 jedoch – so teilte uns das Unternehmen mit – wurden die betroffenen Personen im Zuge einer Umstrukturierung fest angestellt. Dabei verzichtete die Firma aus Gründen der Bequemlichkeit darauf, die Nutzung der privaten E-Mail-Adressen für geschäftliche Zwecke zu unterbinden. Vielmehr wurden sie weiter verwendet, um beispielsweise unternehmensinterne Kommunikation abzuwickeln, Aufträge zu verteilen, Arbeitsanweisungen zu geben, Abläufe zu koordinieren, Bestellungen zu bearbeiten oder geplante Urlaubszeiten abzustimmen. Darüber hinaus sollten die Beschäftigten diesen Kommunikationsweg auch wählen, wenn eine Bilddokumentation im Zusammenhang mit Dienstleistungen bei Kundinnen und Kunden erforderlich war. Insofern wurden also auch Daten Dritter ausgetauscht. Ferner gab das Unternehmen die privaten E-Mail-Adressen an externe Dienstleister weiter, etwa an ein Unternehmen, das mit der Kontrolle der Führerscheine der Beschäftigten beauftragt war oder an Behörden für die Verfolgung von Ordnungswidrigkeiten, die mit den bereitgestellten Geschäftsfahrzeugen begangen wurden.

Immer wieder beschwerten sich Beschäftigte bei der Unternehmensleitung über diese Praxis. Wie wir einzelnen internen E-Mails entnehmen konnten, waren in den IT-Systemen der Firma offensichtlich neben den privaten E-Mail-Adressen auch die Telefonnummern der Außendienstmitarbeiterinnen und -mitarbeiter gespeichert. Beide Kontaktmöglichkeiten gaben die für die Koordination von Anfragen und Aufträgen Zuständigen des Unternehmens bereitwillig an Kun-

dinnen und Kunden heraus, die sich dann auch zu ungewöhnlichen Tageszeiten mit den jeweiligen Beschäftigten in Verbindung setzten. Dieser Umstand war jedoch nicht Teil der Beschwerde an uns.

Erst 2020 wurde die Nutzung der privaten E-Mail-Adressen und Telefonnummern beendet. Im Zuge der schrittweisen Ausstattung mit neuen mobilen Endgeräten stellte das Unternehmen auch alle verwendeten E-Mail-Adressen auf solche aus seiner Internetdomäne um. Dieser Prozess war zwar im November 2020 abgeschlossen, allerdings fanden sich in den genutzten IT-Systemen noch vereinzelt alte, nicht mehr zu verwendende Kontaktangaben. Die Suche danach und deren Löschung dauerten noch mehrere Monate und wurden flankiert von Sensibilisierungen der zugriffsberechtigten Beschäftigten sowie internen Anweisungen, in denen die Nutzung untersagt wurde.

Von uns zur Stellungnahme aufgefordert, gab das Unternehmen an, die Verarbeitung der privaten E-Mail-Adressen auf die gesetzlichen Erlaubnistatbestände des Beschäftigtendatenschutzes zu stützen. Nach § 26 Absatz 1 Bundesdatenschutzgesetz (in der seit 2018 geltenden Fassung) dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies u. a. für dessen Durchführung erforderlich ist. Für die Zeit davor verwies das Unternehmen auf eine gleichlautende Vorschrift in der alten Fassung des Bundesdatenschutzgesetzes.

Diese Begründung war jedoch nicht tragfähig. Hinsichtlich der Eigenschaft der Erforderlichkeit sind im Datenschutzrecht strenge Maßstäbe anzulegen. Insbesondere darf es keine alternativen Möglichkeiten geben, den Zweck der Verarbeitung mit Mitteln zu erreichen, die weniger tief in die Rechte und Freiheiten der betroffenen Personen eingreifen. Genau solche Alternativen gab es allerdings im vorliegenden Fall. Durch die Nutzung von E-Mail-Adressen aus der Domäne des Unternehmens und von geschäftlichen Telefonnummern wurde in erheblich geringerem Maß in die Privatsphäre der Beschäftigten eingegriffen. Nachteile sind dadurch offensichtlich nicht entstanden. Die Umsetzung war auch zumutbar und mit vertretbarem Aufwand zu bewerkstelligen, wie das 2020 abgeschlossene Projekt zeigt.

Auch andere Rechtsgrundlagen konnten die Verarbeitung der privaten E-Mail-Adressen der Beschäftigten für geschäftliche Zwecke nicht rechtfertigen, insbesondere nicht die vom Unternehmen hilfsweise angegebene Vorschrift des Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO). Danach ist die Verarbeitung personenbezogener Daten erlaubt, wenn sie zur Wahrung der berechtigten Interessen des Unternehmens erforderlich (in dem genannten Sinne) ist und nicht die schutzwürdigen Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen. Mit denselben Argumenten wie oben kann schon der erste Teil der Bedingung nicht erfüllt werden. Die in der Beschwerde monierte Praxis war insofern rechtswidrig.

Ergänzend ist darauf hinzuweisen, dass die Nutzung der privaten E-Mail-Adressen der Beschäftigten auch zur Folge hatte, dass diese die jeweiligen E-Mail-Provider auswählten. Das Unternehmen hatte keine Kontrolle darüber, ob diese Provider bei der Kommunikation das Telekommunikationsgeheimnis einhielten oder datenschutzrechtlich im Wege einer Auftragsverarbeitung hätten gebunden werden müssen. Insbesondere wurden auch E-Mail-Adressen genutzt, die zu Dienstleistern in den USA gehören, sodass sich aus Datenschutzsicht zusätzlich die Frage der Rechtmäßigkeit der Übermittlung personenbezogener Daten in Drittstaaten stellte.

Trotz der bereits abgestellten Mängel haben wir das Unternehmen wegen der mehrere Jahre andauernden Verstöße gegen die datenschutzrechtlichen Regelungen nach Artikel 58 Absatz 2 Buchstabe b DS-GVO verwarnt. Hierbei berücksichtigten wir, dass von den Verantwortlichen ein Wandel in der Unternehmenskultur glaubhaft dargelegt und dabei die Bedeutung des Datenschutzes hervorgehoben wurde. Positiv schlug auch zu Buche, dass die Firma bereits vor unserem Tätigwerden agiert hatte. Auf die Verhängung einer Geldbuße verzichteten wir deshalb.

2 Unzureichende Tests vor Einsatz selbst entwickelter Software

Eine weltweit agierende E-Commerce-Plattform, deren europäische Hauptniederlassung sich in Brandenburg befindet, meldete der Landesbeauftragten in den vergangenen beiden Jahren mehrfach Verletzungen des Schutzes personenbezogener Daten im Sinne von Artikel 33 Absatz 1 Datenschutz-Grundverordnung (DS-GVO). Bei näherer Überprüfung stellte sich heraus, dass die Vorfälle hätten verhindert werden können, wenn das Unternehmen die selbst entwickelte Software vor deren Einsatz im Produktivbetrieb umfassender, systematischer und sorgfältiger getestet hätte.

Gegenstand der ersten Meldung nach Artikel 33 DS-GVO war ein Softwarefehler, der die in der Datenbank des Verantwortlichen gespeicherte Geschäftsadresse einer Verkäuferin bzw. eines Verkäufers mit ihrer bzw. seiner Wohnadresse überschrieb, wenn die zuletzt genannte Anschrift aktualisiert werden sollte. Im Ergebnis wurde die Wohnadresse von ca. 1.200 bis 1.300 Personen als deren Geschäftsadresse im Portal angezeigt. Andere personenbezogene Daten z. B. zu Bankverbindungen oder Transaktionen waren laut Angaben des Verantwortlichen nicht von dem Vorfall betroffen. Der Fehler wurde durch eine falsche Verknüpfung von Datenbankfeldern der Software verursacht. Er trat bereits in der Entwurfsphase der Softwareentwicklung auf und wurde weder bei der Testplanung in Betracht gezogen noch bei der Durchführung der Tests im Anschluss an die Implementierung bemerkt.

In einer weiteren Meldung nach Artikel 33 DS-GVO informierte uns das Unternehmen, dass ein anderer Softwarefehler eine unbefugte Offenlegung von personenbezogenen Daten verursachen konnte. Der Fehler trat im Zusammenhang mit dem sogenannten Social Login (z. B. über ein Facebook- oder Google-Konto) auf und wurde von zwei deutschen Nutzern entdeckt, die ihn auch dem Kundenservice des Verantwortlichen meldeten. Eine potenzielle Angreiferin bzw. ein potenzieller Angreifer hätte sich zunächst mit einer korrekten Kombination aus Benutzername und Passwort über ein Social Login in das eigene Konto einloggen müssen. Hierbei speichert der jeweilige Webbrowser eine eindeutige, einzigartige und maschinen-

generierte Kennung (Token), die die erfolgreiche Anmeldung bei der anschließenden Nutzung der Webseiten bestätigt und mit dem Abmelden für ungültig erklärt und gelöscht wird. Wäre zuvor allerdings in der Browsersitzung ein Wechsel in ein anderes Nutzerkonto initiiert worden, hätte die Plattform nur den Namen des gewünschten Nutzerkontos erfragt, jedoch keine Eingabe des zugehörigen Passworts erzwungen. Im Rahmen eines Angriffs hätte so ein Login in ein fremdes Konto erfolgen können. Auch hier soll die Ursache ein Fehler in der Designphase der Software gewesen sein, der in keinem der nachfolgenden Tests oder bei der speziellen Suche nach Sicherheitslücken auffiel.

Datenschutzvorfälle durch Tests verhindern

Der Verantwortliche stellte uns im Rahmen einer Stellungnahme den Prozess der Softwareentwicklung im Unternehmen (Software Development Lifecycle) vor. Der besondere Fokus lag dabei auf der Phase des Testens, in der unterschiedliche Arten von Tests (wie Benutzerakzeptanztests, Modultests, funktionale Tests in einzelnen oder mehreren Softwarekomponenten u. a.) durchgeführt werden. Erläutert wurde, dass erst nachdem Beschäftigte der Qualitätssicherung eine Freigabe erteilt haben und auch das Informationssicherheitsmanagementteam zugestimmt hat, eine neue oder weiterentwickelte Softwareversion produktiv eingesetzt wird.

Das Unternehmen sah schon nach der ersten gemeldeten Datenschutzverletzung Verbesserungsmöglichkeiten im Entwicklungsprozess. So wurden beispielsweise die Zusammenarbeit der Arbeitsgruppen in den verschiedenen Phasen der Softwareentwicklung intensiviert, eine spezielle, verpflichtend zu nutzende Programmierschnittstelle für den Zugriff auf Datenbanken eingeführt und ein Notfallteam mit der Behebung von festgestellten Mängeln oder Fehlern beauftragt. Allerdings verhinderten diese Maßnahmen nicht, dass uns weitere Meldungen nach Artikel 33 DS-GVO erreichten, sodass wir an der konsequenten Umsetzung zweifelten.

Aufgrund der grenzüberschreitenden Verarbeitung personenbezogener Daten beteiligten wir die anderen europäischen Datenschutzaufsichtsbehörden an der Diskussion über Sanktionsmaßnahmen gegen

das Unternehmen. Hierzu sind wir nach den Regelungen des siebten Kapitels der Datenschutz-Grundverordnung verpflichtet. Im Ergebnis des entsprechenden Kohärenzverfahrens sprach die Landesbeauftragte eine Verwarnung gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO wegen eines Verstoßes gegen Artikel 24, 32 DS-GVO aufgrund der mangelhaften bzw. nicht hinreichend wirkungsvollen technischen und organisatorischen Maßnahmen während der Entwicklung der Software und ihrer Überführung in den Produktivbetrieb aus. Die vom Verantwortlichen zu treffenden Maßnahmen hätten Vorfälle, deren Ursache das Unternehmen in „menschlichem Versagen“ sah, verhindern müssen – erst recht vor dem Hintergrund der hohen Anzahl an Nutzerinnen und Nutzern der Plattform.

3 Videoüberwachung einer Saunalandschaft

Ein Bürger informierte uns über eine mutmaßliche Videoüberwachung in einer Saunalandschaft. Er teilte mit, dass sowohl auf dem gesamten Gelände als auch im Innern der einzelnen Saunen Videokameras aufgestellt seien.

Wir eröffneten umgehend das förmliche Verwaltungsverfahren und hörten den Verantwortlichen hinsichtlich der Videoüberwachung an. Daraufhin teilte dieser mit, insgesamt sechs Videokameras auf seinem Gelände einzusetzen. Zwei dieser Videokameras wurden innerhalb der Saunen verwendet. Sie sollten zur Live-Überwachung von bis zu fünf täglichen Show-Aufgüssen mit Licht- und Soundeffekten dienen. Der zuständige Techniker beobachtete das Geschehen über ein Live-Videobild. Während dieser Aufgüsse befinden sich bis zu 200 größtenteils unbekleidete Besucherinnen und Besucher sowie mindestens ein Beschäftigter des Verantwortlichen, der für den Aufguss zuständig ist, in der Sauna. Die Videoaufnahmen aus den Saunen wurden zwar nicht gespeichert, stellten aber dennoch einen gravierenden Eingriff in die Rechte der betroffenen Personen dar. Schließlich wurden dabei immer wieder Menschen leicht- oder unbekleidet von Videokameras erfasst.

Die anderen vier Videokameras betrafen unter anderem den Kassen- und Tresorbereich sowie die Lager auf dem Gelände. Sie zeichneten

dauerhaft auf und speicherten die Aufnahmen. Dabei wurden Besucherinnen und Besucher sowie Beschäftigte des Verantwortlichen gleichermaßen erfasst. Eine umfangreiche Überwachung der Beschäftigten war somit möglich.

In der Sauna unter Beobachtung?

Nach diesen Feststellungen luden wir den Verantwortlichen zu einer Beratung ein, um die Sach- und Rechtslage sowie dringend erforderliche Anpassungen zu erörtern. In diesem konstruktiven Gespräch zeigte er sich bereit, umfangreiche Änderungen an der Videoüberwachung vorzunehmen. Schon zuvor hatte er schriftlich mitgeteilt, dass eine der Videokameras in den Saunen bereits deaktiviert worden sei.

Der Verantwortliche hat im Nachgang alle Videokameras auf dem Gelände überprüft und so eingestellt, dass diese nur noch außerhalb der Geschäftszeiten in Betrieb sind. Dies stellt sicher, dass keine Angestellten oder Besucherinnen und Besucher von der Videoüberwachung erfasst werden. Die verbleibende Videokamera innerhalb einer der Saunen wurde mittels eines Holzbretts abgedeckt und darf nur noch zu Trainingszwecken der Beschäftigten außerhalb der Geschäftszeiten genutzt werden. Dadurch werden keine unbekleideten Besucherinnen und Besucher mehr von der Kamera erfasst.

Aufgrund der Bereitschaft des Verantwortlichen, schnell und umfassend Änderungen an der Videoüberwachung vorzunehmen und damit einen datenschutzkonformen Zustand herzustellen, beließen wir es bei einer Verwarnung nach Artikel 58 Absatz 2 Buchstabe b Datenschutz-Grundverordnung. Das Verfahren haben wir damit abgeschlossen.

4 Datenübermittlungen der Rentenversicherung an Jobcenter und Arztpraxen

Mit einer Beschwerde wandte sich ein Bürger an uns und teilte seinen Unmut über eine Datenerhebung und -übermittlung durch die Deutsche Rentenversicherung Berlin-Brandenburg (im Folgenden:

Rentenversicherung) mit. Dort hatte er eine Rehabilitationsmaßnahme beantragt. In einem Widerspruchsverfahren gegen die erste Entscheidung der Rentenversicherung machte er geltend, dass diese seinen gegenwärtigen Gesundheitszustand nicht berücksichtigt habe. Als Nachweis legte der Beschwerdeführer ein aktuelles Attest eines Facharztes vor. Die Rentenversicherung wandte sich daraufhin an seinen Hausarzt und bat um Auskunft. Bekannt war der Hausarzt der Rentenversicherung aufgrund eines Attests, welches der Beschwerdeführer vor dem Widerspruchsverfahren eingereicht hatte. Der Hausarzt übermittelte der Rentenversicherung einen aktuellen Befundbericht.

Unabhängig davon hatte die Rentenversicherung die Gewährung einer Rehabilitationsmaßnahme für den betroffenen Bürger dem Jobcenter mitgeteilt, von dem er Sozialleistungen bezog. Ziel war unter anderem ein Abgleich, um während des Zeitraums der Rehabilitation mögliche Doppelleistungen durch beide Stellen zu vermeiden.

Eine Einwilligung zu einer solchen Datenerhebung oder -übermittlung hatte der Beschwerdeführer nicht gegeben. Sowohl von der Datenübermittlung an das Jobcenter als auch über die Datenerhebung bei dem Hausarzt wurde der Beschwerdeführer nicht informiert. Vielmehr erhielt er lediglich durch Akteneinsicht bei der Rentenversicherung Kenntnis von den Vorgängen.

Verantwortliche benötigen für die Verarbeitung personenbezogener Daten einen Erlaubnistatbestand. Dieser kann sich aus Artikel 6 Absatz 1 Buchstabe c Datenschutz-Grundverordnung (DS-GVO) ergeben, wonach die Verarbeitung zulässig ist, wenn die Erfüllung einer rechtlichen Verpflichtung sie erfordert. Als Sozialleistungsträgerin im Sinne des Sozialrechts ist die Rentenversicherung Verantwortliche für die Datenverarbeitung. Sie kann sich daher bei Wahrnehmung ihrer gesetzlichen Aufgabe zur Datenverarbeitung u. a. auf die Befugnisse der §§ 67 ff. Zehntes Buch Sozialgesetzbuch (SGB X) stützen, muss dabei jedoch die strengen Voraussetzungen des Sozialdatenschutzes – insbesondere das Sozialgeheimnis – wahren. Als Sozialdatum gilt auch die Information, dass ein Sozialverwaltungsverfahren zu einer bestimmten Person geführt wird.

Außerdem handelt es sich bei den Angaben zu Rehabilitationsleistungen und zum Gesundheitszustand um Gesundheitsdaten. Als besondere Datenkategorie unterliegt die Verarbeitung dieser Angaben den besonderen Rechtmäßigkeitsvoraussetzungen des Artikels 9 Absatz 2 DS-GVO. Nach Buchstabe b dieser Vorschrift darf die Rentenversicherung zur Wahrnehmung der Rechte der sozialen Sicherheit und des Sozialschutzes aber auch solche sensitiven Daten verarbeiten. Das Sozialgeheimnis ist auch hier zu wahren.

Die direkte Datenerhebung bei dem Hausarzt des Beschwerdeführers durch die Rentenversicherung war im vorliegenden Fall rechtswidrig. Nach § 67a Absatz 2 Satz 1 SGB X hätte sie versuchen müssen, die erforderlichen Daten über den aktuellen Gesundheitszustand des Beschwerdeführers bei ihm selbst zu erheben (Ersterhebungsgrundsatz). Scheitert dies oder droht der betroffenen Person durch das Unterlassen ein erheblicher Nachteil, kann eine Datenerhebung gemäß § 67a Absatz 2 Satz 2 SGB X bei einer anderen Person oder Stelle zulässig sein. Hier hatte die Rentenversicherung ein aktuelles Attest eines Facharztes durch den Beschwerdeführer erhalten. Wäre nach ihrer Auffassung ein weiteres Attest erforderlich gewesen, hätte sie den Betroffenen kontaktieren und zu dessen Vorlage auffordern müssen. Eine Erforderlichkeit zur Datenerhebung direkt beim Hausarzt war somit nicht gegeben. Das Kontaktieren des Hausarztes ohne vorherigen Versuch einer Datenerhebung beim Beschwerdeführer stellte eine Verletzung des Ersterhebungsgrundsatzes dar. Außerdem wurden ihm durch die Anfrage Daten, die unter das Sozialgeheimnis fallen, offenbart.

Auch die Datenübermittlung an das Jobcenter zur Rehabilitationsmaßnahme war unrechtmäßig. Sie wäre nur dann zulässig gewesen, wenn sie zur Erfüllung der gesetzlichen Aufgabe der Rentenversicherung erforderlich gewesen wäre. Es ist jedoch nicht Teil der gesetzlichen Aufgabe der Rentenversicherung, Angaben über Rehabilitationsmaßnahmen an ein Jobcenter zu übermitteln. Sie hat damit das Sozialgeheimnis verletzt.

Aufgrund der Verstöße haben wir eine Verwarnung gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO ausgesprochen.

5 Bericht der Bußgeldstelle

5.1 Live-Bilder aus dem Vorraum einer Bank

Ein Kreditinstitut betrieb in einer seiner Geschäftsstellen eine Videoüberwachungskamera. Sie erfasste neben Teilen des Foyers der Filiale mit Kontoauszugsdrucker und Geldautomaten den Eingangsbereich und durch die großflächige Fensterfront auch den davorliegenden Gehweg und die Parkplätze. Für den Kamerabetrieb setzte die Betreiberin zwei dienstleistende Unternehmen ein, ohne mit ihnen einen datenschutzrechtlichen Auftragsverarbeitungsvertrag abzuschließen. Die eine Firma konfigurierte und wartete das Kamerasystem. Die andere sollte bei einer Alarmauslösung durch das System sowie zur Funktionsüberprüfung auf die Kamera zugreifen. Die Übertragung der Bilder sowie der Befehle zum Zugriff erfolgten dabei unverschlüsselt über das Internet. Unbekannte Dritte kompromittierten schließlich die Videokamera und stellten die Echtzeitbilder für jedermann abrufbar ins Netz. In begrenztem Umfang war es auch möglich, die Kamera zu steuern.

Geld abheben – und alle sehen zu

Das Kreditinstitut hatte es versäumt, geeignete technisch-organisatorischen Maßnahmen umzusetzen, um ein dem Risiko der Verarbeitung personenbezogener Daten angemessenes Schutzniveau zu gewährleisten und somit den Anforderungen der Datenschutz-Grundverordnung (DS-GVO) zu entsprechen. Hierfür wäre neben weiteren Maßnahmen jedenfalls die Einrichtung einer Transportverschlüsselung für die Internetkommunikation erforderlich gewesen, insbesondere um einen unbefugten Zugriff Dritter auf die Videobilder und die Steuerung der Kamera zu verhindern. Außerdem hätte mit beiden externen Dienstleistern, die Zugriff auf die Videobilder nehmen konnten, ein schriftlicher Auftragsverarbeitungsvertrag gemäß Artikel 28 DS-GVO abgeschlossen werden müssen. Auch die Tatsache, dass die im Foyer betriebene Videokamera den davorliegenden Gehweg samt Kfz-Stellplätzen erfasste – und so die personenbezogenen Daten der vorbeilaufenden Fußgängerinnen und Fußgänger sowie die Kfz-Kennzeichen der geparkten Fahrzeuge verarbeitet wurden – stellte einen Verstoß dar.

Aufgrund der nicht unerheblichen Zeitspanne von ca. 17 Monaten, in denen die Verstöße vorlagen und die Kamera potenziellen Angriffen durch Dritte ohne den gebotenen Schutz ausgesetzt war, war es erforderlich, eine Geldbuße zu verhängen. Eine Geldbuße als eindrückliche Pflichtenmahnung soll bewirken, dass der Verantwortliche sich künftig rechtstreu verhält. Nach Artikel 83 Absatz 1 DS-GVO stellt die Aufsichtsbehörde sicher, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Neben den tat- und täterbezogenen Umständen sowie spezial- und generalpräventiven Gesichtspunkten muss auch die Höhe des Vorjahresumsatzes des Unternehmens Berücksichtigung finden.

Durch den wochentags stattfindenden Kundenverkehr in der Filiale war eine nicht unerhebliche Anzahl von Personen von der Datenverarbeitung ohne ausreichende Sicherheitsvorkehrungen betroffen. Des Weiteren war zu berücksichtigen, dass die Bilddaten zahlreicher Personen durch den erfolgreichen Angriff Dritter von einem weiten Personenkreis zur Kenntnis genommen werden konnten. Eine Veröffentlichung von Bilddaten im Internet geht mit unkalkulierbaren Risiken für die betroffenen Personen einher. So kann eine Weiterverwendung durch Dritte nicht kontrolliert und können Löschansprüche nicht wirksam durchgesetzt werden. Aufgrund der möglichen Identifizierbarkeit der betroffenen Personen sowie der Möglichkeit, die Zoomfunktion der Kamera zu steuern, wurden die betroffenen Personen dem Risiko ausgesetzt, dass die Erkenntnisse rufschädigend, zum Identitätsdiebstahl oder für gezielte Überfälle verwendet werden. Daneben hatten die Auftragsverarbeiter ohne eine schriftliche Fixierung ihrer Rechte und Pflichten Zugriff auf personenbezogene Daten. Dies birgt Risiken für die Rechte der von der Datenverarbeitung betroffenen Personen, da es dem Verantwortlichen im Zweifel erschwert wird, die Rechte gegenüber dem Auftragsverarbeiter zu proklamieren und durchzusetzen.

Für die drei begangenen Verstöße setzten wir insgesamt eine Geldbuße im oberen fünfstelligen Bereich fest. Insbesondere die kooperative Mitwirkung des Kreditinstituts im Verwaltungsverfahren, sowie der Umstand, dass sie nach dem Datenschutzvorfall unverzüglich reagierte, wurden hierbei mildernd berücksichtigt.

5.2 Newsletter statt Kontaktnachverfolgung

Während der Corona-Pandemie verlangte eine Gaststättenbetreiberin anlässlich der gesetzlich vorgegebenen Kontaktnachverfolgung von den Besucherinnen und Besuchern, im Restaurant ausgelegte Papierbögen auszufüllen. Anzugeben waren der Vor- und Nachname, eine vollständige Anschrift, die Telefonnummer und E-Mail-Adresse. Die zu diesem Zeitpunkt geltende SARS-CoV-2-Eindämmungsverordnung verlangte zwar von Betreibenden eines Restaurants die Kontaktdatenerhebung. Die Erhebung einer E-Mail-Adresse war hierbei jedoch nicht vorgesehen. Auf den ausgelegten Kontaktbögen war zudem ein Ankreuzfeld „Ich bin damit einverstanden, dass mich das Restaurant kontaktieren kann." aufgedruckt. Die im Rahmen der Corona-Kontaktnachverfolgungsbögen angegebenen E-Mail-Adressen nutzte die Restaurantbetreiberin im Nachgang zur Versendung ihres Newsletters für Werbezwecke.

Die Verarbeitung der E-Mail-Adresse erfolgte unbefugt, da weder für die Erhebung noch für die Verwendung einer der in Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) genannten Erlaubnistatbestände erfüllt war.

Nach Artikel 6 Absatz 1 Buchstabe a DS-GVO kann eine Datenverarbeitung rechtmäßig sein, wenn die betroffene Person ihre Einwilligung zur der Datenverarbeitung gegeben hat. Erfolgt die Einwilligung der betroffenen Person durch schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss gemäß Artikel 7 Absatz 2 DS-GVO das Ersuchen um Einwilligung so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Außerdem muss dieses Ersuchen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache formuliert sein. Gemäß Artikel 7 Absatz 3 DS-GVO hat die betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen. Auf ihr Widerrufsrecht ist die betroffene Person vor Abgabe ihrer Einwilligung hinzuweisen.

