Landesbeauftragte
für Datenschutz
und Akteneinsicht

Tätigkeitsbericht 2020
Datenschutz

Titelbild

Motiv: Stadtbibliothek Luckenwalde
Fertigstellung: 2008

Bildrechte: imago images / Rainer Weisflog

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 2020

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 2020 ab.

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

Vorwort

Liebe Leserinnen, liebe Leser,

das Jahr 2020 wird in unserer Erinnerung lange mit der Corona-Pandemie verbunden bleiben – und damit als eine Zeit massiver Grundrechtseinschränkungen. Betroffen war auch das Grundrecht auf informationelle Selbstbestimmung. Gaststätten, Veranstalter und Behörden wurden verpflichtet, die Daten ihrer Gäste zu erfassen, um im Fall einer bestätigten Infektion Gesundheitsämtern die Nachverfolgung von Kontakten zu ermöglichen. Weitere Befugnisse zur Verarbeitung personenbezogener und oftmals gesundheitsrelevanter Daten wurden geschaffen oder angepasst, um die Pandemie zu bekämpfen.

Aber auch pragmatische Lösungen der Unternehmen und Behörden, die insbesondere während der ersten Welle der Pandemie im Frühjahr 2020 sehr schnell und ohne die Gelegenheit einer Vorbereitung gefunden werden mussten, stellten sich als enorme Herausforderung für den Datenschutz dar. Im Vordergrund standen dabei digitale Vorhaben, beispielsweise die Heimarbeit der Beschäftigten in Wirtschaft und Verwaltung, das Distanzlernen an den Schulen sowie Online-Veranstaltungen der Hochschulen. Meine Mitarbeiterinnen und Mitarbeiter mussten in diesem Zusammenhang sowohl zahlreiche Beschwerden über Verstöße gegen den Datenschutz bearbeiten als auch Beratungen leisten und Fragen zu den vielen rechtlichen und technisch-organisatorischen Fragen beantworten. Um Verantwortliche zu sensibilisieren und dadurch die Akzeptanz in der Bevölkerung zu erhöhen, hat meine Behörde eine umfangreiche Kontrolle des Umgangs mit den Kontaktnachweisen durch brandenburgische Cafés und Restaurants durchgeführt. Die Ergebnisse sowohl unserer Kontrollen als auch der Beratungen zeigen, dass die datenschutzgerechte Gestaltung der digitalen Verfahren, die im Berichtsjahr ad hoc aufgesetzt werden mussten, eine Daueraufgabe bleiben wird. Die vielfältigen Aufgaben, die der brandenburgischen Datenschutzaufsicht im Zusammenhang mit der Corona-Pandemie zukamen, stelle ich in meinem Tätigkeitsbericht Datenschutz 2020 als Schwerpunktthema dar.

Darüber hinaus war das Berichtsjahr von Gesetzgebungsverfahren mit erheblicher datenschutzrechtlicher Tragweite geprägt, die ebenfalls Eingang in meinen Tätigkeitsbericht gefunden haben. Auch hier stand die Digitalisierung im Fokus. Beispielsweise hat der Bundesgesetzgeber mit dem Patientendaten-Schutz-Gesetz den Grundstein für die zügige Einführung einer elektronischen Patientenakte gelegt, dabei jedoch der Geschwindigkeit den Vorzug vor einer gründlichen Umsetzung des Datenschutzes gegeben. Ebenfalls deutliche Auswirkungen für die Brandenburgerinnen und Brandenburger wird das noch im Herbst 2020 in den Bundestag eingebrachte Registermodernisierungsgesetz haben. Im kritischen Blick der Datenschutzaufsichtsbehörden – auch meiner Kolleginnen und Kollegen aus Bund und Ländern – steht hier die geplante Einführung einer zentralen Identifikationsnummer für jede Bürgerin und jeden Bürger.