Vorliegend waren die Regelungen zur Bedingung der Einholung einer rechtmäßigen Einwilligung nicht erfüllt. Zum einen sollten Kontaktdaten im Zusammenhang mit der Corona-Pandemie erhoben und zum anderen personenbezogene Daten zu Werbezwecken, nämlich

zur Versendung des Newsletters der Gaststätte, erfasst werden. Dass sich das oben genannte Ankreuzfeld auf die Versendung eines Werbe-Newsletters bezog und nicht im Zusammenhang mit der Corona-Pandemie stand, war für die Besucherinnen und Besucher des Restaurants in keiner Weise erkennbar. Darüber hinaus wurden die betroffenen Personen nicht darüber informiert, dass sie die zu Werbezwecken abgegebene Einwilligungserklärung jederzeit widerrufen können.

Die Gaststättenbetreiberin unterlag auch keiner rechtlichen Verpflichtung zur Erfassung der E-Mail-Adressen der Besucherinnen und Besucher entsprechend Artikel 6 Absatz 1 Buchstabe c DS-GVO i. V. m. der SARS-CoV-2-Eindämmungsverordnung. Das Erfassen der E-Mail-Adresse widersprach dabei bereits dem im Datenschutzrecht geltenden Erforderlichkeitsgrundsatz.

Nach Artikel 6 Absatz 1 Buchstabe f DS-GVO kann eine Datenverarbeitung rechtmäßig sein, wenn sie 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. Aufgrund der Tatsache, dass es im vorliegenden Fall bei der Datenerhebung zu einer Vermischung von Zwecken der Datenverarbeitung kam, konnte das unternehmerische Interesse auch bezüglich der Erhebung zum Zweck des Newsletter-Versands die Grundrechte und Grundfreiheiten der betroffenen Personen aber nicht überwiegen. Diese durften nämlich davon ausgehen, dass ihre personenbezogenen Daten ausschließlich zur Corona-Kontaktnachverfolgung verwendet werden und die Gaststättenbetreiberin hierbei den gesetzlich vorgegebenen Rahmen nicht überschreitet.

Keine Einwilligung unterjubeln!

Sowohl die Erhebung als auch die Verwendung der E-Mail-Adressen erfolgte damit rechtsgrundlos und stellte einen Verstoß gegen die Datenschutz-Grundverordnung dar.

Artikel 83 Absatz 1 DS-GVO bestimmt, dass die Geldbuße in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein muss. Bei

der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag waren die Kriterien des Artikels 83 Absatz 2 DS-GVO gebührend zu berücksichtigen.

Insbesondere war für unsere Entscheidung von Bedeutung, dass der Zweck der Verstöße einen wirtschaftsorientierten Charakter aufwies, weil datenschutzrechtliche Regelungen nicht eingehalten wurden, um wirtschaftliche Vorteile zu erzielen. Die Gewinnung von E-Mail-Adressen zu Werbezwecken ist bei der Einholung einer informierten, rechtmäßigen Einwilligung in der Regel weniger einfach zu erzielen, als es der Betreiberin vorliegend über die Corona-Kontaktbögen gelang. Daneben war eine Vielzahl von Personen betroffen. Zu berücksichtigen war auch, dass bei den betroffenen Personen der Eindruck erweckt wurde, sich an datenschutzrechtliche Vorgaben zu halten. Sie gaben ihre Daten damit unter der Annahme an, dass diese vertraulich und datenschutzkonform behandelt würden. Das Vertrauen in die rechtmäßige Datenverarbeitung wurde durch dieses Handeln verletzt.

Wir setzten eine Geldbuße im unteren fünfstelligen Bereich fest, welche von der Gaststättenbetreiberin akzeptiert wurde.

5.3 Missbrauch von Corona-Kontaktdaten durch Bäderbetrieb

Durch eine Beschwerde erlangten wir davon Kenntnis, dass Besucherinnen und Besucher eines Freibades auf einem Erfassungsdatenblatt zur Kontaktnachverfolgung im Zusammenhang mit der Corona-Pandemie folgende Daten angeben mussten: Vor- und Nachnamen, Telefonnummer, Wohnort, Datum und Zeitraum des Aufenthaltes. Auf diesem Weg erfasste die Betreiberin im Sommer 2021 ca. 4.700 Datensätze betroffener Personen.

Die zum Zeitpunkt der Datenerhebung geltende SARS-CoV-2-Umgangsverordnung verpflichtete Betreiberinnen und Betreiber von Freibädern zum Zweck der Kontaktnachverfolgung jedoch nur zur Erhebung des Vor- und Nachnamens, der Telefonnummer oder der E-Mail-Adresse sowie von Datum und Zeitraum des Aufenthaltes. Die Regelungen umfassten hingegen nicht die Erhebung der per-

sonenbezogenen Daten über den Wohnort der Besucherinnen und Besucher. Damit war die Erhebung des Wohnortes durch die Betreiberin für die Erfüllung der rechtlichen Verpflichtung nach der SARS-CoV-2-Umgangsverordnung nicht erforderlich, Artikel 6 Absatz 1 Buchstabe c Datenschutz-Grundverordnung.

Wegen dieses Datenschutzverstoßes setzten wir ein Bußgeld in fünfstelliger Höhe fest. Dabei waren die hohe Zahl der betroffenen Personen, das verletzte Vertrauen in die Rechtmäßigkeit der Datenverarbeitung sowie die Höhe des Jahresumsatzes zu berücksichtigen. Die Betreiberin des Schwimmbades akzeptierte das Bußgeld.

5.4 Hackerangriff auf die Webseite eines Verbandes der Gesundheitsbranche

Ein Kreisverband einer überregional tätigen Hilfs- und Wohlfahrtsorganisation meldete uns die Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO). Er bietet Fahrdienste für Krankenbeförderung und Erste-Hilfe-Kurse an. Die für die Krankenbeförderung notwendigen Datensätze der Kundinnen und Kunden wurden durch Beschäftigte des Verbandes im passwortgeschützten, internen Bereich der Webseite eingegeben. Die Datensätze beinhalteten u. a. Vor- und Nachname, Wohnort, Geburtsdatum, Krankenkasse, Beförderungsziel, Gesundheitsdaten (z. B. Behinderungen). Bei der Anmeldung für einen Erste-Hilfe-Kurs gaben die betroffenen Personen ihren Namen, Vornamen, Geburtsdatum, Anschrift, Telefon bzw. E-Mail-Adresse selbstständig in entsprechende Textfelder auf der Webseite ein.

Die auf einem Content Management System basierende Webseite des Verbandes war aufgrund einer technischen Schwachstelle über mehrere Tage angreifbar. Dies führte dazu, dass sie auch tatsächlich kompromittiert wurde. Durch eine sogenannte SQL-Injection konnten unwirksam geschützte Datenbankinhalte ausgelesen und ggf. verändert werden. Zum Zeitpunkt des Angriffs befanden sich in den Datenbanken zu den Fahrdiensten und Erste-Hilfe-Kursen ca. 89.000 Datensätze, die teilweise Rückschlüsse auf den Gesundheitszustand der betroffenen Personen zuließen. Der Hacker griff

unbefugt auf diese Daten zu und machte sie (zumindest teilweise) mehreren Vertreterinnen und Vertretern der Presse zugänglich, die im Anschluss über den Vorfall berichteten.

Während unserer Ermittlungen stellte sich heraus, dass zwischen dem Verband und dem externen IT-Dienstleister kein Auftragsverarbeitungsvertrag gemäß Artikel 28 DS-GVO bestand, obwohl dies nach der Art und Weise der Beauftragung des Dienstleisters erforderlich gewesen wäre. Insbesondere ergaben sich aus dem Dienstleistungsvertrag keine durch den Auftragnehmer zu ergreifenden technischen und organisatorischen Maßnahmen in Bezug auf die verarbeiteten personenbezogenen Daten auf der Webseite des Verbandes. Das hatte zur Folge, dass allein der Verband für die technische Pflege und die Sicherheit der genutzten Software zuständig war.

Artikel 32 Absatz 1 DS-GVO verlangt von jedem Verantwortlichen und ggf. seinen Auftragsverarbeitern die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu erreichen. Bei der Auswahl der Maßnahmen sind nach den genannten Vorschriften der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Buchstabe d der Vorschrift verlangt, die technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen und ihre Wirksamkeit zu evaluieren. Im konkreten Fall hätte dies bedeutet, den Webauftritt auf bekannte Sicherheitslücken zu untersuchen und solche Tests in angemessenen zeitlichen Abständen zu wiederholen. Insbesondere bei der Verarbeitung personenbezogener Daten in großer Anzahl und mit hoher Sensitivität wäre dies geboten gewesen. Dieser Pflicht kam der Verband jedoch nicht nach, wodurch der Angriff erfolgreich war.

Vergessene Server bergen Risiken

Der Verband betrieb zudem eine zweite Internetpräsenz, über die ein Duplikat der Original-Webseite erreichbar war. Auch dort existierte die oben genannte Sicherheits-

lücke. Trotz entsprechender Kenntnis ergriff der Verband keine technischen und organisatorischen Abhilfemaßnahmen zur Vermeidung des Risikos weiterer Angriffe. Es dauerte ca. drei Monate, bis die Lücke dort beseitigt wurde.

Für die begangenen Verstöße setzten wir insgesamt eine Geldbuße im fünfstelligen Bereich fest. Hierbei wurde erschwerend berücksichtigt, dass aufgrund der in vielen Fällen eindeutigen Identifizierbarkeit der betroffenen Personen ein erhebliches Risiko bestand, die Erkenntnisse rufschädigend oder zum Zweck des Identitätsdiebstahls verwenden zu können. Der Verband akzeptierte das Bußgeld.

III Anlasslose Prüfungen

1 Prüfung von Autohäusern: Defizite bei Nachweispflichten und Umgang mit Kundendaten

Im Rahmen unserer Aufsichts- und Kontrolltätigkeit stellen wir bei Unternehmen immer wieder ähnliche datenschutzrechtliche und technisch-organisatorische Defizite fest. Oft stoßen wir beispielsweise auf Mängel beim Umfang der verarbeiteten personenbezogenen Daten, ihrer Speicherung, Aufbewahrung und Vernichtung, bei der Gewährleistung der Betroffenenrechte auf Auskunft oder Löschung, bei der Konzeption und Dokumentation von technischen und organisatorischen Maßnahmen zum Schutz der Daten und ihrer Verarbeitung sowie bei der Erfüllung von Nachweispflichten gegenüber unserer Behörde. Im Berichtszeitraum haben wir deshalb eine anlasslose Prüfung bei Autohäusern begonnen, um deren datenschutzkonforme Verarbeitung personenbezogener Daten zu kontrollieren. Im Fokus der Prüfung standen insbesondere der Umgang mit Unterlagen wie Fahrzeugbriefen, Rechnungen und Personalausweiskopien sowie die Nachweisführung zur Erfüllung der datenschutzrechtlichen Anforderungen.

Das Vorgehen bei dieser Prüfung war zweigeteilt: Im ersten Schritt wurden vor Ort Gespräche mit den Verantwortlichen geführt, aus Kundensicht relevante Unternehmensprozesse erörtert (z. B. Verkauf) sowie stichprobenartig Unterlagen und IT-Systeme eingesehen. Beim zweiten, gegenwärtig noch andauernden Schritt steht die Prüfung von Unterlagen im Mittelpunkt. Beispielsweise ließen wir uns das Verzeichnis der Verarbeitungstätigen, Datenschutzerklärungen, Teilkonzepte zur Gewährleistung der Sicherheit der Datenverarbeitung oder Auftragsverarbeitungsverträge vorlegen.

Innerhalb des ersten Prüfungsteils ergab sich ein recht homogenes Bild. Alle Unternehmen sahen in den Vor-Ort-Gesprächen den Datenschutz als notwendigen und wichtigen, stets zu beachtenden Bestandteil ihrer Prozesse an. Leider wiesen jedoch auch alle Autohäuser in unterschiedlicher Ausprägung die von uns befürchteten oben genannten Defizite auf.

Insbesondere fiel auf, dass die Unternehmen auf eine doppelte Datenhaltung setzten. Dies äußerte sich darin, dass die gleichen personenbezogenen Daten von Kundinnen und Kunden sowohl physisch in Papierform als auch digital gespeichert wurden, letzteres zum Teil in verschiedenen Datenbanken unterschiedlicher IT-Systeme. Nicht nur, dass eine mehrfache Datenhaltung die Einhaltung der Datenschutzgrundsätze der Transparenz, der Datenminimierung und der Richtigkeit nach Artikel 5 Absatz 1 Buchstaben a, c bzw. d Datenschutz-Grundverordnung (DS-GVO) erschweren kann. Auch hat sich gezeigt, dass dadurch die Gefahr besteht, personenbezogene Daten zu lange vorzuhalten, nicht rechtzeitig an allen Speicherorten zu löschen und somit dem Grundsatz der Speicherbegrenzung nach Artikel 5 Absatz 1 Buchstabe e DS-GVO nicht gerecht zu werden.

Als Hauptursachen der zu langen Speicherung von personenbezogenen Daten erwiesen sich die Nutzung der herstellereigenen IT-Systeme sowie Befürchtungen eventueller Maßnahmen der Finanzämter. Keines der Herstellersysteme ermöglichte eine Löschung der personenbezogenen Daten, wenn erst einmal finanzielle Transaktionen vorlagen. Dies ist für den Autohandel grundsätzlich eine besonders schwierige Situation. Einerseits werden sie gedrängt, herstellerspezifische IT-Systeme zu nutzen, andererseits birgt deren Verwendung gegenwärtig die Gefahr möglicher Datenschutzverstöße. Auch außerhalb dieser Systeme stießen wir mehrfach auf personenbezogene Daten von Kundinnen und Kunden, die über die handels- oder steuerrechtliche Aufbewahrungsfrist hinaus aufbewahrt wurden. In unseren Gesprächen zeigte sich deutlich, dass eventuelle Sanktionen durch Finanzbehörden als realistischere Bedrohung angesehen wurden, als die aus datenschutzrechtlichen Verfehlungen resultierenden Maßnahmen durch unsere Behörde.

Ein weiteres Problem war die oftmals ungenaue und unvollständige Konzipierung, Dokumentation und Umsetzung von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung von personenbezogenen Daten gemäß Artikel 32 Absatz 1 DS-GVO. Hieraus können sich im Unternehmen schnell vielfältige Probleme ergeben. So mussten wir zum Beispiel beobachten, dass an Bildschirmen angezeigte personenbezogene Daten nicht hinreichend vor Einblicken Dritter gesichert wurden. Zur Kenntnis

genommen werden konnten etwa ausgefüllte Bildschirmmasken mit Kundenstammdaten, Kopien von Fahrzeugbriefen, Finanzierungsunterlagen oder E-Mails in einer Kfz-Schadenssache, wenn Beschäftigte beim Verlassen ihres Arbeitsplatzes die Monitore lediglich ausgeschaltet, aber nicht gesperrt haben. Das Ausschalten des Monitors schützte letztendlich genauso wenig wie eine nur geschlossene, aber nicht abgeschlossene Tür zu einem abgelegenen und schlecht einsehbaren Arbeitsplatz. Auch bauliche Gegebenheiten führten teilweise zu einer grundlegenden Gefährdung der Sicherheit personenbezogener Daten. Zu nennen sind hier „gläserne Büros“ mit ungünstig platzierten Bildschirmen sowie ungeeignete Lagerstätten für Rechnungen und Kundenakten. So fanden wir beispielsweise Akten in abgelegenen, jedoch für Unbefugte erreichbaren Regalen oder in einem umfunktionierten Überseecontainer, in dem auch Reifen gelagert wurden.

Autohandel mit Luft nach oben

Bei fast jedem Autohandel, der herstellereigene IT-Systeme zur Kundenverwaltung einsetzte, ergaben sich tiefgreifende Fragestellungen zur Datenhoheit, zur Verantwortlichkeit und zum Speicherort der digital gehaltenen Kundendaten. Das erwähnte Löschproblem ist hierbei nur ein Teil der noch offenen Punkte. Die Verantwortlichen konnten uns auf Anhieb nicht beantworten, ob die Hersteller die personenbezogenen Daten eigenmächtig einsehen oder ändern konnten oder wo letztendlich die Daten gespeichert sind. Da zum Teil auch der Begriff „Cloud-Anwendung“ genutzt wurde, machten wir darauf aufmerksam, dass die gesetzlichen Regelungen zur Datenverarbeitung in Drittstaaten stets zu beachten sind.

Ferner hat sich gezeigt, dass manche Verantwortliche Schwierigkeiten mit der Transparenz und Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten hatten. So gab zum Beispiel jedes Autohaus bei Unterzeichnung eines Kaufvertrags auch eine Datenschutzerklärung und ein Abfrageformular zur Nutzung der personenbezogenen Daten aus. Leider stellten wir fest, dass die Dokumente zum Teil verwirrende Darstellungen und unklare Formulierungen, u. a. zur Einwilligung, enthielten. Darüber hinaus hatten wir zu erläutern, dass der Austausch von E-Mails mit einem potentiellen Kunden zu einem

möglichen Fahrzeugkauf noch nicht als tragfähige Rechtsgrundlage für die weitere Verarbeitung der personenbezogenen Daten ausreicht, insbesondere nicht, um besagte Daten für mehrere Jahre im E-Mail-System zu speichern oder Kundenakten anzulegen.

Verwundert haben uns weiter der Umgang mit Dienstleisterinnen und Dienstleistern und die eher nachlässig behandelten grundlegenden Dokumentationspflichten. So konnten wir ermitteln, dass manche Autohäuser Dienste anderer Unternehmen oder Personen für die Zulassung der verkauften Fahrzeuge nutzen. Je nach Ort der Zulassung kann es sein, dass diesen der Personalausweis der Kundschaft überlassen werden muss. Die nach Artikel 28 Absatz 3 DS-GVO zu schließenden Auftragsverarbeitungsverträge existierten jedoch nicht oder wiesen erhebliche Mängel auf. Auch mussten wir feststellen, dass bei einigen Autohäusern keine oder nur unvollständige Verzeichnisse von Verarbeitungstätigkeiten nach Artikel 30 Absatz 1 DS-GVO vorlagen.

Insgesamt hat der erste Teil der Prüfung unsere Erfahrungen zu den üblichen Datenschutzdefiziten in Unternehmen bestätigt. Zu den neuen Problemfeldern gehört insbesondere die Abhängigkeit von den herstellerspezifischen IT-Systemen. Sie ist als kritisch zu bewerten, wenn dort die datenschutzrechtlichen Anforderungen nicht oder nur teilweise umsetzbar sind. Hinsichtlich der technischen und organisatorischen Mängel können deren Auswirkungen beträchtlich sein und letztlich auch das Unternehmen an sich bedrohen. Jeder Verantwortliche ist deshalb gut beraten, nicht nur für die konsequente Umsetzung der erforderlichen Maßnahmen zu sorgen, sondern auch regelmäßig ihre Aktualität und Wirksamkeit zu überprüfen. Der zweite Teil der Prüfung dauert an und wird in Anbetracht der bereits festgestellten Defizite noch einige Zeit in Anspruch nehmen.

2 Prüfung eines Kreditinstituts: Fehlversand von Unterlagen

Seit dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) im Jahr 2018 gelten für Verantwortliche und Auftragsverarbeiter erweiterte Melde-, Informations- und Nachweispflich-

ten bei Verletzungen des Schutzes personenbezogener Daten. Es ist insofern nicht verwunderlich, dass auch Kreditinstitute seitdem vermehrt Datenschutzverletzungen an uns melden. Die Offenlegung der Bankdaten von Kundinnen und Kunden beispielsweise durch postalischen Fehlversand, Nachlässigkeiten bei der Pflege von Stammdaten oder das Übertragen von Geldbeträgen auf falsche Konten sind oftmals Grund für solche Meldungen. Bereits im Jahr 2020 führten wir zu diesem Thema eine Vor-Ort-Kontrolle bei einem Kreditinstitut durch. Im Ergebnis dieser Prüfung stellte das Kreditinstitut interne Prozesse um und ergriff weitere Maßnahmen, sodass letztendlich die Zahl der Datenschutzverletzungen dort merklich zurückging.[8] Durch diesen Erfolg bestätigt, planten wir eine weitere Vor-Ort-Kontrolle bei einem anderen Kreditinstitut, von dem wir gehäuft entsprechende Meldungen erhielten. Die pandemische Lage 2021 führte jedoch dazu, dass der Plan aufgeschoben werden musste und wir die beabsichtigte Kontrolle erst in diesem Berichtszeitraum durchführen konnten.

Zunächst erörterten wir mit dem Kreditinstitut grundlegende Modalitäten zu Meldungen von Datenschutzverletzungen. Aus Artikel 33 DS-GVO ergibt sich, dass Verantwortliche solche Meldungen innerhalb von 72 Stunden, nachdem sie von der Verletzung Kenntnis haben, bei der zuständigen Aufsichtsbehörde einreichen müssen. Im vorliegenden Fall beabsichtigte das Unternehmen wegen der Vielzahl von Datenschutzverletzungen, diese gebündelt an uns zu melden. Schon allein aus Gründen der Fristwahrung konnten wir uns damit jedoch nicht einverstanden erklären. Darüber hinaus wäre es für uns durch ein solches Vorgehen erschwert, die Maßnahmen zur Minderung möglicher Risiken für betroffene Personen zu bewerten, zu ergänzen oder zu ändern.

Eine weitere Frage war, welche Datenschutzverletzungen tatsächlich meldepflichtig sind. Hierzu sieht die Datenschutz-Grundverordnung vor, dass bei Sicherheitsvorfällen, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führen, grundsätzlich eine Meldung erfolgen muss. Ausnahmen bestehen lediglich, wenn die Verletzung des Schutzes personenbezogener Daten

8 Tätigkeitsbericht Datenschutz 2020, A III 2.

voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Allerdings müssen auch in diesem zuletzt genannten Fall Datenschutzverletzungen durch den Verantwortlichen intern dokumentiert werden. Für die Praxis empfehlen wir, im Zweifel lieber eine Datenpanne zu viel an uns melden als eine zu wenig. Dies ergibt sich auch daraus, dass eine Bewertung des voraussichtlichen Risikos für betroffene Personen oftmals schwierig und innerhalb der genannten 72 Stunden nicht in jedem Fall abschließend ist. Der (für uns) positive Effekt dieser Empfehlung ist, dass wir auch das kumulative Risiko für die Rechte und Freiheiten betroffener Personen berücksichtigen und systematisch verursachte Häufungen von Datenschutzverletzungen identifizieren können – etwa beim Fehlversand von Unterlagen.

Bei der diesjährigen Kontrolle konnten wir feststellen, dass das betreffende Kreditinstitut bereits zahlreiche effektive Maßnahmen umgesetzt hatte. Beispielsweise ist eine typische Ursache für Datenschutzverletzungen beim Postversand von Schreiben, dass händisch falsche Anlagen zu Anschreiben hinzusortiert werden. Das Kreditinstitut hatte diesen Prozess bereits weitestgehend automatisiert und damit menschliche Fehlerquellen reduziert. Die Ausnahmen, in denen Anlagen manuell hinzugefügt werden müssen, sollen hier künftig noch weiter eingeschränkt werden. Neben dieser Änderung gewährte die Vor-Ort-Kontrolle auch tiefere Einblicke in die internen Prozesse, wodurch es uns möglich wird, zukünftig einfacher weitere geeignete und wirksame Maßnahmen zu empfehlen.

In Bezug auf das kontrollierte Unternehmen ist auch anzuerkennen, dass dort durchschnittlich mehrere tausend Postsendungen pro Tag verschickt werden und damit die Quote der Fehlsendungen insgesamt gering war (im Gegensatz zu ihrer absoluten Zahl). Hinzu kommen zwei weitere Besonderheiten dieses Kreditinstituts: Zum einen hat die typische Kundschaft zu diesem Institut vergleichsweise selten Kontakt. Das kann dazu führen, dass etwa beim Wechsel einer Wohnanschrift oder beim Auflösen einer Ehegemeinschaft die entsprechende Mitteilung gegenüber dem Kreditinstitut vergessen wird. In einigen dieser Fälle resultiert daraus eine meldepflichtige Datenschutzverletzung. Zum anderen werden Aufträge zu Auszahlungen von Kundinnen oder Kunden oftmals über kooperierende Drittins-

titute aufgegeben. Wird hierbei unbemerkt etwa eine falsche IBAN für das Zielkonto angegeben, kommt es zu einer Fehlüberweisung. Das Kreditinstitut kann diese Panne nur feststellen, wenn die betroffenen Kundinnen oder Kunden bzw. die falschen Empfängerinnen oder Empfänger sich bei ihm melden. Mit solchen Fällen verbundene Fragen des Zusammenwirkens der kooperierenden Kreditinstitute und der datenschutzrechtlichen Verantwortlichkeit sollen zukünftig noch genauer erörtert werden.

Auch wenn bei dem kontrollierten Unternehmen vorerst nur kleinere Nachbesserungen erreicht wurden und sich gezeigt hat, dass einige Fehlerquellen außerhalb seines Verantwortungsbereichs lagen, hilft uns die Prüfung, die aufgetretenen Datenschutzverletzungen und ihre Ursachen besser zu verstehen und einordnen zu können. Außerdem zeigt sich besonders in diesen Fällen, wie wichtig es ist, dass aufmerksame Kundinnen und Kunden dem Verantwortlichen Datenschutzverletzungen mitteilen, damit diese überhaupt bemerkt werden und entsprechende Maßnahmen zur Verbesserung des Datenschutzniveaus abgeleitet werden können.

3 Prüfung von Meldeportalen zur einrichtungsbezogenen Impfpflicht

Ein vielbeachtetes Thema im Berichtsjahr war die einrichtungsbezogene Impfpflicht im Kontext der Corona-Pandemie. Beschäftigte von medizinischen oder pflegerischen Einrichtungen oder Unternehmen mussten gemäß § 20a Infektionsschutzgesetz bis zum 15. März 2022 ihren jeweiligen Leitungen einen Nachweis über eine vollständige Impfung, einen Genesenennachweis oder ein ärztliches Attest, dass sie nicht geimpft werden können, vorlegen. Die Leitungen wiederum hatten anschließend das zuständige Gesundheitsamt zu informieren, wenn die Nachweise nicht fristgerecht vorgelegt wurden oder Zweifel an der Echtheit oder Richtigkeit der vorgelegten Nachweise bestanden. Hierbei waren die entsprechenden personenbezogenen Daten der Beschäftigten zu übermitteln.

Im Rahmen der Umsetzung der gesetzlichen Anforderungen stellte sich für Unternehmen und Einrichtungen der Gesundheits- bzw.

Pflegebranche die Frage, wie die datenschutzkonforme Übermittlung der personenbezogenen Daten erfolgen sollte. Um den zuständigen kommunalen Gesundheitsämtern im Land Brandenburg eine Hilfestellung zu geben, stellte das Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz im Sinne des „Einer für Alle"-Prinzips ein Softwarepaket bereit, das die Grundlage für die digitalen Meldeportale der einzelnen Gesundheitsämter bildete. Es war in die jeweilige lokale IT-Infrastruktur zu integrieren und erlaubte den Unternehmen bzw. Einrichtungen, die erforderlichen personenbezogenen Daten unkompliziert zu übermitteln. Somit wurde eine möglichst einheitliche Lösung angestrebt, die auch von fast allen Landkreisen und kreisfreien Städten erfolgreich eingesetzt wurde.