Meine Behörde ist bestrebt, Probleme durch Beratungen bereits im Vorfeld zu vermeiden, gleichwohl kam ich aber auch im Jahr 2020 wieder nicht umhin, meine gesetzlich vorgesehenen Aufsichtsbefugnisse auszuüben. Ihr Augenmerk möchte ich auf die vielen Beschwerden, Hinweise und Meldungen richten, denen meine Mitarbeiterinnen und Mitarbeiter in ihrer täglichen Arbeit nachgegangen sind. Von der Kennzeichenerfassung auf Autobahnen und der Videoüberwachung über die mangelnde Verschlüsselung digitaler Kommunikation bis hin zu unzureichenden Auskünften über die Verarbeitung der eigenen personenbezogenen Daten reicht die Spannbreite der Themen, die ich in meinem Bericht darstelle. Besonders prägten die zahlreichen Meldungen von Datenschutzverletzungen – sogenannter Datenpannen – meine Arbeit. Sie zeigen die klassischen Schwachstellen bei der Verarbeitung personenbezogener Daten auf, sei es die schlichte Unachtsamkeit bei der offenen Verwendung von E-Mail-Verteilern oder die fahrlässige Unkenntnis notwendiger technisch-organisatorischer Maßnahmen. Im Ergebnis verdeutlichen sie,

dass ein wirksamer Datenschutz in einer digitalen Umgebung nicht ohne Datensicherheit möglich ist.

Ich wünsche Ihnen wieder eine interessante Lektüre meines Tätigkeitsberichts Datenschutz 2020.

Dagmar Hartge

Teil A: Bericht nach Art. 59 Datenschutz-Grundverordnung

I Schwerpunkt: Datenschutz während der COVID-19-Pandemie

1 Die Corona-Verordnungen der Landesregierung

Im März 2020 erließ die Landesregierung auf der Grundlage des Infektionsschutzgesetzes die SARS-CoV-2-Eindämmungsverordnung. Im weiteren Verlauf der Pandemie, genauer gesagt im Juni 2020, entstand daraus die später mehrfach geänderte SARS-CoV-2-Umgangsverordnung. Schließlich trat im Zusammenhang mit der erneuten Verschärfung der Maßnahmen gegen die Ausbreitung des Corona-Virus im Dezember 2020 erneut eine angepasste SARS-CoV-2-Eindämmungsverordnung in Kraft. Beim Erlass der Maßnahmen zum Infektionsschutz waren auch Datenschutzaspekte zu berücksichtigen.

Bereits die erste SARS-CoV-2-Eindämmungsverordnung vom 17. März 2020 sah vor, die Daten der Teilnehmerinnen und Teilnehmer von Veranstaltungen zu registrieren. Sie verpflichtete die Verantwortlichen, in einer Anwesenheitsliste mindestens den Vor- und Familiennamen, die vollständige Anschrift sowie die Telefonnummer zu erfassen. Die Listen waren vier Wochen nach dem Ende der Veranstaltung aufzubewahren und dem zuständigen Gesundheitsamt auf Verlangen vollständig auszuhändigen. Mithilfe der Daten sollten im Fall einer später nachgewiesenen Infektion einer Besucherin oder eines Besuchers deren bzw. dessen Kontakte nachverfolgt werden, um mögliche Infektionsketten zu unterbrechen. Im Zuge der späteren Wiedereröffnung von Gaststätten war vorgesehen, auch diese zum Führen solcher Anwesenheitslisten zu verpflichten.

Die beschriebene Regelung war datenschutzrechtlich aus verschiedenen Gründen problematisch. Schließlich ermittelten die Gesundheitsämter schon aus Zeitgründen den betroffenen Personenkreis nicht mithilfe postalischer Schreiben. Die Nachverfolgung geschah vielmehr telefonisch oder per E-Mail. Es genügte daher vollkommen, neben den Vor- und Familiennamen die Telefonnummern oder die E-Mail-Adressen der Anwesenden zu erfassen. Die Angabe der Anschrift war nicht erforderlich, ihre Erhebung in dieser Weise folglich mit dem Datenschutzrecht nicht vereinbar. Wir waren zudem der Auffassung, dass der Verzicht auf unnötige Angaben das Missbrauchspotenzial der Anwesenheitslisten reduziert und die Akzeptanz durch die betroffenen Personen erhöht.