Die für uns in diesem Zusammenhang wichtigen Fragen bezogen sich auf die datenschutzrechtliche Verantwortlichkeit, den Umfang der an die Gesundheitsämter zu übermittelnden Daten sowie die konkrete technische Umsetzung der Verschlüsselung bei der Datenübertragung.

Die ersten beiden Fragen konnten schnell geklärt werden: Die Meldeportale waren technisch betrachtet „digitale Briefkästen". Die von den Unternehmen und Einrichtungen zu erhebenden und zu übermittelnden Daten ihrer Beschäftigten wurden in eine im Browser geöffnete Webseite eingetragen bzw. über das Portal als Datei hochgeladen und dann direkt an die Gesundheitsämter übertragen. Dort wurden die Daten anschließend in eigener Verantwortung weiterverarbeitet. Wir konnten uns auch davon überzeugen, dass nur die tatsächlich erforderlichen personenbezogenen Daten abgefragt und das Prinzip der Datenminimierung somit beachtet wurde.

Um die Frage der sicheren und verschlüsselten Übertragung beantworten zu können, haben wir im Rahmen unserer Aufsichtstätigkeit insgesamt 17 digitale Meldeportale der Gesundheitsämter in den Landkreisen und kreisfreien Städten technisch überprüft. Dabei haben wir lediglich kleine Mängel festgestellt, welche aus unserer Sicht kein akutes Eingreifen erforderten. Auf eine weitergehende Prüfung und insbesondere die Vorlage von Unterlagen haben wir zur Entlastung der ohnehin durch die Pandemie stark beanspruchten Gesundheitsämter verzichtet.

Bei den technischen Prüfungen beobachteten wir zum einen, dass einige der implementierten Meldeportale die Verschlüsselungsprotokolle TLS 1.0 und TLS 1.1 unterstützten. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt grundsätzlich nur die Verwendung von TLS 1.2 und TLS 1.3 für die sichere Übertragung von Informationen über das Internet. Die Nutzung der mittlerweile veralteten Protokolle TLS 1.0 und TLS 1.1 könnte es potenziellen Angreiferinnen und Angreifern ermöglichen, unberechtigten Zugriff auf personenbezogene Daten zu erlangen. Des Weiteren ist uns aufgefallen, dass mehrere Portale sogenannte Wildcard-Zertifikate für die Authentifizierung der Server einsetzten. Dies sind Zertifikate, bei denen im relevanten Namensfeld der Platzhalter „*“ (Wildcard Character) für einen konkreten Server eingetragen ist. Auch hierdurch können personenbezogene Daten in falsche Hände gelangen, da sich auf Clientseite nicht feststellen lässt, ob der Zielserver tatsächlich authentisch ist und Daten entgegennehmen darf. Für die Übertragung von Daten, deren Missbrauch hohe Risiken verursachen kann, wird von der Verwendung von Wildcard-Zertifikaten abgeraten.

Und letztlich ist uns im Zusammenhang mit der Registrierung als Unternehmen oder Einrichtung der Gesundheits- bzw. Pflegebranche am Meldeportal aufgefallen, dass oftmals keine Plausibilitätsprüfung durch das jeweilige Gesundheitsamt erfolgte. So konnten wir uns beispielsweise bei mehreren digitalen Meldeportalen als „ortsfremde“ Einrichtung registrieren. Wir halten an dieser Stelle zumindest eine Überprüfung der Postanschrift für angebracht, da die unrechtmäßige Registrierung durch potenzielle Angreiferinnen und Angreifer z. B. die Gefahr einer Denunziation oder der gezielten „Überschwemmung“ des Gesundheitsamtes mit fehlerhaften Daten birgt.

Die Ergebnisse unserer Prüfung haben wir den Gesundheitsämtern und dem Ministerium schriftlich mitgeteilt. Wir machten dabei deutlich, dass wir von einer zeitnahen Abstellung der beschriebenen Mängel ausgingen. Die gesetzlichen Regelungen zur einrichtungsbezogenen Impfpflicht selbst traten zum Ende des Berichtszeitraums wieder außer Kraft.

4 Prüfung von Sozialbehörden im Rahmen der Leistungsgewährung nach dem Asylbewerberleistungsgesetz

In unserem letzten Tätigkeitsbericht[9] berichteten wir über den Beginn einer anlasslosen datenschutzrechtlichen Prüfung in drei ausgewählten Sozialbehörden bezüglich ihrer Aufgabenwahrnehmung nach dem Asylbewerberleistungsgesetz. Hierzu hatten wir zum einen stichprobenartig Leistungsakten von den Behörden angefordert und die datenschutzgerechte Aktenführung kontrolliert. Zum anderen entwickelten wir einen umfangreichen Fragenkatalog, der neben rechtlichen insbesondere Fragen zur Umsetzung von technischen und organisatorischen Maßnahmen enthielt. Ziel war es, uns anhand der Antworten und ergänzend angeforderter Unterlagen zunächst einen möglichst breit gefächerten Überblick über die bereits etablierten Maßnahmen zu verschaffen, bevor technisch-organisatorische Detailfragen geprüft werden sollten. Zu den Dokumenten, um deren Zusendung wir die Behörden gebeten hatten, gehörten neben dem relevanten Ausschnitt aus dem Verzeichnis der Verarbeitungstätigkeiten das Kryptokonzept, das Berechtigungskonzept, das Löschkonzept sowie interne Vorgaben zur Erfüllung der Anforderungen von Artikel 33 Datenschutz-Grundverordnung (DS-GVO) bei Datenschutzverletzungen.

Die stichprobenartige Prüfung der Aktenführung konnte bereits abgeschlossen werden. Hinsichtlich der technisch-organisatorischen Aspekte dauert die Auswertung der Rückläufe aus den Sozialbehörden an. Unseren ursprünglichen Plan, lediglich hervorstechende Mängel zu thematisieren und zu diesen Hinweise und Empfehlungen für die Verbesserung des technisch-organisatorischen Datenschutzniveaus zu geben, mussten wir verwerfen. Gründe hierfür waren die stark schwankende Qualität sowie der unterschiedliche und schwer vergleichbare Umfang der Antworten. Auch haben die Behörden uns nicht in jedem Fall die erbetenen Dokumente übermittelt oder auf Unterlagen verwiesen, die sie nicht übersandt hatten. Anstatt einer vergleichenden Auswertung nach einheitlichen Kriterien mussten wir in jedem Einzelfall individuelle Versäumnisse bzw. Mängel bei

9 Tätigkeitsbericht Datenschutz 2021, A III 4.

den untersuchten Sozialbehörden identifizieren und bewerten. Einige grundlegend problematische Ergebnisse sind nachfolgend zusammengefasst:

Bei zwei der drei Sozialbehörden mussten wir essenzielle Mängel hinsichtlich des uns zugesandten Ausschnitts aus dem Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DS-GVO feststellen. So waren etwa Verarbeitungsvorgänge nicht ausreichend granular dargestellt, wodurch bereits die konkrete Zuordnung und Bewertung der Eignung von technischen und organisatorischen Datenschutzmaßnahmen wesentlich erschwert oder gar unmöglich wird. Weiter wurden anstelle von Verarbeitungstätigkeiten lediglich knappe Beschreibungen der behördlichen Aufgaben wiedergegeben oder Rechtsgrundlagen für die Datenverarbeitung falsch bzw. lediglich pauschal und ohne Angabe der konkreten Norm benannt. Hinsichtlich der in den Dokumenten aufgeführten technischen und organisatorischen Maßnahmen waren im besten Fall verallgemeinernde, abstrakte Aussagen (wie z. B. „Verschlüsselung“) zu finden. Falls von dort auf weiterführende Fundstellen für detaillierte Konzepte verwiesen wurde, enthielten diese jedoch oftmals keine oder keine ausreichenden Beschreibungen der konkreten Umsetzung bei der jeweiligen Verarbeitungstätigkeit.

Einhaltung des Datenschutzes ist nachzuweisen

Auch hinsichtlich unserer Fragen, die darauf abzielten, die Vertraulichkeit und Integrität der Datenverarbeitung zu bewerten, zeichnete sich ein durchwachsenes Bild. So wurden Berechtigungskonzepte in zwei von drei Fällen nicht übermittelt. Keine der drei Sozialbehörden legte ein Kryptokonzept vor. Zwar ließ sich aus dem Kontext der anderen übermittelten Dokumente schließen, dass in beiden Bereichen Maßnahmen ergriffen wurden, eine systematische und ausreichend vollständige sowie durch uns prüfbare Dokumentation gab es jedoch nicht. Insofern konnten wir auch keine abschließende Bewertung vornehmen.

Darüber hinaus war auffällig, dass bei keiner der geprüften Sozialbehörden eine vollwertige Dokumentensteuerung existierte. Eine solche ist jedoch Voraussetzung für den Nachweis der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der tech-

nischen und organisatorischen Maßnahmen. Dies wird in Artikel 32 Absatz 1 Buchstabe d DS-GVO gefordert.

Positiv fiel uns bei zwei der drei Sozialbehörden auf, dass sie Beschreibungen der Melde- und Informationsprozesse nach Artikel 33 DS-GVO für Verletzungen des Datenschutzes eingereicht hatten. Diese entsprachen vollumfänglich den Anforderungen der Datenschutz-Grundverordnung. Die dritte Behörde machte hierzu keine Angaben.

Aktuell stellen wir die Rückmeldungen für die Sozialbehörden zusammen und prüfen, welche Maßnahmen, Vorgehensweisen und Priorisierungen wir ihnen empfehlen, um die Wahrung des Datenschutzes nachhaltig zu verbessern.

IV Ausgewählte Fälle

1 Online-Babygalerie eines Krankenhauses

Ein Krankenhaus hatte von Mitte 2021 bis Ende April 2022 die Fotos und Namen sowie Geburtsdatum, -gewicht und -größe der dort geborenen Kinder sowie teilweise die Namen der Eltern im Internet veröffentlicht. In einer Online-Babygalerie waren sie für jedermann zugänglich.

Wir baten um nähere Informationen insbesondere zu einer Einwilligung der Sorgeberechtigten. Es stellte sich heraus, dass das Krankenhaus mit einem sächsischen Unternehmen zusammenarbeitete, welches die Fotos fertigte, Einverständniserklärungen für die Übermittlungen an das Klinikum, aber auch für die Veröffentlichungen auf dessen Website, an der Fotowand im Krankenhaus oder in einer lokalen Zeitung einholte und diese Formulare archivierte. Als Pflichtfelder für den Fall, dass eine Veröffentlichung eines Babyfotos durch das Krankenhaus vorgesehen war, wurden von der Firma Bild, Vorname, Geschlecht und Geburtstag des Kindes genannt, optional waren Nachname, Geburtszeit, -gewicht und -größe. Trotzdem wurden vielfach auch die Namen der Eltern veröffentlicht, die vermutlich lediglich für die Veröffentlichung in der Tageszeitung angegeben wurden.

Es erschien uns wesentlich, die Einwilligungserklärungen für das Unternehmen, welches sich grundsätzlich als eigenständigen datenschutzrechtlich Verantwortlichen betrachtete, von jenen für die Klinik zu trennen und die Zwecke der Datenverarbeitung sowie die jeweils dafür vorgesehenen Angaben transparent zu machen. Auch regten wir an, dass die Klinik die sie betreffenden Einwilligungserklärungen selbst aufbewahrt. Wir äußerten außerdem Bedenken gegen die Auffassung des Unternehmens, dass für die weltweite Veröffentlichung in der Online-Babygalerie die Erklärung eines Elternteils genügen sollte. Seiner Bewertung, dass es sich bei den veröffentlichten Daten nicht um Gesundheitsdaten handele, widersprachen wir ebenfalls: Durch die Veröffentlichung der Bilder und zusätzlichen Angaben wird der Aufenthalt im Krankenhaus zu Geburtszwecken offenbart. Bereits dies ist datenschutzrechtlich als Gesundheitsdatum zu werten.

Das Krankenhaus hat unsere Kritik und unsere Empfehlungen umgehend aufgegriffen. Die Angaben in der Babygalerie wurden auf Bild, Vornamen und Geburtsdatum der Neugeborenen reduziert. Dazu wurde eine eigene Einverständniserklärung entwickelt.

2 Datenschutzbeauftragte auf Zuruf?

Der Fehlversand von Dokumenten, ob digital oder analog, stellt immer noch den häufigsten Fall der Verletzung des Schutzes personenbezogener Daten dar. Dies spiegelt sich in den Meldungen zu Datenschutzverletzungen gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) wider, die wir auch im Berichtsjahr zahlreich erhielten.[10] Die Vorfälle sind aus unserer Sicht sehr ärgerlich, da sie leicht vermeidbar wären. Meist ließen sie sich schon durch eine regelmäßige Sensibilisierung der Beschäftigten und die simple Anwendung des Vier-Augen-Prinzips verhindern.

In einem konkreten Fall wurden wir von einer Arztpraxis darüber informiert, dass sie Unterlagen mit personenbezogenen Daten mehrerer Patientinnen und Patienten an eine falsche Adressatin versandt hatte. Auch bei der falschen Adressatin handelte es sich um eine Patientin der Praxis. Das Ungewöhnliche an diesem Fall war der Umstand, dass die Empfängerin beruflich als Datenschützerin tätig war. Sie informierte die Praxis über die Datenschutzverletzung und empfahl eine entsprechende Meldung gemäß Artikel 33 DS-GVO an unsere Behörde. Darüber hinaus bot sie sich sogleich als externe Datenschutzbeauftrage an, da die Praxis bislang keine solche benannt hatte.

Auf den ersten Blick hatte die Arztpraxis in diesem Fall doppeltes Glück im Unglück. Zum einen sind für die abschließende Bewertung der Datenschutzverletzung u. a. das voraussichtliche Risiko und die möglichen Folgen für die Rechte und Freiheiten der betroffenen Personen ein wichtiger Baustein. Da die Offenbarung der personenbezogenen Daten gegenüber einer beruflich im Datenschutzbereich tätigen Person (der neuen externen Datenschutzbeauftragten) stattfand, konnte ein voraussichtlich hohes Risiko hier verneint werden.

10 Siehe A VI 4.

Zum anderen sind bei der Bewertung die von dem Verantwortlichen, in unserem Fall der Arztpraxis, bereits ergriffenen oder geplanten Maßnahmen zur Verhinderung, Behebung und Abmilderung der Datenschutzverletzung zu berücksichtigen. Die neue Datenschutzbeauftragte benannte uns gegenüber sofort geeignete Maßnahmen und stellte eine grundlegende Aufarbeitung datenschutzrechtlicher und -technischer Versäumnisse in Aussicht.

Leider zeigt die Erfahrung, dass viele Arztpraxen das Thema Datenschutz noch recht nachlässig behandeln und sich ihrer datenschutzrechtlichen Verpflichtungen meist nicht hinreichend bewusst sind. Praxen gehen im Alltag mit vielen personenbezogenen Daten besonderer Kategorien gemäß Artikel 9 Absatz 1 DS-GVO um (Gesundheitsdaten). Sie unterliegen deshalb nach Artikel 30 Absatz 5 DS-GVO der gesetzlichen Anforderung, ein Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 Absatz 1 DS-GVO zu führen. Weiterhin müssen Patientinnen und Patienten gemäß Artikel 13 DS-GVO bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten gegeben oder das Recht auf Auskunft nach Artikel 15 DS-GVO, das Recht auf Löschung nach Artikel 17 DS-GVO sowie weitere Betroffenenrechte gewährleistet werden. Darüber hinaus ist jede Arztpraxis als datenschutzrechtlich Verantwortlicher i. S. d. Artikel 4 Nummer 7 DS-GVO verpflichtet, geeignete und wirksame technische und organisatorische Maßnahmen nach Artikel 24 und 32 DS-GVO zu ergreifen, um einen angemessenen Schutz der personenbezogenen Daten bei der Verarbeitung zu gewährleisten. Dies beinhaltet u. a. den Einsatz aktueller Betriebssysteme sowie Virenschutzprogramme, die Absicherung des Zugangs zu Rechentechnik durch eine geeignete Authentisierung, die regelmäßige Erstellung von Sicherungskopien der Daten (Backup), eine verschlüsselte Übermittlung von Gesundheitsdaten (bspw. Befunden) per E-Mail und ein Konzept zum Umgang mit Datenschutzvorfällen. Dies sind zeitaufwendige, aber zwingend notwendige Vorkehrungen. Eine Unterstützung durch eine fachlich versierte Person in der Rolle des bzw. der Datenschutzbeauftragten kann dabei durchaus hilfreich sein.

In unserem konkreten Fall hatte die neue Datenschutzbeauftragte die Umsetzung all dieser Themen angestrebt. Wenig später erhielten

wir jedoch die Nachricht, dass die externe Datenschutzbeauftragte nicht mehr für die Praxis tätig ist. Die Bearbeitung des Vorgangs dauert daher an.

3 Ausweiskopien im Corona-Testzentrum

Zur Durchführung von Corona-Tests werden Namen, Geburtsdatum und Anschrift der getesteten Personen benötigt. Durch eine Beschwerde wurden wir darauf aufmerksam, dass in einem Testzentrum zur Vereinfachung eine Kopie der Rückseite des Personalausweises zu den Unterlagen genommen wurde, statt die Wohnanschrift direkt in das Formular einzutragen. Durch das Kopieren wurden zusätzliche, nicht erforderliche Angaben wie die Augenfarbe und die Größe, aber auch die Nummer des Dokuments und die ausstellende Behörde erfasst und danach weiterverarbeitet.

Eine Ausweiskopie darf nach § 20 Absatz 2 Personalausweisgesetz nur mit Zustimmung der Ausweisinhaberin bzw. des Ausweisinhabers erstellt werden; ihre Verarbeitung darf nur mit ihrer bzw. seiner Einwilligung erfolgen. Da Testwillige im betroffenen Testzentrum die Wahl hatten, ihre Identitätsdaten handschriftlich anzugeben oder den Ausweis kopieren zu lassen, war die Freiwilligkeit der Kopie letztlich kein Problem.

Hinsichtlich des Umfangs der kopierten Daten versuchten wir, darauf hinzuwirken, mithilfe einer Schablone die nicht erforderlichen Angaben abzudecken. Das Testzentrum trug hierzu vor, dass teilweise noch ältere Personalausweise mit einem etwas anderen Format zum Einsatz kommen. Darüber hinaus würden häufig ausländische Ausweispapiere vorgelegt, die wiederum etwas anders gestaltet seien. Setze man aber verschiedene Schablonen ein, so bringe dies wegen der Verwechslungsgefahr ein erhöhtes Fehlerrisiko, Doppelarbeit und Verzögerungen im Ablauf mit sich. Dies würde allen Beteiligten insbesondere in Stoßzeiten viel Geduld und Zeit abverlangen. Aufgrund der dargestellten Situation empfahlen wir dem Testzentrum dringend, für eine gesondert anzukreuzende Einwilligung zu sorgen, in der deutlich wird, dass die gesamte Rückseite des Ausweispapiers kopiert und weiterverarbeitet werden darf.

Im Rahmen einer zusätzlichen Beratung des Testzentrums konnten wir weitere inhaltliche Verbesserungen insbesondere im Zusammenhang mit der Datenschutzerklärung erreichen. Dem Verantwortlichen legten wir dabei nahe, auf die schriftliche Bestätigung der Kenntnisnahme der Datenschutzerklärung zu verzichten und lediglich auf diese Information hinzuweisen.

Der Verantwortliche stellte sich unserer Kritik und nahm die Anregungen auf.

4 Mitgliederdaten eines Anglervereins frei verfügbar

Im Berichtszeitraum erhielten wir einen anonymen Hinweis, dass eine Vielzahl personenbezogener Daten von Mitgliedern eines Anglervereins ohne Zugriffsbeschränkungen im Internet abrufbar sei. Die den Hinweis gebende Person hatte im Internet nach einem Freund gesucht und daher dessen Namen und Wohnort in einer Suchmaschine eingegeben. Einige der aufgelisteten Treffer verwiesen auf die Webseiten eines Anglervereins. Beim Anklicken dieser Links konnten ohne weitere Zugangsbeschränkungen Excel-Dateien des Vereins aus den Jahren 2018 und 2019 heruntergeladen und geöffnet werden. In den Tabellen waren nicht nur die vollständigen Namen und Anschriften, Mitglieds- und Fischereischeinnummern, Telefonnummern, E-Mail-Adressen und Geburtsdaten der etwa 100 Mitglieder des Anglervereins offen einsehbar, sondern auch die jeweiligen Kontoverbindungsdaten sowie getätigte Überweisungen vermerkt. Auch personenbezogene Daten von Kindern wie vollständiger Name, Geburtsdatum und Anschrift waren für jedermann sichtbar.

Daten in Kescher und Reuse

Eine Überprüfung des geschilderten Sachverhaltes durch uns bestätigte die Datenschutzverletzung. Zudem mussten wir feststellen, dass die fraglichen Dateien ebenso auf der Webseite des Anglervereins direkt hätten gefunden werden können. Auch in diesem Fall war das Herunterladen und Öffnen der entsprechenden Tabellen ohne

Eingabe eines Passwortes oder eine andere Beschränkung des Zugriffs möglich.

Wir informierten den verantwortlichen Anglerverein über den Vorfall, der daraufhin die Webseite sofort vom Netz nahm. Des Weiteren wiesen wir ihn darauf hin, dass er uns als zuständiger Behörde die Datenschutzverletzung gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) zu melden hatte. Auch wenn wir von dem Vorfall an sich bereits wussten, interessierten uns die Maßnahmen zur Behebung der Datenschutzverletzung sowie zur Abmilderung möglicher nachteiliger Auswirkungen für die betroffenen Personen. Diese Angaben müssen nach den gesetzlichen Bestimmungen Teil der Meldung sein. Auch machten wir den Verein auf seine Informationspflichten nach Artikel 34 DS-GVO aufmerksam. Danach hat er die betroffenen Personen über die Verletzung des Schutzes ihrer personenbezogenen Daten zu unterrichten, falls die Verletzung ein hohes Risiko für ihre persönlichen Rechte und Freiheiten zur Folge hat.

Der Verantwortliche kam seinen Mitteilungspflichten nach. Wie es zu dem Vorfall gekommen war, konnte er allerdings nicht mehr genau aufklären. Ein ehemaliges Vorstandsmitglied soll die besagten Dateien zwischen 2018 und 2020 auf die Webseite hochgeladen haben. Der derzeitige Vorstandsvorsitzende versicherte, eine neue Internetpräsenz aufzubauen, auf der zukünftig keinerlei Mitgliederdaten abrufbar sein sollen. Weiterhin wurden alle noch aktiven Mitglieder des Vereins über die Datenschutzverletzung informiert; eine Unterrichtung der ehemaligen Mitglieder war vorgesehen.

Aus unserer Sicht war die Datenschutzverletzung schwerwiegend, da zum einen eine Vielzahl von Kontoverbindungsdaten der Vereinsmitglieder offengelegt wurde. Hieraus können möglicherweise finanzielle Verluste oder andere wirtschaftliche Nachteile entstehen. Die sonstigen frei zugänglichen Daten eigneten sich für einen Identitätsdiebstahl, also die missbräuchliche Nutzung von Daten der betroffenen Personen durch Dritte. Zum anderen barg die Veröffentlichung der personenbezogenen Daten von Kindern wie deren Namen, Anschrift und Geburtsdatum erhebliche Risiken. Die Daten von Minderjährigen stehen gemäß Artikel 8 sowie Erwägungsgrund 38

und 75 der DS-GVO unter einem besonderen Schutz. Darüber hinaus ist zu beachten, dass im Internet frei zugängliche Daten auch nachdem die entsprechenden Seiten vom Netz genommen wurden ggf. weiter beispielsweise in Webarchiven aufzufinden sein oder von Dritten verbreitet werden können.

Wir werden die Einleitung von Sanktionsmaßnahmen gegen den Verein prüfen, da er die grundlegenden Anforderungen von Artikel 32 DS-GVO nicht beachtet hatte. Absatz 1 der Vorschrift verlangt, dass geeignete technische und organisatorische Maßnahmen nach dem Stand der Technik zu treffen sind, um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten. Nach Absatz 2 der Vorschrift sind bei der Beurteilung des angemessenen Schutzniveaus insbesondere solche Risiken zu berücksichtigen, die durch den unbefugten Zugang zu personenbezogenen Daten entstehen können. Maßnahmen zur Verhinderung eines solchen unbefugten Zugangs sind seit vielen Jahren auf allen gängigen Internetplattformen verfügbar und mit begrenztem Aufwand leicht umsetzbar.

5 Fischereiaufsicht mit privaten Smartphones?

Im Berichtszeitraum erreichten uns mehrere Beschwerden von Freizeitanglerinnen und -anglern, die an brandenburgischen Gewässern kontrolliert wurden. Sie mussten jeweils ihren Angelschein sowie ihren Personalausweis vorlegen. Die Papiere wurden von den Fischereiaufseherinnen und Fischereiaufsehern eingesehen und mit privaten Smartphones fotografiert. Im Anschluss händigten sie den geprüften Personen einen Kontrollbericht aus. In diesem waren Ort und Zeit vermerkt und die Personalausweisnummer handschriftlich festgehalten. Auch die Dienstnummer der Fischereiaufseherin bzw. des Fischereiaufsehers war eingetragen. In mindestens einem Fall ging aus dem Kontrollbericht nicht hervor, wer genau oder zumindest welche Behörde verantwortlich ist, an wen sich die Betroffenen also wenden könnten. Die ehrenamtlich tätigen Fischereiaufseherinnen und Fischereiaufseher waren von der unteren Fischereibehörde bestellt und amtlich verpflichtet worden.

Wenn Angelnde kontrolliert werden

Zur Sachverhaltsaufklärung wandten wir uns zunächst an die zuständigen Landkreise als untere Fischereibehörden. Wir wollten u. a. wissen, ob die Fischereiaufseherinnen und Fischereiaufseher bei ihren Kontrollen tatsächlich ihre privaten Smartphones nutzten und wenn ja, auf welcher Grundlage dies geschah. Wir fragten außerdem danach, wie die unteren Fischereibehörden sicherstellen, dass die von den Ausweisen und Angelscheinen angefertigten Fotos nur von den zuständigen Stellen verarbeitet werden. Ein Personalausweis enthält neben dem Namen, dem Geburtsdatum und der Anschrift der kontrollierten Person auch deren Lichtbild sowie eine Seriennummer, die nur in wenigen Fällen überhaupt verarbeitet werden darf.

Durch die Antwort einer unteren Fischereibehörde wurden wir darauf aufmerksam, dass die Verwendung von privaten Smartphones bei Fischereikontrollen gängige Praxis ist. Der Landkreis verwies auf das Ministerium für Landwirtschaft, Umwelt und Klimaschutz als oberste Fischereibehörde und stützte sich auf einen Leitfaden „Digitale Fischereiabgabe“, in dem die Verwendung eigener Smartphones für Kontrollen vorgesehen ist.