Das zuständige Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz teilte unsere Auffassung und legte in der SARS-CoV-2-Umgangsverordnung vom 12. Juni 2020 fest, dass nur noch der Vor- und Familienname sowie die Telefonnummer oder die E-Mail-Adresse zu erfassen waren. Zusätzlich verpflichtete die Verordnung die Verantwortlichen, zu verhindern, dass betroffene Personen Kenntnis von den personenbezogenen Daten anderer Betroffener erhalten. Die Anwesenheitsliste war unter Einhaltung datenschutzrechtlicher Vorschriften aufzubewahren und musste – sofern das zuständige Gesundheitsamt nicht seine Herausgabe verlangte –nach Ablauf einer Aufbewahrungsfrist von vier Wochen vernichtet bzw. die Daten gelöscht werden.

Im Verlauf der Umsetzung der SARS-CoV-2-Umgangsverordnung stellte sich auch die Verwendung des Begriffs „Anwesenheitsliste“ als problematisch heraus. Insbesondere ließ sich die neue Regelung, nach der einerseits weiterhin Listen zu führen waren, andererseits die Kenntnisnahme ihres Inhalts durch andere Betroffene verhindert werden sollte, kaum vernünftig umsetzen. Auch stellte sich die Frage, wie die Einhaltung der Löschfrist gewährleistet werden soll, wenn sich auf einer Liste Eintragungen mehrerer Tage oder gar Wochen finden. Die Frist muss sich dann nach dem zuletzt eingetragenen Datensatz richten. Dies bedeutet, dass die zuvor aufgenommenen Daten länger als vier Wochen gespeichert bleiben. Nicht zuletzt verzeichnete die Landesbeauftragte zahlreiche Anfragen und Beschwerden, die sich auf den Umgang mit den Anwesenheitslisten richteten.

Diesen Bedenken trug die Landesregierung mit der Zweiten Verordnung zur Änderung der SARS-CoV-2-Umgangsverordnung vom 11. August 2020 Rechnung. Darin ersetzte sie den Begriff der „Anwesenheitsliste“ durch den des „Anwesenheitsnachweises“. Sie stellte damit klar, dass die Datenerfassung auf einzelnen Blättern bzw. mittels Einzelerhebungen erfolgen sollte.

Später erreichten uns Beschwerden und Hinweise, die sich auf die Zweckentfremdung der im Rahmen des Anwesenheitsnachweises erfassten Daten richteten. In Einzelfällen haben Verantwortliche die

Daten beispielsweise zu eigenen Werbezwecken verwendet.[1] Zwar ergab sich die Unzulässigkeit dieses Vorgehens bereits aus allgemeinen datenschutzrechtlichen Grundsätzen; eine ausdrückliche Regelung in der Verordnung wäre jedoch hilfreich gewesen.

Mit der Vierten Verordnung zu Änderung der SARS-CoV-2-Umgangsverordnung vom 8. Oktober 2020 reagierte die Landesregierung auch darauf. Sie stellte ausdrücklich klar, dass Verantwortliche die Anwesenheitsnachweise ausschließlich zum Zweck der Auskunftserteilung gegenüber dem zuständigen Gesundheitsamt nach infektionsschutzrechtlichen Vorschriften nutzen darf.

Insgesamt bleibt festzuhalten, dass das Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz neben dem primären Ziel des Infektionsschutzes auch die datenschutzrechtlichen Belange der betroffenen Personen im Auge behielt. Nur wenn sichergestellt ist, dass deren Angaben nicht missbraucht oder zweckentfremdet werden, kann mit ihrer Bereitschaft gerechnet werden, personenbezogene Daten korrekt und vollständig anzugeben. Eine effektive Nachverfolgung von Infektionsketten hängt somit vom Vertrauen der Betroffenen ab – in diesem Sinne ist Datenschutz auch Infektionsschutz.