Dies war Anlass für uns, an das Ministerium heranzutreten, unsere erste datenschutzrechtliche Einschätzung darzulegen und es zur Stellungnahme aufzufordern. Wir verwiesen zunächst darauf, dass ehrenamtliche Fischereiaufseherinnen und Fischereiaufseher eine hoheitliche Aufgabe wahrnehmen. Gegenüber Betroffenen und Außenstehenden werden sie in einer staatlichen Funktion tätig. Sie agieren für die unteren Fischereibehörden, die gemäß den gesetzlichen Vorgaben datenschutzrechtlich Verantwortliche sind.

Wir machten deutlich, dass die Verwendung privater Smartphones zur Datenverarbeitung bei einer staatlichen Kontrolle ohne weitere Vorkehrungen datenschutzrechtlich nicht tragbar ist. Der unbefugte Zugriff Dritter auf personenbezogene Daten wird dadurch erleichtert. Ferner können die unteren Fischereibehörden die effektive Kontrolle über die gespeicherten und verarbeiteten Daten nicht gewährleisten. Bilder könnten z. B. weitergeleitet, veröffentlicht oder mittels Cloud-Diensten in Drittstaaten verarbeitet werden. Es ist auch nicht auszuschließen, dass die Fotos gezielt für private Zwecke verwendet werden. Als Verantwortliche muss die untere Fische-

reibehörde deshalb z. B. dafür Sorge tragen, dass technische und organisatorische Sicherheitsmaßnahmen umgesetzt werden. Eine Belehrung zur Verschwiegenheit reicht nicht aus, um einen sicheren Umgang mit personenbezogenen Daten zu gewährleisten.

Zudem genügt es, auf dem Kontrollbericht zu vermerken, dass der Personalausweis gesichtet wurde. Das Fotografieren von Ausweisdokumenten ist datenschutzrechtlich nicht erforderlich. Außerdem kritisierten wir, dass sich auf dem Kontrollbericht weder ein Hinweis auf die Behörde finden lässt, die das Formular ausgestellt hat, noch auf eine Stelle, an die sich eine betroffene Person wenden könnte. Nach den gesetzlichen Vorschriften hat der Verantwortliche zumindest Datenschutzhinweise zur Gewährleistung der Transparenz zur Verfügung zu stellen. Da bei einer Kontrolle durch ehrenamtliche Fischereiaufseherinnen und Fischereiaufseher personenbezogene Daten verarbeitet werden, haben Betroffene das Recht zu erfahren, wie mit ihren Daten umgegangen wird.

Während ein Landkreis die Verwendung privater Smartphones zum Zweck der Fischereiaufsicht inzwischen untersagt hat, waren wir mit einem anderen Landkreis sowie mit dem Ministerium zum Redaktionsschluss dieses Berichts noch im Gespräch.

6 Datenerhebungen durch Jobcenter zur Ermittlung von Bedarfsgemeinschaften

Menschen, die Arbeitslosengeld II (ALG II) beziehen, müssen ihre personenbezogenen Daten gegenüber den Jobcentern offenlegen. Regelmäßig verlangen die Jobcenter auch Angaben von den Partnerinnen und Partnern der Antrag stellenden Person. Hierbei geht es vor allem um Angaben zu Einkommen und Vermögen. Wir erhalten daher regelmäßig Beschwerden und Anfragen von betroffenen Personen zur Klärung der Berechtigung entsprechender Datenerhebungen.

Im Rahmen der gesetzlichen Aufgabenwahrnehmung sind Jobcenter als Sozialleistungsträger gemäß § 67a Zehntes Buch Sozialgesetzbuch (SGB X) zu Datenerhebungen befugt, soweit sie für die Erfül-

lung der gesetzlichen Aufgabe erforderlich sind. Erforderlich ist eine Datenerhebung immer nur dann, wenn die Behörde ihre Aufgaben ohne sie nicht erledigen könnte. Gesetzliche Aufgabe der Jobcenter ist die Leistungsprüfung und -gewährung nach dem Zweiten Buch Sozialgesetzbuch (SGB II). Hierfür dürfen sie auch die Angaben einer Partnerin oder eines Partners von Antrag stellenden Personen anfordern.

Einblicke in die private Lebensführung

Für viele Menschen stellt sich jedoch die Frage, wer genau als Partnerin oder als Partner zählt. Grundsätzlich werden Leistungen nach dem SGB II immer für Bedarfsgemeinschaften gewährt. Zur Bedarfsgemeinschaft zählt gemäß § 7 Absatz 3 Nummer 3 SGB II auch die Partnerin oder der Partner, welche mit der bzw. dem erwerbsfähigen Leistungsberechtigten zusammenlebt. Die Begriffe Partnerin oder Partner umfassen nach § 7 Absatz 3 Nummer 3 Buchstabe a, b SGB II die nicht dauernd getrenntlebende Ehegattin oder den Ehegatten sowie die nicht dauernd getrenntlebende Lebenspartnerin oder den Lebenspartner. Als weiteres Modell der Partnerschaft ist in § 7 Absatz 3 Nummer 3 Buchstabe c SGB II die Verantwortungs- und Einstehensgemeinschaft genannt. Diese wird nach der gesetzlichen Definition angenommen, wenn eine Person mit der erwerbsfähigen, leistungsberechtigten Person in einem gemeinsamen Haushalt zusammenlebt und nach verständiger Würdigung der wechselseitige Wille anzunehmen ist, Verantwortung füreinander zu tragen und füreinander einzustehen. In § 7 Absatz 3a Nummer 1 bis 4 SGB II findet sich zudem die gesetzliche Vermutung, wann eine Verantwortungs- und Einstehensgemeinschaft anzunehmen ist.

Angaben von Partnerinnen oder Partnern können daher gemäß § 67a SGB X gefordert werden, sobald eine Bedarfsgemeinschaft nach § 7 Absatz 3 SGB II angenommen wird, da die Jobcenter Leistungen immer nur für die gesamte Bedarfsgemeinschaft gewähren oder ablehnen können. Deshalb müssen auch die Einkommens- und Vermögensverhältnisse von allen Personen der Bedarfsgemeinschaft geklärt werden.

Es kommt häufig vor, dass sich Jobcenter und Antrag stellende Personen nicht einig sind, ob eine Verantwortungs- und Einstehensgemeinschaft besteht, weshalb sich die Betroffenen mit einer Beschwerde an uns wenden. Die Landesbeauftragte kann jedoch lediglich die Einhaltung der datenschutzrechtlichen Vorgaben prüfen. Das Bestehen einer Verantwortungs- und Einstehensgemeinschaft ist eine materiell-sozialrechtliche Voraussetzung. Die Entscheidung hierüber obliegt nur dem zuständigen Jobcenter und im Zweifel den angerufenen Gerichten, nicht jedoch der Datenschutzaufsichtsbehörde.

7 Videoüberwachung in Gemeinschaftsunterkünften für Geflüchtete

Durch eine Beschwerde erlangten wir Kenntnis davon, dass der kommunale Betreiber einer für Geflüchtete genutzten Gemeinschaftsunterkunft dort in großem Umfang eine Überwachung mittels Videokameras betreibt. Im Rahmen des Anhörungsverfahrens stellten wir fest, dass über 120 Videokameras auf dem in Frage stehenden Gelände zum Einsatz kommen. Diese erfassen dabei sowohl den kompletten Außenbereich mit Kinderspielplatz und Sportplatz, als auch die Flure, Eingänge und Treppenhäuser. Der Sicherheitsdienst kann die Bilder in Echtzeit beobachten, zudem speichern alle Videokameras dauerhaft ihre Aufnahmen.

Praktisch alle öffentlich zugänglichen Bereiche der Unterkunft werden überwacht. Weiterhin sind Kameras auf Türen der Wohnungen der Geflüchteten und auf Zugangstüren zu den sanitären Anlagen gerichtet. Aufgrund dieser Gegebenheiten lag es aus unserer Sicht nahe, dass geflüchtete Personen, die in der Einrichtung leben, dauerhaft überwacht werden.

Nach Angaben des Verantwortlichen wurde die Videoüberwachung unter anderem eingerichtet, um bei Eskalationen im Haus schneller reagieren zu können. Es komme häufig zu teils auch gewalttätigen Auseinandersetzungen. Weiterhin sei nur so der Schutz von Beschäftigten sowie Bewohnerinnen und Bewohnern ausreichend zu gewährleisten.

Die Auswertung der im Vorfeld bereitgestellten Informationen nahm eine beachtliche Zeit in Anspruch, da die Daten vom Verantwortlichen sehr umfangreich und schlecht aufbereitet waren. Zudem fehlten viele wichtige Dokumente, wie beispielsweise ein Konzept zur Protokollierung der Zugriffe auf die Videokameras und die sogenannte Freigabeerklärung. Auf Nachfrage wurde uns sogar bestätigt, dass Zugriffe gar nicht protokolliert werden. Insgesamt sind sowohl die Umsetzung der Videoüberwachung als auch die Dokumentation in einem datenschutzwidrigen Zustand.

Nach unserer ersten Rechtseinschätzung gibt es zahlreiche rechtswidrige Datenverarbeitungen aufgrund des Einsatzes der Videokameras. So ist eine Videoüberwachung von Kinderspielplätzen und Sportplätzen, auf denen sich regelmäßig Familien mit kleinen Kindern aufhalten, grundsätzlich nicht erlaubt. Weiterhin ist eine Kameraüberwachung der Zugangstüren zu den sanitären Anlagen ein tiefgreifender Eingriff in die Rechte der Betroffenen und mithin rechtswidrig.

Wir führten mit der verantwortlichen öffentlichen Stelle ein Gespräch, um die Sach- und Rechtslage zu erörtern. Dabei erläuterten wir zahlreiche Maßnahmen, die der Verantwortliche umsetzen muss, um einen datenschutzrechtlich zulässigen Betrieb der Videoüberwachung zu ermöglichen. Dazu gehören die Veränderung zahlreicher Kameraerfassungsbereiche, die Einschränkung der Aufzeichnungsdauer, das Aussparen von besonders sensiblen Bereichen sowie die Reduzierung der im Betrieb befindlichen Videokameras.

Für diese umfangreichen Anpassungen wurde dem Verantwortlichen angemessen Zeit eingeräumt. Die mit Ablauf der Frist gelieferte Dokumentation wies jedoch immer noch Mängel auf, die vom Verantwortlichen zu beseitigen sind. Wir befinden uns weiterhin in Gesprächen und Abstimmungen, um möglichst schnell einen rechtmäßigen Zustand herstellen zu können. Oberstes Ziel ist, die besonders schutzbedürftigen Personen effektiv vor einer Verletzung ihrer Rechte zu bewahren. Ob die Landesbeauftragte von ihren Abhilfebefugnissen Gebrauch macht, wird im weiteren Verfahren zu entscheiden sein.

8 Weiterleitung von Drittwidersprüchen gegen eine Baugenehmigung – wieviel Transparenz muss sein?

Im September 2022 erreichte uns eine Vielzahl gleichlautender Beschwerden. Alle Beschwerde führenden Personen hatten beim zuständigen Landkreis einen sogenannten Drittwiderspruch gegen eine Baugenehmigung eingelegt und im Anschluss jeweils ein Schreiben der Bauherrin erhalten. Darin äußerte diese ihre Verwunderung über die Widersprüche und teilte mit, dass Schadensersatzansprüche unberührt blieben. Weiterhin konnten wir einem Schreiben des Landkreises an die Bauherrin entnehmen, dass Letzterer Namen und Anschriften der betroffenen Personen genannt wurden.

Die Beschwerdeführerinnen und Beschwerdeführer hielten dies für unzulässig. Es sei ihnen nicht mitgeteilt worden, dass ihr Widerspruch der Bauherrin in personenbezogener Form zugänglich gemacht würde. Außerdem ergebe sich aus dem Anschreiben der Bauherrin eine Drohung, die so nur durch die Weitergabe ihrer personenbezogenen Daten möglich geworden sei.

Für die Übermittlung personenbezogener Daten durch öffentliche Stellen, die immer einen Grundrechtseingriff darstellt, ist eine Rechtsgrundlage erforderlich. Sofern eine gesetzliche Rechtsgrundlage vorliegt, ist davon auszugehen, dass den Betroffenen nach dem Willen des Gesetzgebers die Offenbarung ihrer Daten zuzumuten ist, um höherrangige Interessen zu wahren.

Im konkreten Fall verneinte die Landesbeauftragte ein datenschutzrechtliches Fehlverhalten des Landkreises. Die Übermittlung diente nicht nur der Erfüllung einer gesetzlichen Aufgabe bzw. einer rechtlichen Verpflichtung, sondern war hierfür auch erforderlich. Sie war damit nach Artikel 6 Absatz 1 Buchstabe e bzw. c Datenschutz-Grundverordnung zulässig.

Mit dem hier in Frage stehenden Drittwiderspruch will jemand einen Verwaltungsakt beseitigen, der eine andere Person begünstigt und durch den sie oder er sich selbst beschwert fühlt. Mit der möglichen

Aufhebung eines solchen Verwaltungsaktes wird in die Rechtspositionen der oder des Begünstigten eingegriffen, hier mit der Aufhebung der Baugenehmigung in die Position der Bauherrin. Dagegen muss sich die bzw. der Begünstigte nach rechtsstaatlichen Grundsätzen effektiv zur Wehr setzen können. Voraussetzung ist im vorliegenden Fall aber, dass die Bauherrin überhaupt Kenntnis von Inhalt und Umständen des Widerspruchs erhält, wofür die Kenntnis gerade von Name und Anschrift der Drittwiderspruchsführenden erforderlich ist. Dies folgt schon daraus, dass es bei baurechtlichen Drittwidersprüchen oft auf die konkrete Lage der Grundstücke der betroffenen Personen ankommt, weil Voraussetzung für Widerspruch und Klage die Geltendmachung einer unmittelbaren Betroffenheit in eigenen Rechten ist. So ist ein Drittwiderspruch möglicherweise unzulässig, wenn das Grundstück der Beschwerdeführerin bzw. des Beschwerdeführers von dem genehmigten Bauvorhaben nicht selbst nachteilig betroffen ist, etwa, weil es zu weit entfernt liegt.

In Verwaltungsverfahren, die in die Rechte anderer eingreifen können, besteht darüber hinaus kein allgemeiner Anspruch von Beteiligten darauf, anonym zu bleiben. Es besteht im Gegenteil für Bauamtsbeschäftigte die Amtspflicht, durch rechtzeitige Mitteilung von Drittwidersprüchen an die oder den Begünstigten einer Baugenehmigung mögliche wirtschaftliche Schäden für die Bauherrin oder den Bauherrn abzuwenden.[11] Hieraus ergab sich im konkreten Fall nicht nur die Befugnis, sondern die Verpflichtung zur Weitergabe der personenbezogenen Daten.

Soweit das Vorgehen der Bauherrin, welches den Drittwiderspruchsführenden bedrohlich erschien, als Argument für die Rechtswidrigkeit der Weitergabe ins Feld geführt wurde, so war der Landkreis hierfür datenschutzrechtlich nicht – auch nicht mittelbar – verantwortlich.

Es ist darauf hinzuweisen, dass das Vorstehende lediglich Drittwidersprüche Verfahrensbeteiligter betrifft und keinesfalls auf alle Verwaltungsverfahren verallgemeinert werden kann.

11 Urteil des Bundesgerichtshofs vom 9. Oktober 2003, III ZR 414/02.

9 Verschlüsselung beim Auslesen von Funkwasserzählern

Zwei technisch versierte Bürger informierten uns im Berichtszeitraum darüber, dass neu eingebaute Funkwasserzähler, die in ihren Haushalten im Auftrag des zuständigen Abwasser- und Wasserzweckverbandes installiert worden waren, die Verbrauchsdaten augenscheinlich unverschlüsselt regelmäßig alle 15 Sekunden übertragen. Sie interessierten sich für die Möglichkeiten der Heimautomatisierung, experimentierten etwas und stellten fest, dass sie neben ihren eigenen Daten auch diejenigen anderer Haushalte erhalten und auswerten konnten. Nach einer Ausweitung der Tests im Wohnumfeld identifizierten sie insgesamt 185 derartige Zähler, von denen sie Daten im Klartext empfingen.

Verbrauchsdaten für Fremde

Als Konsequenz aus diesen Feststellungen kontaktierten die beiden Bürger den zuständigen Zweckverband, das Bundesamt für Sicherheit in der Informationstechnik, den Hersteller der verbauten Funkzähler und die Landesbeauftragte. Dem Schreiben waren eine Dokumentation des Versuchsaufbaus, detaillierte technische Informationen zur verwendeten Hard- und Software sowie eine Erläuterung des Vorgehens beigefügt.

Die Antwort des Zweckverbandes, deren Inhalte auch in der Stellungnahme an uns enthalten waren, gab Aufschluss über die vorhandene Situation: Die verbauten Funkwasserzähler nutzten bei der Datenübertragung zwar eine verschlüsselte Kommunikation – allerdings wurde als Verschlüsselungsschlüssel kein individueller, sondern ein Standardschlüssel verwendet. Der Standardschlüssel war offenbar nicht geheim, da er auch in der von den beiden interessierten Bürgern verwendeten Open Source Software hinterlegt war. Dadurch konnten sie die Verbrauchsdaten im Klartext lesen.

Das Unternehmen, welches vom Zweckverband mit dem Einbau der Funkwasserzähler beauftragt war, hatte dies schon einige Wochen zuvor bemerkt und entsprechende Maßnahmen ergriffen. Gemeinsam mit dem Zweckverband führte es unverzüglich eine Klärung mit dem Hersteller herbei. In diesem Zusammenhang sollten in allen

Haushalten, in denen die fehlerhaften Wasserzähler verbaut wurden, Updates vorgenommen und jeweils individuelle Schlüssel im Zähler installiert werden. Dies würde jedoch wegen der Terminfindung mit den Kundinnen und Kunden einige Wochen dauern.

Im Kontakt mit dem Zweckverband waren wir uns einig, dass der Versuchsaufbau und das Vorgehen der beiden Bürger, die uns über den Vorfall informiert hatten, technisches Spezialwissen benötigen. Hierüber verfügen die meisten anderen Personen nicht, sodass wir von keinem hohen Risiko für die Rechte und Freiheiten der Betroffenen ausgingen. Des Weiteren haben wir dem Zweckverband geraten, neben der stichprobenartigen funktionalen Überprüfung der Zähler in Zukunft auch das Vorhandensein von Individualschlüsseln zu kontrollieren. Da der Zweckverband geeignete Maßnahmen ergriffen hatte und das Risiko für die Betroffenen als gering eingeschätzt wurde, schlossen wir den Vorgang ab. Im weiteren Verlauf informierten wir unsere Kolleginnen und Kollegen der für den Hersteller der Funkwasserzähler zuständigen Aufsichtsbehörde in einem anderen Bundesland über den Vorfall.

10 Der Zensus 2022

Bereits im letzten Tätigkeitsbericht hatten wir über die Vorbereitungen zur Durchführung des regelmäßigen Zensus berichtet.[12] Er wurde pandemiebedingt um ein Jahr auf 2022 verschoben. Im Berichtszeitraum haben die Landesämter und das Bundesamt für Statistik zentral sowie die Erhebungsstellen der Kommunen vor Ort die Gebäude- und Wohnraumzählung bzw. die Haushaltebefragung durchgeführt.

Im Rahmen einer Gebäude- und Wohnraumzählung wurden alle privaten Eigentümerinnen und Eigentümer, aber auch gewerbliche Vermieterinnen und Vermieter, Verwalterinnen und Verwalter und andere Verfügungs- und Nutzungsberechtigte von Wohnungen oder Gebäuden mit Wohnraum herangezogen. Gleichzeitig erfolgte eine Haushaltebefragung bei ca. 10 % der Bevölkerung. Die konkret zu befragenden Personen werden mittels eines mathematischen Zu-

12 Tätigkeitsbericht Datenschutz 2021, A V 7.

fallsverfahrens ausgewählt und die Ergebnisse der Befragung dann auf die Gesamtbevölkerung hochgerechnet. Von den so ermittelten Zahlen hängt beispielsweise die Höhe der für die Gemeinden aus dem Landeshaushalt bereitgestellten Gelder ab. Insgesamt wurden in Deutschland für den Zensus 10,3 Millionen und für die Gebäude- und Wohnraumzählung 23 Millionen Menschen befragt.

Die zur Auskunft aufgeforderten Personen waren aufgrund des Zensusgesetzes verpflichtet, die Fragen zu beantworten. In ihr Recht auf informationelle Selbstbestimmung und das damit verbundene Recht, selbst darüber zu entscheiden, wie mit den eigenen Daten umgegangen werden soll, wurde insoweit zulässigerweise eingegriffen. Im Fall einer Weigerung konnten die Betroffenen darüber hinaus mit Zwangs- oder Bußgeldern belegt werden.

Die Erhebung war erstmalig darauf ausgerichtet, die Fragen online zu beantworten. Hiervon versprach man sich u. a. eine vereinfachte Auswertung, eine kürzere Bearbeitungszeit und Kostenersparnisse beim Versand der Unterlagen. Mit der Aufforderung zur Teilnahme an der Befragung wurden daher in diesem Jahr keine Papierfragebögen versandt, sondern lediglich ein Zugangscode, der zur Abgabe der geforderten Angaben der auf elektronischem Weg über das Internet berechtigte. Daneben blieb es möglich, die Beantwortung der Fragebögen auch schriftlich, telefonisch oder nach Terminvereinbarung gemeinsam mit Erhebungsbeauftragten der Kommune vorzunehmen.

Da es in Deutschland keine einheitlichen, bundesweiten Melde- oder Gebäuderegister gibt, wurden die Anschriften der Auskunftspflichtigen durch Abfragen unterschiedlicher Register ermittelt. Verwendet wurden neben den Melderegistern und den Grundbüchern auch die Datenbestände der Vermessungsbehörden, Grundsteuerstellen und der öffentlichen Ver- und Entsorgungsbetriebe. Manche der genutzten Register erwiesen sich als nicht aktuell oder widersprüchlich, da es zwischen ihnen keinen automatischen Abgleich gibt, Schreibweisen nicht konsistent sind oder Inhalte verzögert aufgenommen werden.

Das führte z. B. dazu, dass Menschen zur Auskunft herangezogen wurden, obwohl sie in keinerlei Beziehung zu Gebäuden oder Wohnungen standen, zu denen Daten erhoben werden sollten. In den meisten Fällen ließ sich der Fehler schnell klären. Auch der Online-Fragebogen eröffnete bereits die Möglichkeit mitzuteilen, nicht Eigentümerin oder Eigentümer der fraglichen Immobilie zu sein.

In einigen Fällen wurden Personen angemahnt, die Fragebögen zu beantworten, obwohl sie diese bereits zurückgeschickt hatten. Hier waren entweder Poststücke nicht angekommen, der Rücklauf von den Erhebungsbeauftragen noch nicht erfolgt oder die elektronische Erfassung der Fragebögen noch nicht abgeschlossen. In anderen Fällen erwiesen sich die im Auftrag der Kommunen tätigen Erhebungsbeauftragten als säumig.

Angesichts der großen Zahl der betroffenen Personen war absehbar, dass Fehler nicht ausbleiben würden. Dennoch stellt jede unberechtigte Heranziehung zu Auskünften eine unzulässige Verarbeitung personenbezogener Daten dar. Daher werden die statistischen Ämter neben der Auswertung der erhobenen Daten auch die Prozesse zur Vorbereitung und Durchführung der Erhebung überprüfen und gegebenenfalls anpassen müssen. Gleiches gilt für die kommunalen Erhebungsstellen hinsichtlich der Auswahl und Schulung der Erhebungsbeauftragten.

V Ausgewählte Beratungen

1 Arbeitsgruppe der Datenschutzkonferenz zu Microsoft Online-Diensten

Der Cloud-Dienst Microsoft 365, früher bekannt als Microsoft Office 365, beschäftigt die Datenschutzaufsichtsbehörden bereits seit einigen Jahren – nicht nur in Form von Anfragen, Beratungsersuchen und Beschwerden. Wir berichteten bereits darüber, dass sich der Arbeitskreis „Verwaltung“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) damit befasste und zu einer kritischen Einschätzung in Bezug auf die Einhaltung der datenschutzrechtlichen Anforderungen beim Einsatz durch Verantwortliche kam.[13] Auf Grundlage dieser Vorarbeiten gründete die Konferenz im November 2020 die Arbeitsgruppe „DSK Microsoft Online-Dienste“, deren Auftrag es war, durch einen Dialog mit Microsoft Verbesserungen und letztlich Rechtskonformität zu erreichen.[14]

Nach zweijähriger Tätigkeit, in der 14 umfangreiche Gespräche mit Vertreterinnen und Vertretern des Unternehmens Microsoft aus Deutschland und den USA geführt wurden, beendete die Arbeitsgruppe im November 2022 ihre Arbeit und legte der Datenschutzkonferenz einen Abschlussbericht vor, den wir in unserem Internetangebot veröffentlicht haben. Dieser Bericht basiert auf dem am 15. September 2022 geänderten „Datenschutznachtrag zu den Produkten und Services von Microsoft“. Das Dokument bildet die Grundlage der vertraglichen Regelungen zur Einbindung von Microsoft als Dienstleister und muss deshalb die Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an eine Auftragsverarbeitung, insbesondere Artikel 28 DS-GVO, erfüllen.

Microsoft versuchte, mit Änderungen in dem Datenschutznachtrag auf die Kritikpunkte der Arbeitsgruppe zu reagieren. Nach deren Kenntnis hat das Unternehmen auf Grundlage der geführten Gespräche jedoch keine Veränderungen an den tatsächlichen Datenverarbeitungen mittels Microsoft 365, insbesondere der Verarbeitung personenbezogener Daten, vorgenommen. Es ist daher wichtig hervorzuheben, dass sich der Abschlussbericht der Arbeitsgruppe

13 Tätigkeitsbericht Datenschutz 2020, A V 1.5.
14 Tätigkeitsbericht Datenschutz 2021, A V 1.

allein auf die Änderungen im Datenschutznachtrag und dadurch möglicherweise erzielte Verbesserungen fokussiert. Weder wurden konkrete Verarbeitungstätigkeiten unter Einsatz von Microsoft 365 noch einzelne Komponenten des Online-Dienstes oder gar das komplette Produkt durch die Arbeitsgruppe geprüft. Das wäre auch nicht zielführend, denn schon vor dem Hintergrund der unzähligen Einsatzszenarien und der Vielzahl an Komponenten würden derartige Prüfungen entweder nur einen konkreten Einzelfall abdecken oder wären aufgrund der Komplexität nicht in angemessener Zeit durchführbar.

Bezogen auf die Einhaltung der Anforderungen an eine Auftragsverarbeitung beim Einsatz von Microsoft 365 konnte die Arbeitsgruppe durch die Änderungen im Datenschutznachtrag lediglich geringfügige Verbesserungen feststellen. So wurden die für die Verantwortlichen bereitgestellten Informationen in Bezug auf technisch-organisatorische Maßnahmen, die Microsoft als Dienstleister umsetzt, ergänzt. Hinsichtlich der Löschung bzw. Rückgabe von personenbezogenen Daten zum Ende der Auftragsverarbeitung erläuterte das Unternehmen zwar seine Prozesse, offenbarte dabei jedoch auch Ungenauigkeiten und Widersprüche. Des Weiteren hat Microsoft aufgrund der Erörterungen mit der Arbeitsgruppe der Datenschutzkonferenz das Verfahren verbessert, mit dem Verantwortliche über Änderungen bei der Unterauftragsverarbeitung informiert werden. Sie werden nun proaktiv per E-Mail über solche Änderungen benachrichtigt. Dies ist zwar ein Schritt in die richtige Richtung, allerdings ist die Information noch nicht hinreichend konkret. Darüber hinaus bleiben auch weitere Nachbesserungen erforderlich – etwa Gegenstand, Art und Zweck der Auftragsverarbeitung, Kategorien betroffener personenbezogener Daten und Gruppen betroffener Personen so detailliert wie möglich im Auftragsverarbeitungsvertrag zu beschreiben.