2 Überprüfung der Kontaktdatenerhebung bei Cafés und Restaurants in Brandenburg

Im Zusammenhang mit der Wiedereröffnung der Gastronomiebetriebe im Land Brandenburg am 15. Mai 2020 nach ihrer pandemiebedingten Schließung wurde den Betreiberinnen und Betreibern vorgegeben, die Kontaktdaten ihrer Gäste zu erheben. Zweck dieser Regelung war es, den Gesundheitsämtern die Nachverfolgung von Kontakten im Falle einer festgestellten Infektion mit dem Erreger SARS-CoV-2 zu ermöglichen.

Bei der Erfassung der Kontaktdaten war insbesondere zu verhindern, dass betroffene Personen oder Dritte Kenntnis von personenbezogenen Daten anderer Gäste erhielten. Uns erreichten diesbezüglich wiederholt Hinweise und Beschwerden, wonach verantwortliche

1 siehe A I 2

Stellen offen ausliegende Listen führen würden, in welche sich die Gäste eintragen sollten, sodass ein unberechtigter Zugriff auf personenbezogene Daten anderer Gäste möglich gewesen sei. Um die Einhaltung datenschutzrechtlicher Bestimmungen zum Schutz der betroffenen Personen in den Gaststättenbetrieben sicherzustellen, führten wir im August des Berichtsjahres Kontrollen bei über 50 Betrieben im Land Brandenburg durch. Hierbei stellten wir in 30 Fällen fest, dass zu viele Daten erhoben wurden. So wurde häufig nach der Anschrift gefragt, obgleich deren Erfassung nach der zu diesem Zeitpunkt geltenden Verordnung gar nicht hätte erfolgen dürfen. Auch erkannten viele Gastwirtinnen und -wirte nicht, dass entweder die Telefonnummer oder die E-Mail-Adresse anzugeben war, nicht aber beides.

Hervorzuheben ist an dieser Stelle auch die vorgegebene Aufbewahrungsfrist. Die erfassten Kontaktdaten waren für die Dauer von vier Wochen aufzubewahren und sodann zu vernichten bzw. zu löschen. In 36 Fällen wurde diese Löschpflicht nicht rechtzeitig, in 16 davon überhaupt nicht umgesetzt. In 11 Fällen wurden offen einsehbare Listen geführt. Dabei dient der sorgsame Umgang mit den Daten der Gäste nicht allein dem Schutz dieser Informationen, er schafft auch das nötige Vertrauen, damit Gäste richtige und vollständige Angaben machen. Diese wiederum sind notwendig, um den Gesundheitsbehörden im Bedarfsfall die Kontaktnachverfolgung und damit die Unterbrechung von Infektionsketten erst zu ermöglichen.

In allen Fällen nahmen die Betreiberinnen und Betreiber unsere Hinweise auf und sicherten eine Umstellung der Praxis zu. Ursächlich für die festgestellten Verstöße war häufig die Unsicherheit, wie mit den Daten umzugehen ist und welche Vorgaben überhaupt gelten würden. Hierfür stellten wir Muster und Erläuterungen auch in unserem Internetangebot zur Verfügung.

Werbung dank Corona-Listen?

In einem Fall stellten wir fest, dass die erhobenen Kontaktdaten nicht, wie vorgegeben, ausschließlich zum Zwecke der Kontaktnachverfolgung, sondern vielmehr auch zu eigenen Werbezwecken verarbeitet wurden. Da es an der erforderlichen Rechtsgrundlage für eine derartig zweckwidrige Weiterverarbeitung fehlte, verlangten wir zunächst die unverzügliche

Löschung der rechtswidrig gespeicherten Daten, welche auch erfolgt ist. Aufgrund der Schwere dieser Verletzung prüfen wir weitere aufsichtsbehördliche Abhilfemaßnahmen, insbesondere die Verhängung einer Geldbuße. In insgesamt 15 Fällen sprachen wir hinsichtlich der festgestellten Verstöße eine Verwarnung aus. In fünf weiteren Fällen erteilten wir förmliche Hinweise.