Der Hauptkritikpunkt bei der Nutzung von Microsoft 365 bleibt aber trotz Änderungen im Datenschutznachtrag bestehen: Microsoft verarbeitet personenbezogene Daten aus der Auftragsverarbeitung immer noch für eigene Zwecke, ohne dies hinreichend transparent und nachvollziehbar darzustellen. Die Änderungen im Datenschutznachtrag grenzen zwar diese Verarbeitung für „Geschäftstätigkeiten“ von Microsoft, welche früher als „legitime Geschäftszwecke“ bezeichnet

wurden, etwas ein. Trotz dieser Anpassung bleibt jedoch unklar, welche personenbezogenen Daten für welche Zwecke im Rahmen der „Geschäftstätigkeiten“ wie und wie lange verarbeitet werden.

Eine verantwortliche Stelle, die Microsoft 365 einsetzen will, braucht eine eigene Rechtsgrundlage, damit die im Auftrag verarbeiteten personenbezogenen Daten an Microsoft übermittelt und dort für eigene „Geschäftstätigkeiten“ verarbeitet werden können. Die damit verbundenen Nachweise, zum Beispiel für Interessenabwägungen, oder die Informationen für betroffene Personen, können aufgrund der unvollständigen und ungenauen Angaben von Microsoft allerdings nicht allein auf Basis des Datenschutznachtrages erbracht werden. Öffentliche Stellen (z. B. Behörden oder Schulen in öffentlicher Trägerschaft) haben beim Einsatz von Microsoft 365 das zusätzliche Problem, dass sich deren Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten typischerweise aus der Erfüllung öffentlicher Aufgaben oder aus spezialgesetzlichen Regelungen ergeben. Die Weitergabe personenbezogener Daten an Microsoft, damit sie dort für eigene „Geschäftstätigkeiten“ verarbeitet werden, kann durch derartige Rechtsgrundlagen nicht legitimiert werden.

Wegen der weiter bestehenden Mängel stellte die Datenschutzkonferenz auf Basis des Abschlussberichts der Arbeitsgruppe fest, dass von Verantwortlichen der Nachweis, Microsoft 365 datenschutzkonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten Datenschutznachtrags vom 15. September 2022 nicht geführt werden kann. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden. Im Kontext der Datenschutz-Grundverordnung bedeutet diese Feststellung, dass ein Verantwortlicher gegen seine Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DS-GVO verstößt, solange der Nachweis nur auf der Grundlage des Datenschutznachtrags geführt wird.

Anzumerken ist noch, dass der Bericht der Arbeitsgruppe der Datenschutzkonferenz auch Aussagen zur Rechtmäßigkeit von Datentransfers in Drittstaaten (hier: insbesondere in die USA) und die Berück-

sichtigung der Anforderungen des sogenannten Schrems II-Urteils des Europäischen Gerichtshofes enthält. Da sich in diesem Kontext allerdings Änderungen anbahnen (z. B. durch das Microsoft-Projekt „EU Data Boundary“ oder die Verhandlungen zwischen der Europäischen Kommission und den USA zur Feststellung der Angemessenheit des Datenschutzniveaus in den USA und einen entsprechenden Beschluss nach Artikel 45 Absatz 3 DS-GVO), spielte dieser Punkt in der Bewertung der Datenschutzkonferenz nur eine untergeordnete Rolle.

2 Datenschutzverletzungen durch Angriffe auf Dienstleisterinnen und Dienstleister

Im Berichtszeitraum erreichte uns eine erhebliche Anzahl an Meldungen nach Artikel 33 Datenschutz-Grundverordnung (DS-GVO) zu Datenschutzverletzungen, die Ergebnis von Hacking-Angriffen auf externe Dienstleistungsunternehmen der datenschutzrechtlich Verantwortlichen waren. Erstmalig beobachteten wir eine solche Entwicklung im Jahr 2021 im Zusammenhang mit IT-Sicherheitslücken des von Behörden und Unternehmen häufig eingesetzten Produkts Microsoft Exchange Server.[15] Der Aufwärtstrend setzte sich in diesem Jahr nicht nur fort, sondern verstärkte sich noch.

Nach Artikel 4 Nummer 7 DS-GVO ist diejenige Stelle (Behörde, Einrichtung, Unternehmen, Verein usw., ggf. auch Privatperson) datenschutzrechtlich Verantwortlicher, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Den Verantwortlichen trifft die Pflicht, die gesetzlichen Bestimmungen der Datenschutz-Grundverordnung und weiterer Vorschriften über den Datenschutz einzuhalten. Er muss dies auch nachweisen können. Hiervon umfasst ist insbesondere die Umsetzung von technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes und der Informationssicherheit bei der Verarbeitung personenbezogener Daten.

Mit der zunehmenden Komplexität, Kompliziertheit und Vernetzung von Datenverarbeitungsprozessen einerseits und der gleichzeitig

15 Tätigkeitsbericht Datenschutz 2021, A IV 1.

abnehmenden Verfügbarkeit personeller, finanzieller und zeitlicher Ressourcen bei den Verantwortlichen andererseits hat in den letzten Jahren die Tendenz, Datenverarbeitungen an externe Unternehmen auszulagern, zugenommen. Die Palette reicht von einzelnen Verarbeitungsschritten wie der Vernichtung von Papierakten, über den Betrieb von IT-Verfahren wie der Personal- oder Bewerberverwaltung bis hin zu einem kompletten Outsourcing der gesamten IT-Landschaft in die sogenannte Cloud.

Outsourcing mit Verantwortung!

Viele Verantwortliche meinen, sie könnten sich auf diese Weise auch ihrer datenschutzrechtlichen Pflichten entledigen. Immerhin kümmert sich ja nun ein (hoffentlich) kompetentes Unternehmen. Diese Schlussfolgerung ist jedoch trügerisch: Aus datenschutzrechtlicher Sicht ist ein Auftragsverarbeiter im Sinne des Artikel 4 Nummer 8 DS-GVO weisungsgebunden. Für die Ausgestaltung des Verhältnisses zwischen beiden Seiten ist ein Vertrag zu schließen, dessen wesentliche inhaltliche Anforderungen Artikel 28 DS-GVO auflistet. Ein vollständiger Übergang der Verantwortung für die Datenverarbeitung auf den Auftragsverarbeiter ist hiermit jedoch nicht verbunden. Insbesondere ist der Verantwortliche verpflichtet, die Auftragsausführung durch die Dienstleisterin oder den Dienstleister zu kontrollieren.

Die zunehmende Spezialisierung im Bereich der IT-Dienstleistungsunternehmen führt auch zu einer Konzentration von Auftragsverarbeitungen. Die spezialisierten, deutschland- oder europaweiten Angebote dieser Unternehmen werden von sehr vielen datenschutzrechtlich Verantwortlichen in Anspruch genommen. Ein erfolgreicher Angriff auf einen Auftragsverarbeiter – z. B. durch das Ausnutzen von IT-Sicherheitslücken, das Platzieren von Schadsoftware, das Einschleusen von Ransomware zur Verschlüsselung von Datenbeständen, die Erpressung von Lösegeld zur Entschlüsselung, das Ausleiten und anschließende Offenlegen von personenbezogenen Daten u. a. m. – hat deshalb zur Folge, dass jeweils eine Reihe von Verantwortlichen von dem Angriff betroffen sein kann. Falls es dabei zu einer Verletzung des Datenschutzes kommt, sind die Verantwortlichen nach Artikel 33 DS-GVO jeweils verpflichtet, diese der für sie zuständigen Datenschutzaufsichtsbehörde zu melden.

Wie wir feststellen mussten, kann dabei schnell eine mittlere zweistellige Zahl an Verantwortlichen zusammenkommen, die wegen desselben Vorfalls bei demselben Auftragsverarbeiter und derselben Ursache eine Meldung an uns abgeben. Häufig erschöpfen sich diese Meldungen jedoch darin, lediglich die Informationen der Dienstleisterin bzw. des Dienstleisters unkommentiert zu wiederholen. Da in vielen, insbesondere kleinen Unternehmen oder Vereinen die erforderliche Datenschutz- und IT-Kompetenz fehlt, können dort auch keine detaillierten, eigenen Bewertungen des Vorfalls vorgenommen werden. Die Verantwortlichen sind insofern den Auftragsverarbeitern „ausgeliefert", müssen deren Ausführungen, Ermittlungen und Zusicherungen glauben und hoffen, dass die erforderlichen Datenschutz- und Sicherheitsmaßnahmen getroffen werden, um eine Wiederholung des erfolgreichen Hackings zu verhindern.

Diese Entwicklung beunruhigt uns. Sie deutet sich bereits seit einigen Jahren beispielsweise dadurch an, dass Verantwortliche Auftragsverarbeitungsverträge nach Artikel 28 DS-GVO, die ihnen von potenziellen Dienstleistungsunternehmen vorgelegt werden, trotz zum Teil erheblicher Mängel akzeptieren. Auch hier ist unseres Erachtens unzureichende Kompetenz in grundlegenden datenschutzrechtlichen und technischen Fragen die Ursache.

Vor diesem Hintergrund sind alle Verantwortlichen aufgefordert, dauerhaft personelle, finanzielle und zeitliche Ressourcen einzuplanen, um Fachkenntnisse und Prüfkompetenz auf den Gebieten des Datenschutzes und der Informationssicherheit zu entwickeln und aufrechtzuerhalten – vorzugsweise in der Behörde, im Unternehmen oder im Verein selbst. Hierbei kommt der bzw. dem Datenschutzbeauftragten eine besondere Bedeutung zu. Zu ihren bzw. seinen Aufgaben gehören z. B. die Beratung des Verantwortlichen in allen datenschutzfachlichen Angelegenheiten und die Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften. Eine Stärkung der Position und Kompetenz dieser Rolle kann somit direkte Auswirkungen auf die rechtskonforme Ausgestaltung und eigenständige Kontrolle von Auftragsverarbeitungen haben.

Auch in unserer Beratungs- und Aufsichtstätigkeit werden wir den Fokus in diesem Zusammenhang vermehrt auf die Stärkung der

Position der Verantwortlichen gegenüber Auftragsverarbeitern, die Herausbildung und Fortentwicklung eigenen Fachwissens und eigener Fähigkeiten bei den Verantwortlichen sowie der intensiveren Überprüfung von Dienstleisterinnen und Dienstleistern und ggf. der Ahndung rechtswidrigen Verhaltens dort legen.

3 Novellierung des Staatsvertrages zwischen dem Land Brandenburg und dem Land Berlin über die Führung eines Krebsregisters

Aufgrund der Kündigung des Vertrages zur Führung des Gemeinsamen Krebsregisters,[16] einem epidemiologischen Register der neuen Bundesländer und Berlins, zum 31. Dezember 2022, wurde es notwendig, dessen Aufgaben für Brandenburg neu zu regeln. Gleiches galt u. a. auch für Berlin. Eine Zusammenführung im Staatsvertrag zum Klinischen Krebsregister für Berlin und Brandenburg[17] lag aufgrund der Sachnähe, aber auch wegen bereits praktizierter Datenflüsse zwischen den beiden Einrichtungen nahe. Der entsprechende Entwurf eines Staatsvertrages für ein klinisch-epidemiologisches Krebsregister der Länder Brandenburg und Berlin wurde uns Ende 2021 vorgelegt. Etwa ein halbes Jahr lang setzten wir uns immer wieder intensiv und sehr konstruktiv mit dem Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz, der zuständigen Berliner Senatsverwaltung und der Berliner Beauftragten für Datenschutz und Informationsfreiheit dazu auseinander. Der Staatsvertrag wurde schließlich im September 2022 unterzeichnet; er erlangte zum Ende des Berichtsjahres Gesetzeskraft.[18]

Zunächst sollten Regelungen zu Datenverarbeitungen und zur Organisation in einer Verwaltungsvereinbarung getroffen werden. Dies hielten wir für nicht angemessen. Nicht alle Aufgaben des künftigen Registers wurden bedacht, die Begriffe im Staatsvertrag teilweise

16 Tätigkeitsbericht 2014/2015, B 7.1.1.
17 Tätigkeitsbericht 2014/2015, B 7.1.2.
18 Gesetz zu dem Staatsvertrag zwischen dem Land Brandenburg und dem Land Berlin über die Führung eines klinisch-epidemiologischen Krebsregisters nach § 65c des Fünften Buches Sozialgesetzbuch und § 1 des Bundeskrebsregisterdatengesetzes vom 16. Dezember 2022, GVBl. I, Nr. 28.

nicht an die Datenschutz-Grundverordnung angepasst, Datenschutzrechte der Patientinnen und Patienten mehr als notwendig eingeschränkt und auch der Umgang mit einem Widerspruchsrecht der betroffenen Personen noch nicht richtig umgesetzt. Nach den oben genannten Erörterungen nahm sich der Staatsvertrag all dieser Themen und Probleme in einer datenschutzfreundlichen Weise an. Zusätzlich wurden die Forschungsklauseln verbessert, der Zweck der bundesweiten Gesundheitsberichterstattung, die allein mit aggregierten Daten erfolgt, getrennt davon geregelt und dafür gesorgt, dass die Abrechnung mit personenbezogenen Angaben vorgenommen werden kann.

Der zwischenzeitlich aufgekommenen Idee, die Meldepflichtigen könnten freiwillig über den bundesweit festgelegten Basisdatensatz hinaus personenbezogene Daten zu Krebskranken übermitteln, traten wir erfolgreich entgegen, da sie andere gesetzliche Vorgaben nicht berücksichtigte. Zum zunächst zwingend vorgesehenen Abgleich mit dem Deutschen Kinderkrebsregister wurde geklärt, dass er nicht mit der freiwilligen Befüllung dieses Registers vereinbar ist. Für diese Ausnahmefälle erhielt letztlich das Deutsche Kinderkrebsregister das Recht, vom neuen Krebsregister der Länder Brandenburg und Berlin die erforderlichen Auskünfte einholen zu dürfen.

4 Prüfung der Verfassungstreue vor Berufung in das Beamtenverhältnis

Um etwaigen extremistischen Tendenzen im öffentlichen Dienst zu begegnen und deren Entstehung vorzubeugen, hat der Landtag Brandenburg im Sommer 2020 die Landesregierung u. a. aufgefordert zu prüfen, wie eine Zuverlässigkeitsprüfung von Bewerberinnen und Bewerbern vor der Einstellung in den öffentlichen Dienst des Landes Brandenburg erfolgen könnte.

Der Parlamentarische Beratungsdienst des Landtages Brandenburg hat mit seinem Gutachten vom 26. Mai 2021 die Zulässigkeit einer Regelanfrage beim Verfassungsschutz zur Prüfung der Verfassungstreue von Beamtinnen und Beamten und den damit verbundenen

Eingriff in das Recht auf informationelle Selbstbestimmung festgestellt. Dessen Auffassung teilen wir.

Die Landesregierung erarbeitete daraufhin einen Gesetzentwurf, mit dem eine Regelanfrage bei der Verfassungsschutzbehörde vor der erstmaligen Begründung eines Beamtenverhältnisses sowie im Rahmen von Disziplinarverfahren, bei denen der Verdacht der Verletzung der Verfassungstreue im Raum steht, eingeführt werden soll. Zu Beginn des Berichtszeitraums erhielten wir im Rahmen der Anhörung nach § 18 Absatz 5 Brandenburgisches Datenschutzgesetz Gelegenheit, zum Entwurf eines Gesetzes zur Verbesserung des Schutzes der Beamtenschaft in Brandenburg vor Verfassungsgegnern Stellung zu nehmen.

Der Gesetzentwurf berücksichtigte zunächst datenschutzrechtliche Anforderungen nicht in ausreichendem Maß. So wurden beispielsweise im Rahmen der Regelungen zur Datenübermittlung von der Verfassungsschutz- an die Einstellungsbehörde Begriffe nicht normenklar und einheitlich verwendet, Löschszenarien zu ungenau geregelt und für elektronische Datenübermittlungen – gemessen am hohen Schutzbedarf der zu verarbeitenden Daten – nur allgemein die Beachtung von Vertraulichkeit, Integrität und Authentizität verlangt. Dies genügt allerdings nicht. Vielmehr hat die Verfassungsschutzbehörde bereits gemäß § 9 Absatz 1 Brandenburgisches Verfassungsschutzgesetz unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Person die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Verfassungstreue erforderlich, Prüfung auch?

Das Ministerium des Innern und für Kommunales hat unsere Stellungnahme zum Anlass genommen, den Gesetzentwurf unter datenschutzrechtlichen Aspekten noch einmal zu schärfen und zu korrigieren. Die von der Landesregierung Ende August 2022 be-

schlossene Fassung wurde als Gesetz zur Verbesserung des Schutzes des Berufsbeamtentums in Brandenburg vor Verfassungsgegnern in den Landtag eingebracht. Dieser hat den Entwurf zur Beratung an den Ausschuss für Inneres und Kommunales verwiesen.

Am Ende des Berichtszeitraums hatte die Landesbeauftragte im Rahmen der Anhörung im vorgenannten Ausschuss Gelegenheit darzulegen, dass sie die Regelanfrage beim Verfassungsschutz für erstmalig zu verbeamtende Bewerberinnen und Bewerber aller Berufsgruppen als ein geeignetes Mittel ansieht, um ein Unterwandern des öffentlichen Dienstes durch Verfassungsgegnerinnen und -gegner möglichst zu verhindern. Die Anfrage wird nur für diejenigen Personen gestellt, die über alle sonstigen Einstellungsvoraussetzungen verfügen. Das Merkmal der Gewährleistung der Verfassungstreue ist dann das letzte durch die Einstellungsbehörde zu prüfende Kriterium. Weil die Allgemeinheit ein überwiegendes Interesse daran hat, zu verhindern, dass Verfassungsgegnerinnen und -gegner unerkannt den Beamtenstatus erlangen und damit z. B. das Funktionieren von Rechtsstaat und Demokratie beeinträchtigt wird, steht die Regelanfrage nicht von vornherein außer Verhältnis zum Recht auf informationelle Selbstbestimmung.

Sofern der Landtag Brandenburg das Gesetz beschließen sollte, mahnte die Landesbeauftragte insbesondere die Einhaltung der Löschfristen sowohl bei der Einstellungs- als auch der Verfassungsschutzbehörde aber auch die Transparenz einer Ablehnungsentscheidung gegenüber den betroffenen Personen an.

Einer Evaluierung des Gesetzes nach ca. vier Jahren misst die Landesbeauftragte aufgrund der Eingriffstiefe in die Persönlichkeitsrechte besondere Bedeutung zu. Einstellungsbehörden sollten für diesen Zweck Prozesse etablieren, um (Negativ-) Entscheidungen, die aufgrund der Erkenntnisse des Verfassungsschutzes getroffen wurden, nicht personenbezogen vorzuhalten.

5 Der Zweckverband Digitale Kommunen Brandenburg

Bereits im April 2020 wurde der Zweckverband Digitale Kommunen Brandenburg (DIKOM) gegründet. Gemäß seiner Satzung stellt er den Mitgliedern Datenverarbeitungsverfahren, Datenverarbeitungsleistungen und zugehörige Serviceleistungen zur Erledigung oder Vereinfachung von Verwaltungsaufgaben mit technikunterstützter Informationsverarbeitung zur Verfügung. Die Verbandsmitglieder können diese freiwillig ganz oder teilweise nutzen. Zu den Aufgaben des Zweckverbandes gehören u. a.

- die Wartung, Pflege und Weiterentwicklung der bereitgestellten Verfahren,

- die Beratung und Unterstützung der Mitglieder in den Bereichen Digitalisierung und E-Government sowie bei der Auswahl, Beschaffung und Nutzung von Hard- und Software,

- die Planung, die Einrichtung und der Betrieb eines Rechenzentrums einschließlich der Kommunikationsnetze sowie

- die Beratung und Unterstützung der Verbandsmitglieder in Angelegenheiten des Datenschutzes und der IT-Sicherheit.

Zum Ende des Berichtszeitraums waren ca. 70 brandenburgische Städte, Ämter und Gemeinden als Mitglieder des Zweckverbandes registriert.

Bereits seit der Gründung des Verbandes beabsichtigten wir, mit den Verantwortlichen vor Ort ins Gespräch zu kommen, datenschutzrechtliche und technisch-organisatorische Aspekte der Tätigkeit zu erörtern und die Räumlichkeiten – insbesondere das Rechenzentrum – zu besichtigen. Durch die Corona-Pandemie verzögerte sich die Umsetzung dieses Anliegens jedoch. Erst im Berichtszeitraum konnte ein Treffen mit allen Beteiligten durchgeführt werden.

Im Rahmen der Beratung gaben der Verbandsvorsteher, der Datenschutzbeauftragte und einige Beschäftigte einen Einblick in die

Tätigkeit. Hierzu gehören insbesondere die Betreuung von ca. 350 kommunalen Fachverfahren (u. a. für die Personalverwaltung und -abrechnung oder für das Personenstandswesen), die Bereitstellung von Rechenzentrums- und Infrastrukturdiensten sowie der Betrieb einer Druckstraße. Darüber hinaus bietet der Zweckverband Unterstützung für Kommunen bei der Umsetzung des Brandenburgischen E-Government-Gesetzes und des Onlinezugangsgesetzes, z. B. durch den Betrieb eines Formularservers sowie die Anbindung von IT-Basiskomponenten des Landes Brandenburg. Weiterhin stellt er Serviceleistungen für Schulen bereit, indem z. B. Informationstechnik beschafft, eingerichtet und betrieben, Geräte wie Smart Boards konfiguriert und Schulserver administriert werden.

Gemeinsam zu einem besseren Datenschutz

Der Zweckverband DIKOM unterstützt seine Mitglieder auch in Belangen des Datenschutzes und der Informationssicherheit, insbesondere durch die Erarbeitung von Konzepten und Analysen, die Planung und Umsetzung von Datenschutz- und Sicherheitsmaßnahmen sowie die Sensibilisierung und Schulung. Er informierte uns über sein Datenschutz- und Informationssicherheitsmanagement. Abschließend besichtigten wir das im Auftrag des Zweckverbandes durch ein externes Unternehmen betriebene Rechenzentrum. Es wurde im Mai 2022 eröffnet. Wir haben vereinbart, den Austausch mit dem Zweckverband fortzusetzen.

Zu beachten ist, dass auch im Falle einer Beauftragung des DIKOM jede Kommune selbst datenschutzrechtlich verantwortliche Stelle im Sinne der gesetzlichen Regelungen bleibt.

6 Registrierung von Geflüchteten aus der Ukraine durch die Sozialbehörden

Mit der groß angelegten russischen Invasion in der Ukraine im Februar 2022 sah sich auch das Land Brandenburg mit einer gesteigerten Zahl von geflüchteten Personen konfrontiert. Um sie mit dem Notwendigsten zu versorgen und ihnen eine Unterkunft zu geben, war es erforderlich, die geflüchteten Menschen zunächst zu regis-

trieren. Regulär geschieht das durch das Bundesamt für Migration und Flüchtlinge sowie durch die regional zuständigen Ausländerbehörden. Erst danach kommt die Zuständigkeit der Sozialbehörden für die Gewährung von Hilfeleistungen zum Tragen. Durch den Massenzustrom konnte ein geordnetes Verfahren nicht immer realisiert werden. Der Datenschutzbeauftragte eines Landkreises bat daher zu Beginn des Jahres um Auskunft, ob eine Registrierung der Geflüchteten durch die Sozialbehörden und die Weiterleitung dieser Registrierungsdaten an die Ausländerbehörden aus datenschutzrechtlicher Perspektive zulässig ist. Damit sollte eine zügige Erfassung und gleichzeitig auch die schnelle Gewährung von Sozialleistungen ermöglicht werden.

Der Durchführungsbeschluss (EU) 2022/382[19] legte fest, dass alle Menschen, die aufgrund des Angriffskrieges aus der Ukraine geflohen sind, einen humanitären Aufenthaltsstatus erhalten – in Deutschland nach § 24 Absatz 1 Aufenthaltsgesetz (AufenthG). Langwierige Antragsverfahren sollten mit Hinblick auf die große Anzahl von geflüchteten und hilfsbedürftigen Menschen vermieden werden. Kurz darauf erließ das Bundesministerium des Innern und für Heimat zur Umsetzung des Durchführungsbeschlusses zudem eine Leitlinie, die u. a. festgelegt, dass jegliche Bitten um Unterstützung durch Geflüchtete, z. B. nach Unterkunft, Verpflegung oder medizinische Versorgung, als Schutzbegehren nach § 24 Absatz 1 AufenthG zu werten sind.

Zwar war durch diese Maßnahmen der Europäischen Union und des Bundesministeriums die Rechtslage klargestellt, jedoch verblieb die Zuständigkeit zur Antragsbearbeitung bei den Ausländerbehörden. Für die Landkreise stellte sich die Frage, ob bzw. wie die Sozialbehörden tatsächlich rechtmäßig die geflüchteten Menschen registrieren können. Denn eine erlaubte Datenübermittlung von den Sozialbehörden an die Ausländerbehörden kann nur im Rahmen von Artikel 6 Absatz 1 Buchstabe e, Absatz 3 Buchstabe b Datenschutz-Grundverordnung vorgenommen werden. Dies setzt voraus, dass die Da-

19 Durchführungsbeschluss (EU) 2022/382 des Rates vom 4. März 2022 zur Feststellung des Bestehens eines Massenzustroms von Vertriebenen aus der Ukraine im Sinne des Artikels 5 der Richtlinie 2001/55/EG und zur Einführung eines vorübergehenden Schutzes, ABl. L 71 vom 4. März 2022, S. 1.

tenübermittlung zur Erfüllung einer gesetzlichen Aufgabe der Sozialbehörden erforderlich ist. Weiterhin muss neben der gesetzlichen Aufgabe auch eine Befugnis zur Datenverarbeitung vorliegen. Und auch die Ausländerbehörden müssen als empfangende Stellen zur Datenverarbeitung befugt sein und die erhaltenen Daten zur Aufgabenwahrnehmung benötigen.

Zu den gesetzlichen Aufgaben der Sozialbehörden gehört die Prüfung des Aufenthaltsstatus nach § 1 Absatz 1 Nummer 3a Asylbewerberleistungsgesetz (AsylBLG), da alle Menschen mit einem Aufenthaltsstatus nach § 24 Absatz 1 AufenthG auch einen Anspruch auf Sozialleistungen nach der genannten Vorschrift haben. Zuständig für diese Aufgabe der Leistungsprüfung sind nach dem Landesaufnahmegesetz die Sozialbehörden der Landkreise.

Sobald eine öffentliche Stelle in Erfüllung ihrer gesetzlichen Aufgabe Kenntnis über eine ausländische Person erlangt, die keinen Aufenthaltstitel besitzt, muss sie die zuständige Ausländerbehörde gemäß § 87 AufenthG hierüber informieren. Ukrainische Staatsbürgerinnen und Staatsbürger müssen gemäß den Vorgaben des Aufenthaltsgesetzes einen Aufenthaltstitel zum rechtmäßigen Aufenthalt in der Bundesrepublik Deutschland aufweisen können. Es besteht somit die gesetzliche Verpflichtung der Sozialbehörden, die Ausländerbehörden zu informieren, sobald eine aus der Ukraine geflüchtete Person ohne Aufenthaltstitel Sozialleistungen beantragt. Dabei müssen den Ausländerbehörden insbesondere Identifizierungs- und Kontaktdaten der betroffenen Person zur Verfügung gestellt werden, da ohne diese Angaben kein aufenthaltsrechtliches Verfahren möglich ist. Angaben zum Einreisedatum sind ebenso erforderlich, um den Aufenthaltstitel erteilen zu können.

Datenschutz steht schneller Hilfe nicht im Weg

Das Aufenthaltsgesetz legt fest, dass Ausländerbehörden Daten, die für ihre Aufgabenerfüllung erforderlich sind, sowohl von anderen öffentlichen Stellen empfangen als auch selbst erheben dürfen. Deshalb können die Ausländerbehörden Informationen der Sozialbehörden entgegennehmen. In diesem Zusammenhang ist die örtliche Zuständigkeit zu beachten. Stellt sich zum Beispiel eine aus der

Ukraine geflohene Person beim Sozialamt in einem Landkreis vor, so ergibt sich die Notwendigkeit zur Erteilung eines Aufenthaltstitels immer in demselben Landkreis.

Wir konnten daher dem Datenschutzbeauftragten mitteilen, dass eine Datenübermittlung von den Sozialbehörden an die Ausländerbehörden datenschutzrechtlich zulässig ist. Die Registrierung der geflüchteten Personen durch die Sozialbehörden und damit eine Unterstützung der Ausländerbehörden konnte somit auch vor dem weiteren Tätigwerden des Gesetzgebers datenschutzkonform vorgenommen werden.

7 Datenschutzgerechte Formulare für Volksbegehren

Von Oktober 2021 bis April 2022 fand das Volksbegehren „Volksinitiative zur Abschaffung der Erschließungsbeiträge für Sandpisten“ statt. Das vom Landesabstimmungsleiter für die Beantragung von Stimmzetteln zur Verfügung gestellte Musterformular war Gegenstand dreier Anfragen, nämlich aus der Mitte des Landtages Brandenburg, aus einem Amt im Landkreis Barnim und schließlich durch den Landesabstimmungsleiter selbst.

Bei dem Formular handelte sich um ein digital ausfüllbares Dokument, welches mit „Elektronische Beantragung eines Eintragungsscheins“ überschrieben war. Die Antrag stellende Person sollte es per Post oder als Anlage zu einer E-Mail an die Abstimmungsbehörde übersenden. Gegenstand der Anfragen war eine auf dem Schreiben abgedruckte Notiz zur Übermittlung des Antrags per E-Mail. Dieser wichtige datenschutzrechtliche Hinweis lautete: „Wir wollen Ihnen mit diesem Angebot einen Weg zu uns ersparen. Wir weisen Sie aber darauf hin, dass Ihre angegebenen Daten im Internet/über E-Mail unverschlüsselt übermittelt werden. Dem Datenschutz wird also insoweit keine Rechnung getragen.“ In einer Fußnote war zu lesen: „Dieser Hinweis entfällt, wenn die Datenübertragungen durch geeignete (Verschlüsselungs-)Verfahren geschützt sind.“ Die Angabe zur E-Mail-Adresse im Formularfeld war als freiwillig gekennzeichnet.

Die Landesbeauftragte stellte fest, dass der Hinweis rein informatorisch neben den gesetzlichen Transparenzpflichten stand, keine unrichtigen Aussagen enthielt und nicht rechtswidrig war. Wohl aber erkannten wir hier eine verpasste Chance, die datenschutzrechtlichen Risiken bei der Versendung des Formulars zu verdeutlichen und nach Möglichkeit zu vermeiden – ein Defizit, das sich für zukünftige Fälle abzustellen lohnte.

Auffällig war die Diskrepanz zwischen dem Hinweis selbst und der Fußnote. Der Hinweis sagte aus, dass das Versenden per E-Mail als Übertragungsweg generell riskant ist und der Datenschutz dabei nicht berücksichtigt wird. Die Fußnote hingegen enthielt die Aufforderung, den Hinweis für den Fall zu ignorieren, dass für die Übertragung ein Verschlüsselungsverfahren existiert. Dies hielten wir in zweierlei Hinsicht für problematisch: Einerseits verwirrte die Zweiteilung mit ihren entgegengesetzten Botschaften. Anderseits war die Fußnote abstrakt so formuliert, dass sie Adressatinnen und Adressaten ohne spezielles technisches Wissen keine Anhaltspunkte gab, wie die Sicherheit der Verbindung geprüft und gewährleistet werden kann.

Partizipation datenschutzgerecht

Wir schlugen vor, die Zweiteilung zwischen Haupttext und Fußnote aufzuheben und darüber hinaus Antragstellerinnen und Antragstellern zu empfehlen, sich zu informieren, ob ihr E-Mail-Provider eine Transportverschlüsselung unterstützt. Bei den meisten kommerziellen Anbieterinnen und Anbietern ist dies der Fall. Darüber hinaus ist (auch durch die Kommunen) sicherzustellen, dass das Transportverschlüsselungsprotokoll Transport Layer Security (TLS) mindestens auf dem Stand der Version 1.2 zur Verfügung steht. Davon unabhängig schlugen wir vor, darauf hinzuweisen, dass eine Einsendung des Formulars per Post jederzeit ohne Nachteile möglich ist.

Hinsichtlich des Feldes zur freiwilligen Angabe der E-Mail-Adresse der Teilnehmerinnen und Teilnehmer am Volksbegehren regten wir an, bereits in dem Feld, in dem die E-Mail-Adresse eingetragen werden konnte, die Zwecke mitzuteilen, für welche diese genutzt werden soll. Diese können z. B. darin bestehen, Abstimmungsscheine

auf elektronischem Weg zu versenden oder Rücksprachen mit den Antragstellenden zu halten.

Wenn Vorschläge wie diese berücksichtigt werden, sind betroffene Personen in der Lage, das Risiko bei der Übermittlung selbst einzuschätzen und ihre eigenen, souveränen Entscheidungen über die Verwendung ihrer Daten zu treffen (sogenannter Selbstdatenschutz). Allerdings blieb an der Lösung über die Einsendung per E-Mail grundsätzlich der Umstand verbesserungswürdig, dass es überhaupt von Entscheidungen und Nachforschungen der betroffenen Person abhängt, eine sichere Übermittlung zu gewährleisten. Es ist grundsätzlich Aufgabe der Verantwortlichen, sichere Transportwege in allen Fällen anzubieten. Da diese auch für andere Verwaltungsangelegenheiten im Zuge der Digitalisierung erforderlich sind, führt an der technischen Umsetzung dauerhaft kein Weg vorbei.

8 Geheimhaltung des Abstimmungsverhaltens in Gemeindevertretungen?

In einer Lokalzeitung war zu lesen, dass vier namentlich genannte Stadtverordnete in nicht öffentlicher Sitzung gegen einen Antrag gestimmt hatten. Die Stadtverwaltung wollte wissen, ob die Weitergabe dieser Information durch in der Sitzung Anwesende einen Datenschutzverstoß darstellte. Die Landesbeauftragte verneinte diese Frage.

Sitzungen von Kommunalvertretungen und ihren Ausschüssen sind nach § 36 Absatz 2 Kommunalverfassung des Landes Brandenburg (BbgKVerf) im Regelfall öffentlich. Der Ausschluss der Öffentlichkeit ist nur in ausdrücklich normierten Fällen vorgesehen, wenn überwiegende Belange des öffentlichen Wohls oder berechtigte Interessen Einzelner es erfordern.

Beschlüsse der Gemeindevertretung kommen gemäß § 39 Absatz 1 BbgKVerf entweder wie hier durch offene Abstimmung oder durch geheime Wahl zustande. Eine geheime Abstimmung sieht die Kommunalverfassung nicht vor. Im Gegenteil kann ausdrücklich die namentliche Abstimmung beantragt werden, bei der das Stimmverhal-

ten der einzelnen Stimmberechtigten ausdrücklich protokolliert wird. Anwesende können das Abstimmungsverhalten stets direkt verfolgen. Die Beschlüsse der Gemeindevertretung sind schließlich gemäß § 39 Absatz 3 BbgKVerf in ortsüblicher Weise der Öffentlichkeit zugänglich zu machen. Abstimmungsergebnisse enthalten in der Regel nur dann Namen, wenn eine namentliche Abstimmung erfolgte.

Die Einwohnerinnen und Einwohner haben regelmäßig ein zu berücksichtigendes Interesse daran, über die Tätigkeit der Gemeindevertretung und auch über das Verhalten ihrer Gemeindevertreterinnen und Gemeindevertreter informiert zu sein, um hierauf künftige Wahlentscheidungen stützen zu können. Um das rechtsstaatliche Prinzip der Sitzungsöffentlichkeit zu wahren, sind der Ausschluss der Öffentlichkeit und die verkürzte Veröffentlichung von Beschlüssen nur in dem Maße zulässig, wie ansonsten tatsächlich Rechtsgüter der genannten Art gefährdet würden.

Wir haben für den vorliegenden Fall die Auffassung vertreten, dass das Abstimmungsverhalten als solches nicht Gegenstand des Schutzes war, der mit dem Ausschluss der Öffentlichkeit bzw. der Veröffentlichung des Beschlusses in gekürzter Form beabsichtigt wurde. Klassische Beispiele, warum die Öffentlichkeit ausgeschlossen sein kann, sind Grundstücksverkäufe, Personalangelegenheiten in der Verwaltung oder Vergabeverfahren. Kein Anwendungsfall der nicht öffentlichen Sitzung oder Abstimmung ist danach der bloße Umstand, dass ein kontroverses Thema diskutiert wird und Gemeindevertreterinnen bzw. Gemeindevertreter sich daher scheuen, ihr Abstimmungsverhalten offenzulegen. Die Kommunalverfassung sieht kein rechtlich geschütztes Interesse daran, das individuelle Abstimmungsverhalten zu verbergen. Auch ist durch die Bekanntgabe des Stimmverhaltens eine Gefährdung des Beratungsgeheimnisses nicht zu befürchten. Insoweit stehen die Mandatsträgerinnen und Mandatsträger bewusst unter demokratischer Kontrolle.

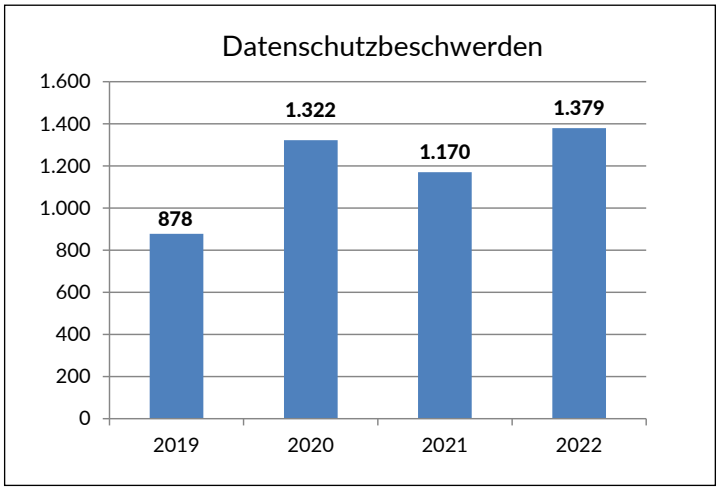
Anders als die Beratungen selbst unterfällt das Abstimmungsverhalten – selbst da, wo es mangels namentlicher Abstimmung nicht seinen Weg in die Niederschrift der Sitzungen findet, sondern nur von Anwesenden wahrgenommen wird – nicht ohne Weiteres dem Schutz der nicht öffentlichen Sitzungen. Die Frage, ob diese Daten

wirksam der kommunalverfassungsrechtlichen Verschwiegenheitspflicht unterworfen werden können, ist grundsätzlich zwar keine datenschutzrechtliche, dürfte aber nach dem Vorstehenden zu bezweifeln sein.

VI Zahlen und Fakten

1 Beschwerden

Im Berichtszeitraum gingen bei der Landesbeauftragten – neben einer Vielzahl telefonischer – 1.379 schriftliche Beschwerden gemäß Artikel 77 Datenschutz-Grundverordnung ein. Damit hat sich die Anzahl gegenüber dem Vorjahr noch einmal erhöht. Die Beschwerden wurden von Personen eingereicht, die der Ansicht waren, dass die Verarbeitung ihrer personenbezogenen Daten sie in ihren Rechten verletzt und gegen das Datenschutzrecht verstößt. Lässt man die zahlreichen Beschwerden im Kontext der Corona-Pandemie im Jahr 2020 unberücksichtigt, hält der Aufwärtstrend an.



2 Beratungen

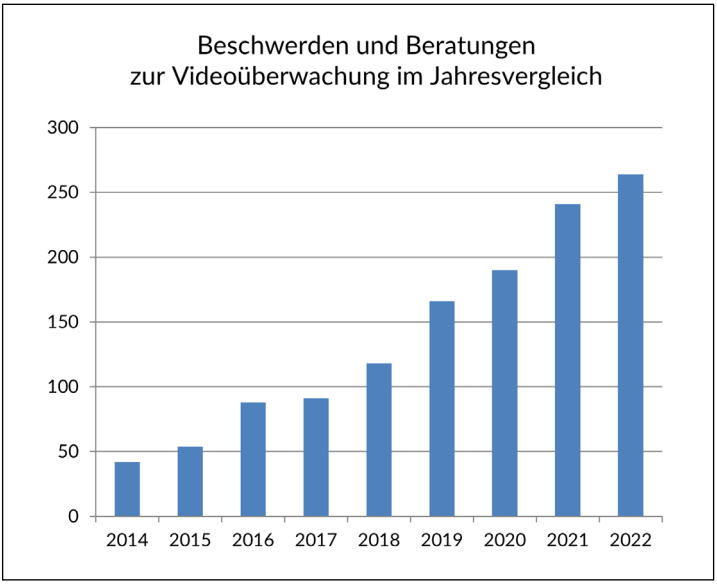
Neben der Bearbeitung von Beschwerden berät die Landesbeauftragte auch zu Datenschutzfragen. Im Berichtsjahr unterstützte sie in 445 Fällen betroffene Personen, Verantwortliche im öffentlichen wie nicht öffentlichen Bereich sowie die Landesregierung. Es lässt sich zwar ein zahlenmäßiger Rückgang beobachten, dem jedoch höhere Anforderungen und eine gestiegene Komplexität im Einzelfall gegenüberstehen. Einzelne Beratungen beinhalten oft eine umfassende Begleitung von Projekten, die erhebliche Ressourcen binden. Im Gegenzug ist es wieder gelungen, zahlreiche telefonische Anfragen mündlich zu beantworten, die wir statistisch nicht erfasst haben.

3 Videoüberwachung: Beschwerden und Beratungen

Die Landesbeauftragte stellte im Berichtsjahr erneut einen Anstieg von Beschwerden und schriftlichen Beratungsanfragen im Bereich der Videoüberwachung durch Privatpersonen, Unternehmen und öffentliche Stellen fest. Von den insgesamt 1.379 Beschwerden, die im Jahr 2022 in unserer Behörde eingingen, betrafen allein 247 die Videoüberwachung. 17 der insgesamt 445 Beratungen führten wir zu diesem Thema durch. Im Vergleich zu 2019, dem ersten vollständigen Jahr der Anwendung der Datenschutz-Grundverordnung, ist dies eine Zunahme um 60 %. Die zur Verfügung stehenden Stundenanteile bleiben hingegen konstant, sodass die Arbeitslast intern umverteilt werden musste. Die zahlreichen telefonischen Auskünfte haben wir nicht statistisch erfasst.

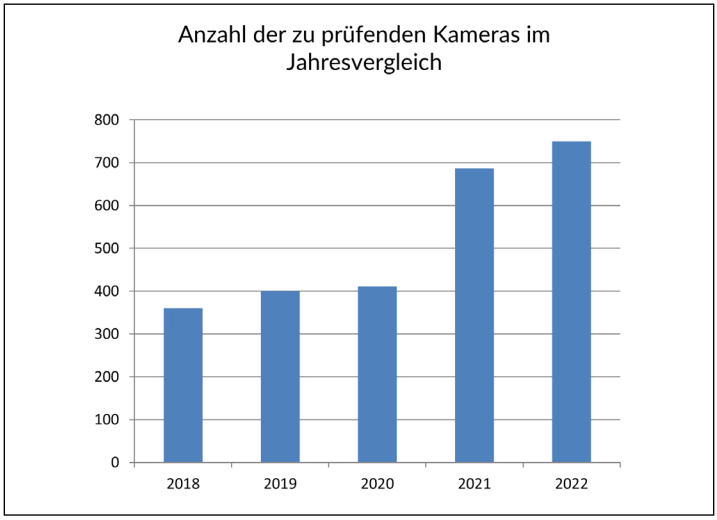
Ähnlich wie im letzten Jahr beschwerten sich Bürgerinnen und Bürger überwiegend über Videoüberwachungen im öffentlichen Straßenland, zum Beispiel durch Nachbarinnen bzw. Nachbarn mittels einer Klingelkamera oder einer am Wohnhaus montierten Kamera, die weit über das eigene Grundstück hinaus den öffentlichen Raum erfasst. Hinzu kommen einige wenige Fälle, in denen hauptsächlich ein angespanntes Nachbarschaftsverhältnis Grund für die Installation einer Videokamera ist und somit nur die jeweiligen Grundstücke gefilmt werden. Vermehrt stellten wir fest, dass Vermieterinnen und

Vermieter das unmittelbare Wohnumfeld ihrer Mieterschaft filmten. Auch mussten wir uns mit Pflegeeinrichtungen befassen, die Kameras in den privaten Rückzugsorten der Bewohnerinnen und Bewohner einsetzten. Weitere Beschwerden betrafen Videoüberwachungen am Arbeitsplatz, auf Baustellen sowie in Freizeiteinrichtungen, wie etwa Saunalandschaften, gastronomischen Betrieben und Fitnessstudios. Zunehmend mussten wir Beschwerden bearbeiten, die sich auf Fahrzeuge bezogen, die mit Videotechnik ausgestattet waren und entweder am fließenden Verkehr teilnahmen oder am Straßenrad abgestellt waren.



Da die datenschutzrechtliche Bewertung einer Videoüberwachung stets eine Einzelfallprüfung erforderlich macht, ist jede Kamera gesondert auf ihre rechtliche Zulässigkeit sowie gegebenenfalls auf die Umsetzung technisch-organisatorischer Maßnahmen zu kontrollieren. Im Berichtsjahr überprüften wir 750 Videokameras, im Jahr zuvor waren es 63 weniger. Im Jahr 2020 lag die Zahl der Kameras

noch bei 411. Insgesamt ließ sich somit ein deutlicher Zuwachs bei der Anzahl der zu bewertenden Videokameras feststellen.

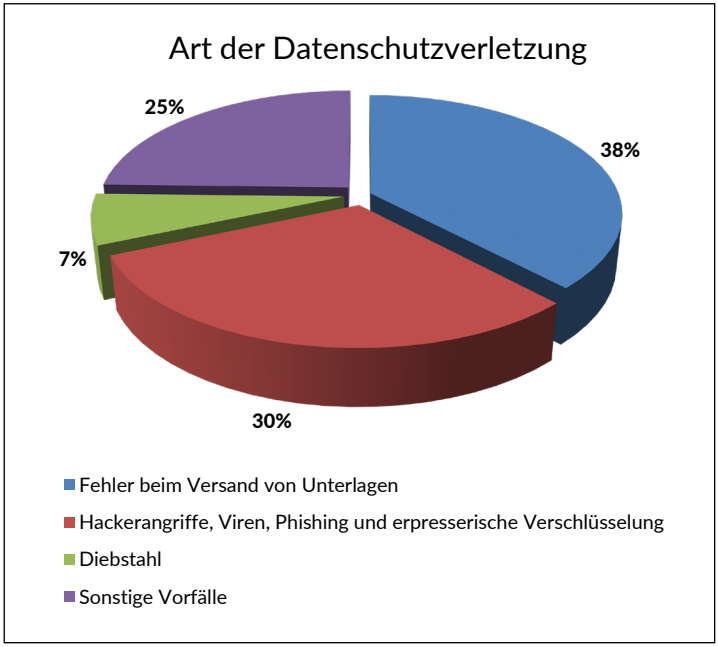


4 Meldungen von Datenschutzverletzungen

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 451 Meldungen von Datenschutzverletzungen. Die gemeldeten Daten-

schutzverletzungen geschahen sowohl im öffentlichen (178 Meldungen) als auch im nicht öffentlichen Bereich (273 Meldungen). Damit verringerte sich die Gesamtzahl um etwa 10 %.



Ein erheblicher, wenn auch im Vergleich zum Vorjahr geringerer Anteil der Meldungen betraf wieder den Fehlversand von Unterlagen (insgesamt 171 Fälle). Hiervon umfasst sind sowohl Fehlkuvertierungen von Briefpost, versehentlicher E-Mail-Versand an einen offenen Verteilerkreis, Namensverwechslungen oder die Beifügung von Unterlagen unbeteiligter Dritter.

138 Meldungen betrafen Datenschutzverletzungen, die auf technischen Mängeln beruhen und insofern Virenbefall, Phishing, Hacking-Angriffe, unberechtigte Zugriffe Dritter und erpresserische Verschlüsselungen von Datensätzen ermöglichen. An dieser, im Vergleich zum Vorjahr um 16 % gestiegenen Zahl wird deutlich, dass

Verantwortliche dem Einsatz und der Aktualisierung der technischen und organisatorischen Datenschutzmaßnahmen verstärkt Aufmerksamkeit widmen müssen. Ein Abhandenkommen physischer Datenträger, etwa durch Diebstähle aus den Räumen des Verantwortlichen oder durch den Verlust auf dem Postweg, wurde der Landesbeauftragten in 31 Fällen gemeldet – dies ist sogar ein Anstieg um ca. 30 %. Die 111 verbliebenen Fälle verteilten sich auf verschiedenste Gebiete des Umgangs mit personenbezogenen Daten.

Die Eingriffsqualität der hinter den Meldungen stehenden Datenschutzverletzungen ist sowohl qualitativ als auch quantitativ sehr unterschiedlich. So können Meldungen sich auf Einzelfälle beziehen und etwa bei der falschen Zustellung eines Werbebriefes zudem nicht besonders schwerwiegend sein, während in anderen Fällen die Zahl der betroffenen Personen sehr hoch ist und zugleich sensitive Daten eine Rolle spielen. In einem Fall waren beispielsweise Angaben in Höhe einer mittleren vierstelligen Zahl zu Beschäftigungsverhältnissen versehentlich zugänglich.

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. Insbesondere bei den immer noch im Mittelpunkt der Beschwerden stehenden Verwendung von Videokameras ist das der Fall: Ist eine Anlage oder ein Grundstück mit einer Vielzahl von Kameras ausgestattet, muss jede für sich bewertet werden. So gab es beispielsweise im Jahr 2022 eine Anordnung gegen den Verantwortlichen einer Videoüberwachungsanlage, die gleich 14 Kameras betraf. Sie wiesen ganz unterschiedliche Einstellungen auf, die jeweils individuell zu prüfen waren.

Die Landesbeauftragte sprach im Berichtszeitraum 10 Verwarnungen sowie 6 Anordnungen und Anweisungen aus.

5.2 Geldbußen

Im Berichtszeitraum wurden der Bußgeldstelle der Landesbeauftragten 52 Sachverhalte wegen Verstößen gegen datenschutzrechtliche Vorgaben zur Kenntnis gegeben. Die Verfahren wurden zu einem großen Anteil, nämlich in 43 Fällen, von den zuständigen Polizeibehörden oder Staatsanwaltschaften an die Bußgeldstelle weitergeleitet. Insgesamt 9 Sachverhalte haben aufsichtsbehördlich tätige Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten oder andere Aufsichtsbehörden mangels eigener Zuständigkeit an uns abgegeben.

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

In 13 Fällen verhängte die Landesbeauftragte wegen der festgestellten datenschutzrechtlichen Verstöße ein Bußgeld. Die Gesamtsumme der festgesetzten Bußgelder betrug knapp 123.000 Euro. In den übrigen Fällen wurde entweder kein Ordnungswidrigkeitenverfahren

eingeleitet, das Verfahren eingestellt oder mangels Zuständigkeit an die entsprechende Verfolgungsbehörde abgebeben.

6 Europäische Verfahren

Kapitel VII der Datenschutz-Grundverordnung (DS-GVO) sieht vor, dass in Fällen grenzüberschreitender Datenverarbeitung eine europaweite Zusammenarbeit der Datenschutzaufsichtsbehörden erfolgen muss. Eine solche grenzüberschreitende Verarbeitung liegt zum Beispiel dann vor, wenn der Verantwortliche personenbezogene Daten von betroffenen Personen aus mehreren Mitgliedsstaaten verarbeitet oder verarbeiten lässt. Um die Zusammenarbeit der EU-Behörden zu erleichtern, erfolgt der gegenseitige Austausch elektronisch über das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission. In diesem Rahmen hat die Landesbeauftragte in 1.702 Fällen geprüft, ob und welche Maßnahmen zu treffen sind:

In 645 Fällen, die von anderen europäischen Aufsichtsbehörden gemeldet wurden, prüften wir allgemein, ob eine Zuständigkeit der Landesbeauftragten als federführende oder betroffene Aufsichtsbehörde in Betracht kommt und entsprechende Verfahrensschritte ergriffen werden müssen. Neun bei uns eingegangene Beschwerden gegen eine grenzüberschreitende Datenverarbeitung haben wir den übrigen europäischen Aufsichtsbehörden mithilfe des Binnenmarkt-Informationssystems zur Kenntnis gegeben. Sie hatten damit die Gelegenheit, ebenfalls zu prüfen, ob sie in diesen Fällen federführende oder betroffene Aufsichtsbehörde sind. 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 keinem Fall feststellen können. Eine Betroffenheit der Landesbeauftragten ergab sich in 52 Fällen. In den übrigen Fällen haben wir nach Prüfung

der vorliegenden Informationen entschieden, uns nicht an dem weiteren Verfahren zu beteiligen, da die Verantwortlichen keine Niederlassung in Brandenburg hatten und keine erheblichen Auswirkungen auf Brandenburgerinnen und Brandenburger festzustellen waren.

In 1.005 Fällen beteiligten wir uns an Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII DS-GVO, etwa im Rahmen gegenseitiger Amtshilfe bzw. bei der Vorbereitung einer Stellungnahme des Europäischen Datenschutzausschusses oder prüften, ob die Landesbeauftragte einen Einspruch gegen die Entscheidung einer federführenden Aufsichtsbehörde einlegt.