3 Nutzung von Corona-Gästelisten zur Einleitung von Ordnungswidrigkeitenverfahren

Im Berichtszeitraum erreichte uns eine Beschwerde, wonach die Bußgeldstelle einer Verwaltungsbehörde personenbezogene Daten aus einer Anwesenheitsliste (sogenannte Corona-Gästeliste) genutzt hatte, um gegen in dieser Liste genannte Personen Verwarnungen mit Verwarnungsgeld nach dem Waldgesetz des Landes Brandenburg zu erteilen. Hintergrund war eine nicht genehmigte private Geburtstagsfeier der Beschwerdeführerin in einem brandenburgischen Waldstück und ein hierdurch ausgelöster Polizei- und Feuerwehreinsatz. Im Rahmen der Auflösung dieser Feierlichkeit stellte die Polizei bei der Beschwerdeführerin die Corona-Gästeliste mit 50 Datensätzen (Vor- und Nachnamen, Wohnadressen, Telefonnummern sowie einer E-Mail-Adresse) von Teilnehmerinnen und Teilnehmern dieser Veranstaltung sicher und leitete diese an die jeweils zuständigen Verwaltungsbehörden zur Einleitung von Ordnungswidrigkeitenverfahren weiter.

Die Verarbeitung personenbezogener Daten aus Corona-Gästelisten zum Zweck der Verfolgung und Ahndung von Ordnungswidrigkeiten ist grundsätzlich unverhältnismäßig und somit unzulässig. Nach § 49 Satz 1 Bundesdatenschutzgesetz (BDSG) ist eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, zulässig, wenn es sich bei dem anderen Zweck um einen der in § 45 BDSG genannten Zwecke handelt, der Verantwortliche befugt ist, Daten dafür zu verarbeiten, und die Verarbeitung erforderlich und verhältnismäßig war.

Zweck der Erhebung der personenbezogenen Daten im Rahmen der Anfertigung von Corona-Gästelisten ist nach den jeweils geltenden

Regelungen zur Eindämmung von und zum Umgang mit SARS-CoV-2 die Gewährleistung einer Nachverfolgbarkeit im Falle einer Infektion. Die Verarbeitung von personenbezogenen Daten aus solchen Listen durch die Polizei bzw. die Bußgeldstellen der jeweiligen Verwaltungsbehörden erfolgte zur Verfolgung und Ahndung von Ordnungswidrigkeiten und somit zu einem anderen als dem ursprünglichen Erhebungszweck.

Im Rahmen der Verhältnismäßigkeitsprüfung kam die Landesbeauftragte zu dem Ergebnis, dass im Vergleich zur hohen Schutzwürdigkeit des Ziels der Nachverfolgbarkeit und Eingrenzung zukünftiger Infektionsketten dem Interesse der öffentlichen Stellen an der Verfolgung und Ahndung von Ordnungswidrigkeiten grundsätzlich ein geringeres Gewicht zukommt. Dem Erfordernis eines sensiblen Umgangs mit den zur Kontaktverfolgung erhobenen Anwesenheitsdaten kann man nur durch einen zurückhaltenden Gebrauch dieser Daten durch öffentliche Stellen gerecht werden. Sonst besteht die Gefahr, dass Gäste keine korrekten Angaben mehr in der Kontaktnachweisliste eintragen, und dass dadurch das wesentliche Ziel der Nachverfolgbarkeit und Eingrenzung zukünftiger Infektionsketten nicht erreicht werden kann. Dies bedeutet für die praktische Umsetzung, dass öffentliche Stellen grundsätzlich nicht auf die personenbezogenen Daten aus Corona-Gästelisten zurückgreifen dürfen, um Ordnungswidrigkeiten, die beispielsweise durch Parkverstöße vor einem Restaurant oder wie hier im Rahmen einer Geburtstagsfeier im Wald verwirklicht worden sind, zu ahnden.

Bußgelder dank Corona-Listen?

Anders verhält es sich bei der Verfolgung und Ahndung von Ordnungswidrigkeiten, die im Zusammenhang mit der Erfassung von Personendaten in der Corona-Gästeliste nach den jeweils geltenden Regelungen zur Eindämmung von und zum Umgang mit SARS-CoV-2 stehen und ausdrücklich durch Verordnung geregelt sind. Das bedeutet, dass öffentliche Stellen die Gästelisten kontrollieren dürfen, um festzustellen, ob zum Beispiel Gastwirtinnen und Gastwirte die Personendaten in den Kontaktnachweisen ordnungsgemäß erfasst bzw. ob Besucherinnen und Besucher ihre Kontaktdaten vollständig und wahrheitsgemäß in die Listen eingetragen haben.

Um künftigen etwaigen Datenschutzverstößen und Unsicherheiten im Zusammenhang mit dem Umgang mit Corona-Gästelisten entgegenzuwirken, haben wir die Polizei sowie die hier jeweils involvierten Verwaltungsbehörden ausdrücklich schriftlich auf die grundsätzliche Unzulässigkeit der Verarbeitung von personenbezogenen Daten aus diesen Listen zum Zweck der Verfolgung und Ahndung von Ordnungswidrigkeiten, die nicht im Zusammenhang mit der SARS-CoV-2-Eindämmungs- oder Umgangsverordnung stehen, hingewiesen.

Eine positive Rückmeldung auf unseren Hinweis erfolgte durch den brandenburgischen Polizeipräsidenten. Das Polizeipräsidium nahm unseren Hinweis zum Anlass, die verantwortliche Polizeiinspektion unter Verweis auf eine hausinterne Verfügungslage zum polizeilichen Umgang mit personenbezogenen Daten aus den Corona-Gästelisten zu sensibilisieren. Auch von der weiteren involvierten Verwaltungsbehörde erhielten wir ein zustimmendes Feedback.

4 Software zur Bewältigung der Corona-Pandemie

Bereits vor der Corona-Pandemie haben wir ein gemeinnütziges Potsdamer Unternehmen, das aus dem Hasso-Plattner-Institut ausgegründet wurde, bei der Entwicklung von cloudbasierten Gesundheitsanwendungen beratend unterstützt. Hierbei bestand zunächst das Ziel, einer Gruppe von Patientinnen und Patienten mit einem bestimmten Krankheitsbild einen sicheren, verschlüsselten Speicher für ihre Gesundheitsdaten im Internet bereitzustellen, der nicht durch Dritte oder den Anbieter selbst eingesehen werden kann. Die weitere Umsetzung sah vor, aus den Gesundheitsdaten nützliche Informationen und Empfehlungen zur gesunden Lebensweise abzuleiten und letztlich auch die Möglichkeit anzubieten, die eigenen Daten für Forschungszwecke freizugeben. Im Rahmen der Corona-Pandemie hat das Unternehmen seine Prioritäten neu geordnet und aufbauend auf den Vorarbeiten unter anderem zwei Projekte zur besseren Bewältigung der Pandemiefolgen umgesetzt.

Das erste Projekt adressierte die Patientenaufnahme von Krankenhäusern und anderen Institutionen, die Corona-Tests durchführen. Kooperationspartner war die Berliner Charité. Das Ausfüllen eines

papiernen Anamnesebogens mit diagnoserelevanten Fragen durch die Patientinnen und Patienten verursachte regelmäßig einen erheblichen Stau bei der Aufnahme. Zur Beschleunigung des Vorgangs entwickelte das Unternehmen einen webbasierten Fragebogen, der auch mit Smartphones ausgefüllt werden kann und aus den Antworten der Nutzerinnen und Nutzer einen QR-Code erzeugt. Dieser enthält in pseudonymisierter Form die Anamnesedaten und kann bei der Aufnahme wahlweise ausgedruckt oder auf dem Smartphone vorgezeigt werden. Die Daten werden kontaktlos mittels Scanner eingelesen und so der organisatorische und zeitliche Aufwand vor der Durchführung der Tests erheblich reduziert. Eine automatische Übernahme der Anamnesedaten in andere Systeme (z. B. das Krankenhausinformationssystem) ist möglich.