Einen besonderen Schwerpunkt bildet dabei das gegenseitige Amtshilfeverfahren zwischen der Commission nationale pour la protection des données (CNPD), der Datenschutzaufsichtsbehörde des Großherzogtums Luxemburg, und der Landesbeauftragten. Diese erfolgt zur Bearbeitung von Beschwerden, die gegen das Unternehmen PayPal (Europe) S. à r. l. & Cie, S. C. A. (PayPal) gerichtet sind. PayPal hat seinen europäischen Hauptsitz in Luxemburg, weshalb die CNPD für datenschutzrechtliche Fragestellungen und Beschwerden, die PayPal-Dienste in Europa betreffen, die federführende Aufsichtsbehörde ist. In Brandenburg verfügt das Unternehmen über eine unselbstständige Zweigniederlassung, sodass wir die sachnächste Aufsichtsbehörde innerhalb Deutschlands gemäß § 19 Absatz 2 Satz 1 Bundesdatenschutzgesetz sind. Beschwerden gegen PayPal werden deswegen deutschlandweit an unsere Dienststelle abgegeben und hier zentral bearbeitet. Einen Teil übermitteln wir an die CNPD, einen Teil bearbeiten wir im Rahmen der gegenseitigen Amtshilfe und in engem Austausch mit der luxemburgischen Aufsichtsbehörde. Im Berichtsjahr sind 77 Beschwerden gegen PayPal entweder direkt an die Landesbeauftragte gerichtet oder von anderen deutschen Aufsichtsbehörden an sie weitergeleitet worden. In 22 – teilweise noch aus den Vorjahren weitergeführten – Verfahren haben wir für die CNPD Amtshilfe gemäß Artikel 61 DS-GVO geleistet. Davon lagen jedem Verfahren durchschnittlich jeweils fünf Beschwerden zugrunde.

7 Förmliche Begleitung von Rechtsetzungsvorhaben

Aus den zahlreichen Beratungen ist die Begleitung rechtsetzender Maßnahmen durch die Landesbeauftragte besonders hervorzuheben. Insgesamt nahmen wir im Berichtszeitraum 30 Mal zu Gesetzen, Verordnungen, Satzungen oder Verwaltungsvorschriften Stellung.

Die rechtliche Grundlage zur Beteiligung der Landesbeauftragten folgt aus § 18 Absatz 5 Satz 1 Brandenburgisches Datenschutzgesetz. Danach ist sie vor dem Erlass von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, zu hören. Auch die Datenschutz-Grundverordnung überträgt in Artikel 57 Absatz 1 Buchstabe c den Aufsichtsbehörden eine Beratungsfunktion bei rechtsetzenden Maßnahmen.

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

1 Begleitung von polizeilichen Projekten

Im Berichtszeitraum wurden wir von der Polizei intensiv in verschiedene Verfahren und Digitalisierungsprojekte eingebunden, die die polizeiliche Arbeit verändern werden und datenschutzrechtliche Relevanz haben. Während im vergangenen Jahr pandemiebedingt unsere Beratungen eher über schriftliche oder Online-Kommunikation erfolgten, fand nun auch wieder ein regelmäßiger Austausch vor Ort statt.

Das Fundament der polizeilichen IT-Sicherheit in Brandenburg, das Rahmensicherheitskonzept, dessen Erarbeitung und Umsetzung wir seit dem Jahr 2018 kritisch begleiten, hat im Berichtszeitraum weitere Fortschritte gemacht. Auch sind die wichtigen Vereinbarungen zur Auftragsverarbeitung inhaltlich wesentlich vorangekommen.[20]

Im Anwendungsbereich der Datenschutz-Grundverordnung ist das in Artikel 35 geregelte Instrument der Datenschutz-Folgenabschätzung inzwischen aufgrund von veröffentlichten Leitlinien des Europäischen Datenschutzausschusses und Handreichungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gut ausdifferenziert. Dies ist im Anwendungsbereich der EU-Richtlinie 2016/680 (JI-Richtlinie) noch nicht der Fall. Die entsprechenden Prozesse zur Erstellung von Datenschutz-Folgenabschätzungen bei der Polizei nach den Vorgaben des § 21 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz und § 67 Bundesdatenschutzgesetz müssen noch festgelegt werden. Dabei sind u. a. die spezifischen Risiken für die Rechte und Freiheiten Betroffener zu untersuchen und wirksame technische und organisatorische Maßnahmen zu bestimmen, um derartige Risiken zu verringern oder zu beseitigen.[21]

Regelmäßiger Austausch erfolgte auch über Teilprojekte des Programms P20 (ehemals Polizei 2020), eines übergreifenden Vorhabens von Bund und Ländern, das der Modernisierung und Harmonisierung der polizeilichen Informationsverarbeitung dienen und die bisher heterogene Datenverarbeitung in einem „gemeinsamen Datenhaus“

20 Tätigkeitsbericht Datenschutz 2021, B 3.2.
21 Siehe B 4.

vereinheitlichen soll. Um die Programmaktivitäten für das Teilnehmerland Brandenburg zu koordinieren und zu unterstützen bzw. für Digitalisierungsprojekte fachliche Kompetenzen zu bündeln, wurde beim Polizeipräsidium die Stabsstelle Digitalisierung eingerichtet, die auch für die Landesbeauftragte als Ansprechpartnerin fungiert. Im Zusammenhang mit P20 wurden uns die Planungen für ein neues Interims-Vorgangsbearbeitungssystem vorgestellt, das ausgehend von einem bereits in den Ländern Berlin und Nordrhein-Westfalen zum Einsatz kommenden System weiterentwickelt wurde. Es ist als notwendiger Teilschritt für eine später vereinheitlichte Vorgangsbearbeitung aller Teilnehmerinnen und Teilnehmer des Programms in Bund und Ländern erforderlich. In diesem Verfahren sollen u. a. neuere verfassungsrechtliche Anforderungen zum Datenaustausch zwischen Polizeibehörden und Nachrichtendiensten berücksichtigt, ein Unterstützungstool für das Erstellen von Negativprognosen und ein integriertes Asservaten- und Spurenmanagement umgesetzt werden. Verschiedene polizeiliche Informationssysteme müssen daran angeschlossen sein. Die flexible Nutzbarkeit auch außerhalb des festen Arbeitsplatzes stellt ebenfalls ein wichtiges Kriterium dar.

Uns wurden auch Informationen zu einem neu entwickelten mobilen Messenger bereitgestellt, der künftig auf den neu beschafften mobilen Diensttelefonen einsatzbegleitend genutzt werden soll. Die Telefone sollen darüber hinaus mit entsprechenden Apps sowohl für Abfragen aus Auskunftssystemen als auch für die Vorgangsbearbeitung ausgestattet werden.

Abgestimmt haben wir uns auch über die Notwendigkeit und den Umfang der Dokumentation für die Pilotphase von IT-Services der Polizei. Das Dilemma: Vielfach ergibt sich erst aus der Erprobung eines Verfahrens, welche konkreten Risiken für die Betroffenen bestehen bzw. welche technischen und organisatorischen Maßnahmen diese minimieren können. Die Pflicht zur Erstellung einer Datenschutz-Folgenabschätzung sieht aber vor, dass diese bereits vor Beginn des Pilotprojekts in der gesetzlich vorgeschriebenen, zeitaufwendigen Dokumentation bewertet werden. Der Arbeitsaufwand ist deshalb hoch, auch wenn das Projekt nach der Pilotphase gegebenenfalls nicht weitergeführt wird. Für einen Verzicht auf die erforderliche Dokumentation ist aufgrund der klaren rechtlichen

Vorgaben aus unserer Sicht zwar kein Raum, wir konnten aber einen guten Kompromiss hinsichtlich des Umfangs der zu erstellenden Dokumentation erzielen.

Zum Redaktionsschluss dieses Berichts war die nächste Beratung bereits avisiert, denn die Polizei in Brandenburg soll ein neues Führungs- und Einsatzleitsystem bekommen.

Wir begrüßen, dass wir von der Polizei nicht nur als kontrollierende Aufsicht wahr-, sondern auch als beratende Stelle in Anspruch genommen werden. Dies erlaubt, dass wir uns bei bedenklichen Entwicklungen für die IT-Sicherheit oder den Datenschutz frühzeitig einbringen können und Verfahren nicht erst nach Abschluss der Planungen von uns bewertet werden.

2 Koordinierte Prüfung von Personenausschreibungen im Schengenraum

Im Dezember 2021 und Januar 2022 prüfte die Landesbeauftragte in einer mit anderen Aufsichtsbehörden von Bund und Ländern abgestimmten Kontrolle insgesamt zehn nationale und schengenweite Personenausschreibungen aus Brandenburg. Dabei handelt es sich um eine Maßnahme, die – entweder zum Zweck der vorbeugenden Bekämpfung von Straftaten oder zur Strafverfolgung – zu einer verdeckten Beobachtung oder gezielten Kontrolle der betroffenen Personen durch die Polizei oder Grenzbehörden führt. Grundlage ist der Beschluss 2007/533/JI[22] (SIS II-Beschluss). Die erhobenen Daten zu Person, Ort, Zeit und Anlass der Überprüfung, Reiseweg und Reiseziel, Begleitpersonen, benutztem Fahrzeug, mitgeführten Sachen der oder des Betroffenen und Umständen des Antreffens dürfen an die ausschreibende Stelle übermittelt und dort gespeichert werden. Personenausschreibungen zur polizeilichen Beobachtung dürfen ferner angeordnet werden, um die Einhaltung von Weisungen zu überprüfen, die einer Straftäterin oder einem Straftäter nach Verbüßung der

22 Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 205 vom 7. August 2007, S. 63.

Haft im Rahmen der Führungsaufsicht gerichtlich auferlegt werden. Von den zum Stichtag 29. Oktober 2021 festgestellten 22 aktiven Personenausschreibungen aus Brandenburg wählten wir zur Prüfung jeweils vier aus, die zu präventiven und repressiven Zwecken erfolgten, sowie zwei, die der Führungsaufsicht dienten.

Die polizeiliche Maßnahme der Personenausschreibung stellt – insbesondere im Falle einer verdeckten Beobachtung – einen erheblichen Eingriff in das Persönlichkeitsrecht dar. Daher sind an die Anordnungen präzise Voraussetzungen geknüpft. Die polizeiliche Ausschreibung gemäß § 36 Brandenburgisches Polizeigesetz darf nur durch die Behördenleitung und für maximal ein Jahr angeordnet werden. Dieser Zeitraum kann um jeweils ein Jahr verlängert werden, doch muss in jedem Fall spätestens nach Ablauf von sechs Monaten in einer Einzelfallbewertung geprüft werden, ob die Voraussetzungen weiterhin vorliegen. Andernfalls ist die Maßnahme zu beenden. Eine Ausschreibung im gesamten Schengenraum zu präventiven Zwecken ist grundsätzlich nur erlaubt, wenn besonders schwere Straftaten zu befürchten sind, die dem Straftatenkatalog des § 100b Absatz 2 Strafprozessordnung (StPO) bzw. einer gelisteten Straftat nach Artikel 2 Absatz 2 Rahmenbeschluss 2002/584/JI[23] entsprechen.

Wir überprüften die Stichproben beim zuständigen Referat im Landeskriminalamt vor Ort in Cottbus. Dort konnten wir uns anhand der über das Auskunftssystem POLAS verfügbaren Daten einen Überblick über die gespeicherten Angaben zu den Personenausschreibungen verschaffen und den dazugehörigen Aktenrückhalt einsehen. Artikel 20 Absatz 3 SIS II-Beschluss listet abschließend die Datenkategorien auf, die zu einer Person gespeichert werden dürfen. Darüber hinausgehende Angaben konnten wir nur in einem Fall feststellen, in dem zu den zulässig gespeicherten Fingerabdrücken auch Handflächenabdrücke der betroffenen Person abrufbar waren. Anlass für die Maßnahmen waren stets die präventive oder repressive Bekämpfung von schwerem Bandendiebstahl gemäß § 244a Strafgesetzbuch und damit eines ausschreibungsfähigen Delikts nach dem Rahmenbeschluss 2002/584/JI.

23 Rahmenbeschluss des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedsstaaten, ABl. L 190 vom 18. Juli 2002, S. 1.

Die Erstanordnungsvoraussetzungen lagen im Übrigen bei allen zur Gefahrenabwehr und Strafverfolgung angeordneten Maßnahmen vor. Lückenhaft war jedoch die Dokumentation der nach sechs Monaten fälligen Aussonderungsprüfungen. Die datierten Einzelfallabwägungen wurden zwar nach Auskunft von Mitarbeiterinnen im Referat in Cottbus fristgerecht vorgenommen, dann jedoch an das für die Eintragung zuständige zentrale Referat beim Landeskriminalamt in Eberswalde übersandt. Nur wenn hiervon Kopien in den Akten vorhanden waren, konnten wir die Fristabläufe und den Inhalt der Prüfung einsehen. Eine zusätzliche Nachschau in Eberswalde war aus Kapazitätsgründen für uns zum gegebenen Zeitpunkt nicht möglich. In zwei Fällen konnten wir anhand der für die Überprüfung vermerkten Daten feststellen, dass sie erheblich verspätet erfolgte. Obwohl unsere inhaltliche Kontrolle ergab, dass auch zu dem späteren Zeitpunkt die Voraussetzungen für eine polizeiliche Beobachtung noch vorlagen, stellt die Fristverletzung aus unserer Sicht einen Datenschutzverstoß dar.

Bei Ausschreibungen von Personen Fristen wahren

Die Ausschreibungen zur Beobachtung anlässlich von polizeilichen Kontrollen zur Strafverfolgung nach § 163e StPO prüften wir darauf, ob das Anlassdelikt eine Straftat von erheblicher Bedeutung war, der bestehende Richtervorbehalt beachtet wurde, Aussonderungsprüfungen fristgemäß erfolgten und bei Verlängerungen die maximale Dauer von drei Monaten eingehalten wurde. Hier wurden alle formellen Voraussetzungen erfüllt und die Prüfungen waren vollständig dokumentiert.

Zur Überprüfung der Voraussetzungen der beiden Führungsaufsichtsfälle forderten wir bei der zentralen Führungsaufsichtsstelle beim Brandenburgischen Oberlandesgericht die Akten an. Im Vergleich zu den Ausschreibungen zur Gefahrenabwehr und Strafverfolgung können Ausschreibungen von verurteilten Straftäterinnen und Straftätern für die gesamte Dauer der Führungsaufsicht von der Aufsichtsstelle angeordnet werden. In den beiden von uns untersuchten Fällen hatte die zuständige Stelle eine Anordnung zur polizeilichen Beobachtung für die gesamte fünfjährige Führungsaufsicht beider Straftäter getroffen. Diese ist gemäß § 463a Absatz 2 Satz 4 StPO

mindestens jährlich auf ihre Erforderlichkeit zu überprüfen. Erstmalige und Folgeanordnungen waren in den Vorgängen dokumentiert.

Die angeordneten Ausschreibungen und damit die Eingriffe in das Persönlichkeitsrecht sind jedoch nur gerechtfertigt, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die betroffene Person eine entsprechend gewichtige Straftat begehen wird oder – im Fall einer repressiven Anordnung – begangen hat. Gründe können sich aus der Gesamtwürdigung der Person, den bisher begangenen Straftaten oder aus anderen Tatsachen ergeben und sind individuell zu prüfen. Die uns vorgelegten polizeilichen Antragsbegründungen legten in nachvollziehbarer Weise dar, weshalb eine polizeiliche Beobachtung plausibel und als erforderlich angesehen wurde, etwa, weil eine Person bereits mehrfach auf frischer Tat oder in der Nähe von Tatorten wegen einschlägiger Delikte angetroffen wurde oder es andere Spurentreffer oder Erkenntnisse gab. Um teilweise wechselnde beteiligte Personen einer Bande zuordnen zu können, war es erforderlich, die Beobachtung aufgrund des konspirativen Vorgehens der Banden und dem Mangel an Zeuginnen und Zeugen zu verlängern. Das planmäßig organisierte Vorgehen und Verbringen des Diebesgutes über die nationale Landesgrenze erklärte die Notwendigkeit einer Ausschreibung zur verdeckten Registrierung im Schengenraum.

In den Fällen der Ausschreibungen im Rahmen der Führungsaufsicht waren die entlassenen Sexualstraftäter wegen Straftaten von erheblicher Bedeutung (Vergewaltigung mit Körperverletzung, schweren sexuellen Missbrauchs von Kindern, Herstellung pornographischer Schriften) teilweise mehrfach verurteilt worden und mit unterschiedlichen Weisungen z. B. zu Aufenthaltsverboten an bestimmten Orten oder Kontaktverboten belegt worden. Zwar waren die Gründe in den Anordnungen der Führungsaufsichtsstelle nur formelhaft vorhanden, in dem sie in einem Vordruck angekreuzt wurden, aus dem Akteninhalt ergab sich jedoch nachvollziehbar, worauf die Einschätzung beruhte, dass die Maßnahme zur Überprüfung der Weisung erforderlich war. Der Aktenrückhalt enthielt Berichte und Informationen zur Persönlichkeit der Betroffenen, ihrem sozialen Umfeld, medizinische Bewertungen, Einschätzungen zur Rückfallprognose und polizeiliche Erkenntnisse. Auch die Ausschreibung über die Landesgrenzen Deutschlands hinaus war plausibel begründet, weil sich ein

ausländischer Betroffener mit ungesichertem Aufenthaltsstatus in Brandenburg aufhielt, eine Ausweisung drohte und er den angewiesenen Aufenthaltsort ohne Angaben von Gründen verlassen hatte. In dem anderen Fall hatte sich der Betroffene bereits zuvor grenzüberschreitend im Schengenraum aufgehalten, sodass auch dort die Gefahr der Begehung künftiger Straftaten bestand.

Schließlich überprüften wir stichprobenweise noch sogenannte Treffermeldungen, die bei Antreffen der Person an die ausschreibende Behörde verschickt werden. Dabei wurden keine datenschutzrechtlichen Defizite offenbar.

Insgesamt konnten wir in Brandenburg keine gravierenden Mängel bei der Kontrolle der ausgewählten Personenausschreibungen feststellen. Insbesondere ergaben sich wegen vorliegender Hintergrundinformationen und individuellen Antragsbegründungen aus den geprüften Vorgängen keine Hinweise auf unrechtmäßige Ausschreibungen von Personen zur polizeilichen Beobachtung. Wir stellten in zwei Fällen lediglich Fristüberschreitungen für die gesetzlich vorgesehenen Prüfungen zur weiteren Erforderlichkeit der Maßnahme fest und Dokumentationsmängel. Wir haben deshalb gegenüber den anordnenden Stellen klargestellt, dass eine rechtzeitige Befassung mit den Folgeanordnungen notwendig ist, um Prüffristen einzuhalten. Die getroffenen Abwägungsentscheidungen müssen vollständig dokumentiert werden. Erforderlich ist, dass die die Anordnung begründenden Tatsachen in jedem Einzelfall zusammengetragen werden, damit der Abwägungsprozess nachvollziehbar ist und nicht formelhaft reduziert wird.

3 Beratung einer Justizvollzugsanstalt zum Datenschutz

In Justizvollzugsanstalten werden große Mengen personenbezogener Daten der Gefangenen und Untergebrachten verarbeitet. Dazu gehören z. B. Daten zu religiösen Überzeugungen und sexuellen Neigungen ebenso wie Angaben zu gesundheitlichen Einschränkungen und Suchterkrankungen. Deren Verarbeitung greift teilweise tief in die Privatsphäre der betroffenen Personen ein. Ein sorgfältiger und

rechtskonformer Umgang mit diesen sensitiven Daten muss daher durch jede Justizvollzugsanstalt gewährleistet werden. Um uns einen Überblick über die entsprechende Datenverarbeitung zu verschaffen und mögliche Schwachstellen zu identifizieren, haben wir im Berichtszeitraum eine große Justizvollzugsanstalt besucht und mit den Verantwortlichen ausgewählte Aspekte der Einhaltung datenschutzrechtlicher und technischer Anforderungen erörtert.

Im Vorfeld forderten wir das Verzeichnis der Verarbeitungstätigkeiten gemäß § 24 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsgesetz an, um die vorhandenen Datenverarbeitungsprozesse kennenzulernen. Die Unterlagen wurden uns auch rechtzeitig vor unserem Besuch zur Verfügung gestellt. Zwar waren die verschiedenen Verarbeitungsprozesse anhand der Benennung gut zu identifizieren und voneinander abzugrenzen, jedoch erkannten wir zum Teil erheblichen Verbesserungsbedarf hinsichtlich der auf die konkreten Verarbeitungen bezogenen Angaben zu den Zwecken, den Kategorien von Daten, betroffenen Personen sowie Empfängerinnen und Empfängern und zu den technischen und organisatorischen Maßnahmen.

Im Rahmen eines Vor-Ort-Termins ließen wir uns zunächst die verschiedenen Prozesse zur Verarbeitung personenbezogener Daten von der Aufnahme einer betroffenen Person in die Anstalt über den Aufenthalt bis zur Entlassung erläutern. Anhand von Beispielen wurde uns die automatisierte Datenverarbeitung in dem bundesweit einheitlichen Fachverfahren Basis.WEB, mit dem elektronische Akten zu Gefangenen und Untergebrachten geführt werden, demonstriert. Die Vorgaben, welche Daten konkret verarbeitet werden, basieren auf dem Brandenburgischen Justizvollzugsgesetz bzw. dem Brandenburgischen Sicherungsverwahrungsvollzugsgesetz und sind in Basis.WEB implementiert. Weit umfangreicher als der Datensatz zu einer betroffenen Person in dem Fachverfahren ist jedoch die zugehörige Papierakte, die unter anderem auch Gutachten, Berichte und den Vollzugsplan enthält. Sie kann je nach Aufenthaltsdauer in der Anstalt auf eine zweistellige Anzahl von Bänden anwachsen.

Zugriffsrechte werden in Basis.WEB auf der Grundlage aufgaben- und funktionsbezogener Rollen differenziert vergeben. Umfassen-

de Rechte hat die Vollzugsgeschäftsstelle. Auch die Rolle des Allgemeinen Vollzugsdienstes ist weit gefasst und hat Zugriff auf die Datensätze aller Hafthäuser, da die entsprechenden Bediensteten in allen Hafthäusern tätig sind. Der Stationsdienst des Vollzugskrankenhauses hat eine eigene Rolle mit entsprechend getrennten Zugriffsrechten. Aus infrastruktureller Sicht konnten wir uns davon überzeugen, dass sich die zentrale Rechentechnik wie Server und Netzkomponenten in einem Neubau befindet, der allen modernen Anforderungen an die Gebäude- und Raumsicherheit genügt. Dies ist ein großer Fortschritt im Vergleich zu dem Zustand, der noch vor etwa 20 Jahren vorherrschte und zum damaligen Zeitpunkt von uns bemängelt wurde.

Während der Beratung stellten wir fest, dass das Thema Datenschutz sowohl auf Leitungsebene als auch bei den Mitarbeiterinnen und Mitarbeitern beachtet und ernst genommen wird. Allerdings besteht auch hier – wie in vielen anderen Bereichen – die Problematik, ungenügende personelle Ressourcen ausgleichen zu müssen. Dies hat zur Folge, dass einzelnen Bediensteten aufgrund der Vielzahl an Aufgaben mehrere Rollen in Basis.WEB mit teils sehr weit gefassten Rechten zugewiesen sind. Wir haben der Anstaltsleitung empfohlen zu prüfen, inwieweit hier Einschränkungen vorgenommen werden können, ohne den Arbeitsablauf zu behindern. Dabei haben wir auf den hohen Stellenwert des Grundrechts auf informationelle Selbstbestimmung hingewiesen. Außerdem haben wir die Schwachpunkte im Verzeichnis der Verarbeitungstätigkeiten erläutert und beispielhaft erklärt, wie es zu verbessern ist. Die Verantwortlichen haben zugesagt, unsere Hinweise umzusetzen.

Durch den Vor-Ort-Termin konnten wir einen informativen Einblick in die Arbeit einer Justizvollzugsanstalt gewinnen. Gravierende Defizite bei der Umsetzung des Datenschutzes wurden nicht festgestellt. Alle Beteiligten waren uns gegenüber aufgeschlossen, auskunftsbereit und konstruktiv. Sie brachten jedoch auch zum Ausdruck, dass sie sich mehr Austausch zum Thema Datenschutz mit anderen Justizvollzugsanstalten und insgesamt mehr Unterstützung durch das Ministerium der Justiz, dem sie nachgeordnet sind, wünschen. Dies würden auch wir begrüßen.

4 Datenschutz-Folgenabschätzungen bei der Polizei

Datenverarbeitungen bei der Polizei sind häufig mit hohen Risiken für die Rechtsgüter der betroffenen Personen verbunden. Derartige Verarbeitungen unterliegen deshalb besonderen Sorgfaltspflichten der Verantwortlichen, um jederzeit die Rechte und Freiheiten der betroffenen Personen zu gewährleisten. § 21 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsgesetz sieht hierfür das Instrument der Datenschutz-Folgenabschätzung vor, mit der Datenverarbeitungsvorgänge unter anderem auf ihre Risiken für die betroffenen Personen untersucht und wirksame technische und organisatorische Maßnahmen zu Abmilderung dieser Risiken ermittelt werden können. Bereits im Jahr 2020 haben wir einen ausführlichen Beitrag zu den Anforderungen, der allgemeinen Vorgehensweise für eine Datenschutz-Folgenabschätzung und dem damaligen Sachstand bei der Polizei Brandenburg veröffentlicht.[24]

Hohe Risiken – besondere Maßnahmen

Inzwischen haben die Verantwortlichen einen detaillierten Prozess entwickelt, um die erforderlichen Datenschutz-Folgenabschätzungen sowohl systematisch und ausreichend gründlich als auch für alle Beteiligten handhabbar durchführen zu können. Im Rahmen eines konstruktiven Austausches wurden die prozessualen und inhaltlichen Festlegungen auf Arbeitsebene mit unserer Behörde erörtert. Als grundsätzliches Problem zeigte sich dabei, dass es keine einheitliche Methodik zur Erstellung von Datenschutz-Folgenabschätzungen gibt und bislang auch konkrete Beispiele aus dem Bereich des polizeilichen Datenschutzes fehlen. Die Verantwortlichen haben daher eine eigene Handreichung für die Polizei Brandenburg erstellt, die sowohl bei der Anwendung der Datenschutz-Grundverordnung als auch der EU-Richtlinie 2016/680 (sog. JI-Richtlinie) und des oben genannten Gesetzes genutzt werden soll.

Im Verlauf unseres Austausches wurde eine Vielzahl von Einzelfragen diskutiert, die bei der Ausgestaltung des Prozesses zur Erstellung einer Datenschutz-Folgenabschätzung eine Rolle spielen – unter an-

24 Tätigkeitsbericht Datenschutz 2020, B.3.

derem zu der Schwellwertanalyse, der Risikomatrix, möglichen Standardrisikoszenarien sowie der Auswahl geeigneter und wirksamer technischer und organisatorischen Maßnahmen. Auch die digitale Unterstützung des Vorgehens wurde erörtert.

Kritisch sahen wir die Erstellung einer Positivliste mit Beispielen für polizeiliche Datenverarbeitungen, für die die Notwendigkeit einer Datenschutz-Folgenabschätzung bejaht wird. Aus unserer Sicht besteht dabei die Gefahr, dass der Prüfprozess, ob eine solche erforderlich ist, durch eine ausschließliche Fokussierung auf diese Beispiele zu schnell eingeengt und damit unzulässig verkürzt wird. Wir haben daher dafür plädiert, bei polizeilichen Datenverarbeitungen grundsätzlich immer von der Notwendigkeit einer Datenschutz-Folgenabschätzung auszugehen und eine Begründungspflicht vorzusehen, wenn von diesem Grundsatz abgewichen werden soll.

Als eine weitere Schwierigkeit wurde die Identifikation wirksamer Maßnahmen zu den ermittelten Risiken thematisiert. In diesem Zusammenhang wurde unter anderem besprochen, wie dem Risiko innerpolizeilicher unberechtigter Datenabfragen[25] entgegenzuwirken sei. Problematisch ist hierbei, dass dieses Risiko in der Regel nicht durch technische Maßnahmen eingedämmt werden kann und pauschale organisatorische Maßnahmen wie Sensibilisierungen und Belehrungen oftmals nicht die gewünschte Wirkung erzielen. Wir sehen daher eine kluge und bedarfsangepasste Kombination von Maßnahmen wie regelmäßige Belehrungen, verpflichtendes E-Learning über das interne Bildungsportal mit der Beantwortung von Fragen sowie die Ankündigung und Durchführung von Stichprobenkontrollen als eine Möglichkeit, das Risiko missbräuchlicher Datenabfragen zu mindern. Dieses Beispiel zeigt, wie kompliziert es sein kann, geeignete Maßnahmen zu finden, die tatsächlich auch auf die Risikoquelle einwirken.

Der Austausch mit den Verantwortlichen bei der Polizei Brandenburg ist noch nicht abgeschlossen und wird fortgeführt. Wir gehen davon aus, dass auch die genannte Handreichung weiterentwickelt wird, indem die Erfahrungen mit der Erstellung von Datenschutz-Folgenabschätzungen dort einfließen.

25 Tätigkeitsbericht Datenschutz 2021, A 4.4.

5 Meldepflicht bei Datenschutzverletzungen – neue Richtlinie für die Polizei

In unserem letzten Tätigkeitsbericht[26] hatten wir über Rechtsgrundlagen und Fallgruppen berichtet, die eine Meldepflicht von Datenschutzverletzungen an die Landesbeauftragte auslösen. Bei repressivem Tätigwerden der Polizei, wie z. B. Datenverarbeitung durch die Zentrale Bußgeldstelle, bestimmt sich die Meldepflicht in der Regel nach § 500 Strafprozessordnung i. V. m. § 65 Bundesdatenschutzgesetz, bei präventivem Tätigwerden nach § 29 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz. Nachdem wir mit den zuständigen Stellen bei der Polizei verschiedene Konstellationen aus uns bekannt gewordenen Fällen abgestimmt hatten, stellte uns die Polizei eine Richtlinie vor, die die Behandlung von Verletzungen der Sicherheit personenbezogener Daten in der Polizei Brandenburgs systematisiert und den Ablauf vom Erkennen einer möglichen Verletzung bis zur Meldung und Nachbereitung regelt.

Ziel dieser Richtlinie ist es auch, Ereignisse, die die Sicherheit von personenbezogenen Daten beeinträchtigen könnten, frühzeitig zu erkennen und effektive Gegenmaßnahmen zu ergreifen. Sie gilt für alle Polizeibehörden und -einrichtungen des Landes Brandenburg sowie deren Dienstleisterinnen und Dienstleister, soweit diese als Verantwortliche bzw. Auftragsverarbeiter personenbezogene Daten verarbeiten.

Die Richtlinie verlangt zunächst eine interne Sachverhaltsklärung, bevor die Verletzung an die Landesbeauftragte als Datenschutzaufsichtsbehörde gemeldet wird. Bei Verdacht einer Datenschutzverletzung wird mit Hilfe eines standardisierten Formulars eine interne Meldung an die zuständige behördliche Datenschutzbeauftragte bzw. den zuständigen behördlichen Datenschutzbeauftragten veranlasst. Für die Angehörigen der Polizei erläutert eine Anlage die Definition einer Verletzung der Sicherheit personenbezogener Daten und stellt klar, dass diese nicht von absichtlichem Tun herbeigeführt werden muss und sowohl durch technisches als auch menschliches Versagen entstehen kann. Zugleich werden typische meldepflichtige

26 Tätigkeitsbericht Datenschutz 2021, B 2.2.

Verletzungen beispielhaft aufgelistet. Durch das frühzeitige Erfassen und Informieren über ein Datenschutzproblem ist gewährleistet, dass die 72-Stunden-Frist bis zur Meldung an unsere Behörde in der Regel eingehalten werden kann.

Die oder der behördliche Datenschutzbeauftragte, die oder der im Falle einer behördenübergreifenden Beeinträchtigung oder eines hohen Risikos für Rechte Betroffener auch weitere Personen für ein Ad-hoc-Team einberufen kann, entscheidet, ob eine Meldepflicht besteht. Auch hierfür wurde ein standardisiertes Formular entworfen, das gewährleistet, dass keine wesentlichen Informationen vergessen werden und das sich inzwischen bereits mehrfach bei Meldungen bewährt hat. Die weitere Sachverhaltsaufklärung und Analyse der Verletzung der Sicherheit personenbezogener Daten erlaubt es, Sofortmaßnahmen zu veranlassen und im Anschluss unter Hinzuziehung von fachverantwortlichen Bereichen den Sicherheitsvorfall zu beheben. Die Richtlinie sieht auch vor, in diesem Schritt die für die Aufklärung notwendigen Daten zu sichern und die getroffenen Maßnahmen zu dokumentieren. Abschließend wird auch die Nachbereitung des Vorfalls geregelt, damit durch Korrektur- und Vorbeugemaßnahmen eine erneute Verletzung künftig vermieden werden kann.

Die am 1. Juni 2022 in Kraft getretene Richtlinie ist ein positives Beispiel dafür, wie allgemeine organisatorische Festlegungen helfen können, datenschutzrechtliche Vorschriften – wie die rechtzeitige und vollständige Meldung einer Datenschutzverletzung – einzuhalten. Durch klar strukturierte Abläufe und Hilfestellungen für die Daten verarbeitenden Beamtinnen und Beamten in Form von Checklisten, Kontakten von Ansprechpersonen und Formularen wird nicht nur das Bewusstsein für Verletzungen des Datenschutzes geschult, sondern auch die Schritte zu einer fristgerechten Meldung erleichtert. Der offene Umgang mit solchen Vorfällen und ihrer Aufarbeitung dürfte auch möglichen Vertuschungstendenzen entgegenwirken. Nach unserer Einschätzung ist dies ein gelungener Beitrag zum Datenschutzmanagement und für mehr Datensicherheit innerhalb der Polizei.

6 Zahlen und Fakten

Im Berichtszeitraum konnten wir einen Rückgang an schriftlichen Beschwerden über Datenverarbeitungen durch Staatsanwaltschaften und die Polizei verzeichnen. Insgesamt erreichten uns 27 Beschwerden betroffener Personen und 8 Anfragen öffentlicher Stellen. Sie bezogen sich – bis auf zwei Fälle – auf die Polizeibehörden des Landes. Neben E-Mails und Briefen nutzten Betroffene zunehmend die Möglichkeit, sich über das Beschwerdeformular in unserem Internetangebot an uns zu wenden. Zugenommen haben dagegen die Anfragen von Bürgerinnen und Bürgern, die sich telefonisch an uns wandten. Insgesamt wurden wir 37 Mal telefonisch um Erläuterungen zu datenschutzrechtlichen Bestimmungen, Auskunftsrechten, Speicherdauer, Löschfristen und Ad-hoc-Beurteilungen von polizeilichem Datenerhebungsmaßnahmen gebeten. Dies führte jedoch nicht zur Eröffnung eines Verwaltungsvorgangs. Die Zahl der Meldungen von Datenschutzverletzungen reduzierte sich geringfügig von 8 im Vorjahr auf 7 im Berichtszeitraum.

Zugleich standen wir mündlich wie schriftlich in einem intensiven Austausch mit dem Ministerium des Innern und für Kommunales und verantwortlichen Organisationseinheiten im Polizeipräsidium. Dabei verfassten wir Stellungnahmen zu zwei Gesetzentwürfen sowie einer Richtlinie und führten vor Ort oder telefonisch Gespräche mit Vertreterinnen und Vertretern von Ministerium sowie Polizei. Insgesamt wurden wir 11 Mal im Zuge von Gesetzgebungsvorhaben und Verwaltungsmaßnahmen beratend tätig. Fünf Besprechungen fanden ausschließlich zur Umsetzung von technisch-organisatorischen Maßnahmen statt.

Im Berichtszeitraum hat die Landesbeauftragte gegenüber Polizei und Staatsanwaltschaften weder Warnungen oder Beanstandungen nach dem Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz ausgesprochen, noch von Abhilfebefugnissen gemäß der Datenschutz-Grundverordnung Gebrauch gemacht.

Teil C: Die Dienststelle

1 Öffentlichkeitsarbeit

In jedem Jahr führt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder anlässlich des Europäischen Datenschutztages eine zentrale Veranstaltung durch. Im Berichtsjahr konnte sie pandemiebedingt erneut ausschließlich online durchgeführt werden. Die Veranstaltung fand am 28. Januar 2022 statt und stand unter der Überschrift: „Die digitale Brieftasche in der EU – Datenschutz-Albtraum oder Meilenstein für die Gestaltung der digitalen Zukunft Europas?“. Hintergrund war ein europäisches Vorhaben, das vorsieht, den Bürgerinnen und Bürgern eine europaweit nutzbare digitale Brieftasche („wallet“) zur Verfügung zu stellen. Diese soll offizielle Ausweisfunktionen haben und zusätzlich durch Verknüpfung mit weiteren persönlichen Attributen, wie Führerschein, Ausbildungsnachweis oder Bankkonto, die Grundlage einer europäischen digitalen Identität bilden. Gäste aus Zivilgesellschaft, Behörden und Wissenschaft diskutierten die datenschutzrechtlichen Implikationen dieser Planungen. Ausgerichtet wurde die Veranstaltung von der saarländischen Landesbeauftragten für Datenschutz und Informationsfreiheit im Namen der Konferenz.

Durch die im Laufe des Berichtsjahres wesentlich reduzierten Maßnahmen zur Eindämmung der Corona-Pandemie hat auch die Nachfrage nach Informationen über einen datenschutzgerechten Umgang damit nachgelassen. Die häufig gestellten Fragen zur Erhebung der Kontaktdaten sowie das entsprechende Musterformular haben wir bis zur Beendigung der Maßnahmen regelmäßig aktualisiert. Drei Faltblätter hat die Landesbeauftragte umfassend überarbeitet und in einer Neuauflage herausgegeben: Das Faltblatt „Datenschutz und Akteneinsicht in Brandenburg“ stellt unsere Aufgaben sowie die Behörde und ihre Befugnisse kurz und übersichtlich dar. Zwei weitere, aktualisierte Faltblätter enthalten praktische Tipps und Hinweise zum sicheren Löschen von Festplatten („Verräterische Spuren auf Datenträgern“) sowie zum Selbstdatenschutz am eigenen Rechner und im Internet („Digitale Angriffe? Nicht bei mir!“). Die Handreichung zur Meldung von Datenschutzschutzverletzungen in Brandenburg sowie zu den technischen und organisatorischen Maßnahmen zur Umsetzung des Datenschutzes bei Heimarbeit haben wir ebenfalls auf den neuesten Stand gebracht. Die zuvor teilweise uneinheitliche

Optik auch weiterer Veröffentlichungen konnten wir entsprechend dem behördlichen Design anpassen. Wichtiger noch war es uns jedoch, nicht nur die aktuell herausgegebenen, sondern auch Handreichungen und Broschüren aus den Vorjahren im PDF-Format weitgehend barrierefrei anbieten zu können. Letzteres bedurfte sowohl einer rechtlichen und technischen Einarbeitung in die Grundlagen der Barrierefreiheit als auch einer zeitaufwändigen Aufbereitung der entsprechenden Veröffentlichungen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder veröffentlicht zahlreiche Orientierungshilfen und Anwendungshinweise zu wichtigen Fragen der Umsetzung des Datenschutzes sowohl in rechtlicher als auch in technisch-organisatorischer Hinsicht. Im Rahmen ihrer Mitgliedschaft in der Konferenz ist auch die Landesbeauftragte hieran beteiligt. Im Berichtszeitraum verabschiedeten die Datenschutzbeauftragten eine Orientierungshilfe zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung. Mit einer Liste häufig gestellter Fragen (und natürlich Antworten) zum Betrieb von Facebook-Fanpages erläuterte die Konferenz unter anderem, warum dieser datenschutzrechtlich problematisch ist und warum Verantwortliche in der aktuellen Situation den Datenschutz nicht gewährleisten können. Die genauen rechtlichen Probleme hat sie parallel in einem Kurzgutachten dargestellt. Im Anschluss an die Veröffentlichung der Orientierungshilfe Telemedien im Jahr 2021 hat die Datenschutzkonferenz ein öffentliches Konsultationsverfahren eingeleitet. Nach dessen Auswertung nahm sie Anpassungen und Ergänzungen vor und verabschiedete im Berichtsjahr die aktuelle Version der „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021“. Außerdem hat die Konferenz eine neue, inhaltlich ergänzte Version des Standard-Datenschutzmodells herausgegeben.

Neben den Papieren der Datenschutzkonferenz hat die Landesbeauftragte im laufenden Berichtsjahr auch wieder die neuen, vom Europäischen Datenschutzausschuss verabschiedeten Leitlinien in ihrem Internetangebot veröffentlicht. Die Leitlinien bezwecken die Förderung eines gemeinsamen Verständnisses der EU-Datenschutzvorschriften. Im Jahr 2022 hatten sie Verhaltensregeln als Instrument für Übermittlungen in Drittstaaten, die Anwendung des Artikels 60

Datenschutz-Grundverordnung sowie die praktische Anwendung der gütlichen Einigung zum Inhalt. Üblicherweise erscheinen diese Dokumente des Europäischen Datenschutzausschusses zunächst in englischer Sprache und werden nach ihrer Veröffentlichung in andere Sprachen der Europäischen Union übersetzt. Wir sind bestrebt, die deutsche Übersetzung zur Verfügung zu stellen, sobald sie vorliegt.

2 Pressearbeit

Nachdem die Pflicht zur Corona-Kontaktdatenerhebung weitgehend entfallen war, wies die Landesbeauftragte im Februar 2022 mit einer Presseinformation darauf hin, dass die Kontaktnachweise nach einer vierwöchigen Aufbewahrungsfrist datenschutzgerecht zu vernichten oder zu löschen waren. Sie informierte in diesem Zusammenhang über Möglichkeiten, die Nachweise gemäß den Vorschriften zu entsorgen.

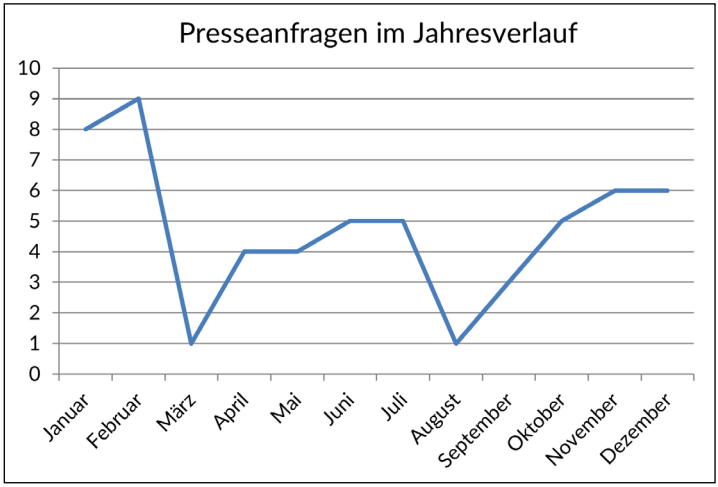
Das 30jährige Bestehen der Datenschutzaufsicht in Brandenburg nahmen wir im März 2022 zum Anlass, gegenüber Journalistinnen und Journalisten ein Resümee der bisherigen Entwicklungen auf dem Gebiet des Datenschutzes zu ziehen. Die Landesbeauftragte betonte die Herausforderungen, aber auch die Chancen, die sich aus der umfassenden Digitalisierung des Alltags für uns alle ergeben. Insbesondere stellte sie die Bedeutung der IT-Sicherheit in den Mittelpunkt.

Ebenso wie andere deutsche Datenschutzaufsichtsbehörden gingen wir im April 2022 davon aus, dass Behörden, die Facebook-Fanpages betreiben, einen datenschutzgerechten Betrieb nicht nachweisen können. Die Landesbeauftragte forderte zunächst die obersten Landesbehörden auf, ihrer Vorbildfunktion gerecht zu werden und entsprechende Auftritte abzuschalten. Gleichzeitig informierte sie über die Fortsetzung ihrer Aufsichtstätigkeit in Sachen Fanpages.

Am Tag der Übergabe des Tätigkeitsberichts Datenschutz 2021 an die Präsidentin des Landtags Brandenburg am 9. Mai 2022 stellte sie ihren Bericht der Öffentlichkeit im Rahmen einer hybriden Pressekonferenz vor. Sie informierte in einer ausführlichen Presseinformation über die wichtigsten Entwicklungen der Datenschutzpraxis

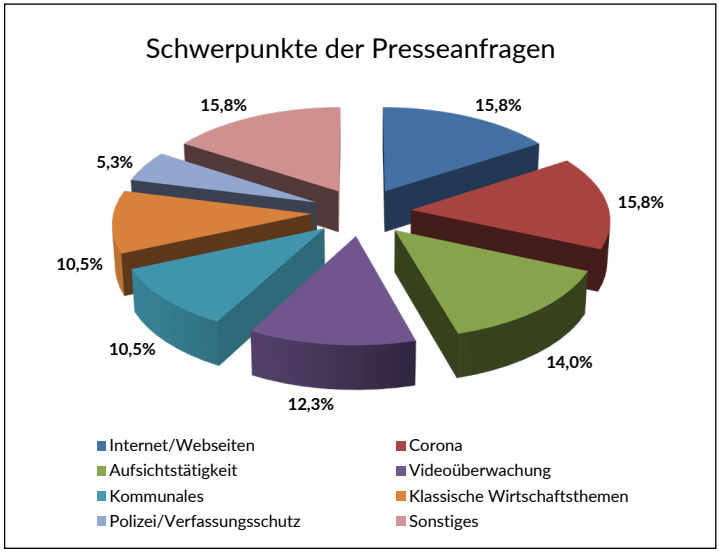
in Brandenburg sowie über herausragende Fälle, mit denen wir im Berichtsjahr befasst waren.

Im Berichtszeitraum haben wir 57 Medienanfragen zum Datenschutz beantwortet. Das entspricht knapp der Vorjahreszahl (60). Zeitlich betrachtet häuften sich die Anfragen in den beiden ersten und letzten Monaten des Jahres 2022. Während sich die Medien im Vorjahr noch zu gleichen Anteilen für die Datenverarbeitung durch öffentliche Stellen und private Unternehmen interessiert hatten, verschob sich das Interesse im Berichtsjahr wesentlich hin zu den Unternehmen.



Der inhaltliche Schwerpunkt der Anfragen lag im Jahr 2021 noch bei Datenschutzthemen im Zusammenhang mit der Corona-Pandemie. Hierzu erreichte uns im Berichtsjahr die letzte Anfrage bereits Ende Februar. Ein klarer Themenschwerpunkt des journalistischen Interesses ist über den Jahresverlauf indes nicht zu erkennen. Neben dem schnell schwindenden Interesse an coronabezogenen Themen bezogen sich viele Fragen auf den Datenschutz im Internet, auf die Videoüberwachung und auf Einzelfälle aus den Kommunen. Auch klassische Wirtschaftsthemen wie Adresshandel oder Datenschutz

bei Versicherungen waren von Belang. Weiterhin erhielten wir Anfragen zu unserer Aufsichtstätigkeit, die beispielsweise auf statistische Angaben zu den Sanktionsmaßnahmen zielten.



Bei der Verteilung der anfragenden Medien zeichnet sich eine Tendenz zu mehr Nachfragen von Online-Medien ab. Im Vorjahr betrug deren Anteil an den gesamten Anfragen noch 8 %; immerhin 53 % stammten von Zeitungen oder Zeitschriften. Im Berichtsjahr stellten die Anfragen der Online-Medien bereits 19 %, jene der Print-Medien reduzierte sich auf 42 %.

Die regionale Herkunft der Anfragen ist im Vorjahresvergleich relativ unverändert: Knapp 60 % der Anfragen stammen aus den Ländern Brandenburg oder Berlin, ein Drittel aus anderen Bundesländern oder von überregional tätigen Medien und knapp ein Zehntel der Anfragen werden von internationalen Medien gestellt. Für diese steht die Aufsichtstätigkeit der Landesbeauftragten im Hinblick auf solche Themen im Vordergrund des Interesses, die aktuell auch in anderen Mitgliedstaaten der Europäischen Union eine Rolle spielen.

3 Personal und Organisation der Dienststelle

Wie bereits in den Vorjahren war auch im Berichtszeitraum die Personalsituation der Dienststelle sehr angespannt. Einerseits waren neu bewilligte Stellen zu besetzen, andererseits mussten mehrere Personalweggänge und Elternzeiten kompensiert werden. Die aktuelle Arbeitsmarktsituation mit einer äußerst begrenzten Verfügbarkeit qualifizierten Personals hat unsere Suche erheblich erschwert.

Die im Bereich Verwaltung dringend benötigte und bereits im Jahr 2021 für den Berichtszeitraum bewilligte Stelle einer IT-Systemkoordinatorin oder eines IT-Systemkoordinators konnte trotz mehrfach wiederholter Ausschreibungen weiterhin nicht besetzt werden. Eine mögliche Lösung deutete sich nach Redaktionsschluss dieses Berichts an. Darüber hinaus konnte durch den Ruhestand eines Mitarbeiters und eine interne Umorganisation eine Stelle für den IT-Sicherheitsbeauftragten der Dienststelle vorgesehen und ausgeschrieben werden. Auch diese wird voraussichtlich Anfang des Jahres 2023 besetzt. Die temporären Vakanzen führten zu einer erheblichen Arbeitsverdichtung und der Verzögerung wichtiger Projekte im Bereich Verwaltung.

Im Bereich Technik und Organisation waren zwei Weggänge von Stelleninhabern auszugleichen. In einem Fall gelang dies bereits im ersten Quartal. Für die Nachbesetzung der zweiten offenen Stelle benötigten wir erneut mehrere Anläufe. Gerade für diese Stelle war es besonders kompliziert, eine geeignete Nachfolge zu finden. Ihr sind schwerpunktmäßig Fragen der Verwaltungsdigitalisierung und des E-Government sowie darüber hinaus die Leitung eines Arbeitskreises der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sowie die Mitwirkung in einer Arbeitsgruppe der europäischen Datenschutzaufsichtsbehörden zugeordnet. Vor diesem Hintergrund konnte die Beratungstätigkeit zu Fragen der Umsetzung des Onlinezugangsgesetzes im Berichtsjahr nur teilweise und mit großer Mühe fortgesetzt werden.

Auch im Bereich Recht und im Justiziariat meiner Dienststelle hatten wir für die Besetzung mehrerer offener Stellen zu sorgen. In einem Fall gelang die Nachbesetzung innerhalb weniger Monate. Nach dem

Weggang eines Gruppenleiters konnten wir auch dessen Nachfolge im Ergebnis einer Ausschreibung hausintern mit einer Mitarbeiterin des Justiziariats zwar noch sicherstellen. Die im weiteren Verlauf daraus entstandenen Lücken ließen sich jedoch nicht mehr in vollem Umfang schließen. Die fehlenden personellen Ressourcen im Justiziariat haben zur Folge, dass Bußgeldverfahren zum Teil erst mit zeitlicher Verzögerung oder nicht in der gebotenen Geschwindigkeit bearbeitet werden können. Gleiches gilt für den Bereich Recht der Dienststelle. Die bestehenden Personallücken führen dazu, dass Aufgaben manchmal liegenbleiben bzw. nicht in der gewünschten Tiefe bearbeitet werden.

Die Geburt eines Kindes ist an sich ein schöner Anlass und die Möglichkeit der Elternzeit familienpolitisch sehr zu begrüßen. Mutterschutz und Elternzeit bedeuten für eine kleine Dienststelle allerdings immer eine besondere organisatorische Herausforderung. Im Berichtsjahr waren insgesamt drei Elternzeiten zu kompensieren. Während ich zwei Vertretungen erfolgreich besetzen konnte, ließ sich für eine weitere Stelle trotz mehrfacher Ausschreibung kein Ersatz finden. Neben den oben schon erwähnten Problemen bei der Gewinnung von Fachpersonal kommt hier noch die zeitliche Befristung der Vertretung zum Tragen.

An dieser Stelle möchte ich mich ausdrücklich bei meinen engagierten Mitarbeiterinnen und Mitarbeitern in allen Bereichen bedanken, die erhebliche Mehrarbeit geleistet haben, um die entstandenen personellen Lücken zu füllen. Dies kann jedoch nur eine Übergangslösung sein. Auf lange Sicht, darf die wichtige Arbeit für den Datenschutz nicht von persönlichem Engagement abhängen, sondern muss auf einer nachhaltigen und belastbaren personellen Grundlage basieren, die eine gleichmäßige Verteilung der Arbeit ermöglicht. Der herrschende Fachkräftemangel und die zusätzliche Konkurrenz mit den Verwaltungen des Bundes und des Landes Berlin um qualifizierte IT- und Verwaltungsfachkräfte sowie Juristinnen und Juristen erschweren die Personalgewinnung inzwischen jedoch dauerhaft.

Wie bereits im Vorjahr hat sich die räumliche Situation meiner Dienststelle – nicht zuletzt aufgrund des Personalzuwachses – weiter verschlechtert. Die Sanierung eines Gebäudes auf der von mei-

ner Behörde genutzten Liegenschaft in Kleinmachnow steht erst in einigen Jahren in Aussicht. Nachdem ich vorhandene Besprechungs- und Funktionsräume in Büros umwandeln lassen musste, ist es zwar gelungen, in diesem Gebäude einen Besprechungsraum anzumieten. Für längere Beratungen, insbesondere mit Gästen, fehlt jedoch die erforderliche Infrastruktur. Auch sind die auf drei Häuser verteilten Büros meiner Mitarbeiterinnen und Mitarbeiter allesamt weiterhin nicht barrierefrei zugänglich.

Für die Haushaltsjahre 2023 und 2024 bewilligte der Landtag Brandenburg noch einmal vier dringend benötigte Stellen. So hoffe ich, eine Sekretariatskraft einstellen zu können, die zur Entlastung der Referentinnen und Referenten beitragen und Unterstützungsarbeiten nach der Einführung der E-Akte in meinem Haus leisten soll. Zwei weitere Stellen sollen sowohl für den Bereich Recht als auch den Bereich Technik und Organisation auf dem Arbeitsgebiet Wirtschaft unterstützen. Außerdem wird das Justiziariat zu verstärken sein. Lösungen für die sich hierdurch voraussichtlich noch verschärfenden räumlichen Probleme sind nicht in Sicht.

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