Im Rahmen dieses ersten Projekts traten zwei Beratungsthemen besonders in den Vordergrund. Zum einen müssen die Nutzer über die Verarbeitung ihrer Daten im Sinne von Artikel 13 Datenschutz-Grundverordnung angemessen aufgeklärt werden. Hier gaben wir Hinweise zur Gestaltung der Datenschutzerklärung und kontrollierten deren Umsetzung. Zum anderen muss auf technischer Seite sichergestellt werden, dass eine Datenverarbeitung erst nach der Einwilligung stattfindet, die Daten nur pseudonymisiert zwischengespeichert werden und sie auch wieder gelöscht werden können. Positiv fiel auf, dass die Anamnesedaten zu jedem Zeitpunkt lokal auf dem Gerät der jeweiligen Nutzerinnen und Nutzer verbleiben und dort auch der QR-Code generiert wird. Das Risiko einer Übertragung der Daten über das Internet und ihrer Speicherung bei einem Dienstleister wird somit von vornherein ausgeschlossen. Weiterhin stellten wir fest, dass das Unternehmen zur Verbesserung des Angebots und Unterstützung der Softwareentwicklung zwar eine Software zur Nutzeranalyse einsetzte, diese jedoch auf datenschutzkonforme Art und Weise konfiguriert war. Letztlich wurden alle Datenschutzanforderungen umgesetzt. Der Programmcode steht zur Adaptierung durch andere Teststellen auf der Plattform GitHub öffentlich zur Verfügung.

Bei dem zweiten Projekt handelte es sich um die Entwicklung eines Symptomtagebuchs – auch hier in Form einer Webanwendung und als App auf dem Smartphone. Das Tagebuch hat zum Ziel, Nutze-

rinnen und Nutzern bei einer potenziellen oder tatsächlichen Corona-Infektion die regelmäßige Aufzeichnung der behandlungsrelevanten Symptome zu ermöglichen und diese sicher zu verwahren. Zur Speicherung des Tagebuchs wird die technische Infrastruktur der ursprünglich geplanten Gesundheits-Cloud genutzt. Das Potsdamer Unternehmen richtete diese auf Servern in Deutschland ein und führt die Administration vollständig selbst durch. Um ein hohes Datenschutzniveau zu ermöglichen, entwickelte das Unternehmen eine komplexe kryptografische Infrastruktur, bei der nur der Nutzerin bzw. dem Nutzer selbst die Entschlüsselung und somit auch der Zugriff auf die eigenen Daten möglich sind. Bei Bedarf können die Daten des Tagebuchs exportiert und damit z. B. dem medizinischen Personal bereitgestellt werden.

Apps helfen durch die Krise

Einen wesentlichen Schwerpunkt der Beratung im zweiten Projekt bildete die Überprüfung der zugrundeliegenden kryptographischen Umsetzung zur Speicherung der Daten. Hierbei ist besonders positiv aufgefallen, dass es dem Unternehmen als Betreiber der Plattform zu keinem Zeitpunkt möglich ist, die hinterlegten Daten einzusehen. Vielmehr sind die Nutzerinnen und Nutzer die einzige Instanz, die jeweils auf den eigenen, verschlüsselten Datenbereich zugreifen kann. Dieser sogenannte Zero-Knowledge-Ansatz ist aktuell noch nicht selbstverständlich und ermöglicht den betroffenen Personen eine weitreichende Datensouveränität. Auch in diesem Projekt überprüften wir die Datenschutzerklärung und gaben entsprechende Hinweise.

5 Technische und organisatorische Maßnahmen zur Umsetzung des Datenschutzes bei der Heimarbeit

Die Corona-Pandemie erfordert von Unternehmen und Behörden die Bewältigung einer Vielzahl von Herausforderungen auf unterschiedlichsten Ebenen. Neben krankheitsbedingten Abwesenheiten, Gewinneinbrüchen und plötzlich untauglich gewordenen Geschäftsmodellen sind insbesondere Kontaktbeschränkungen sowie nicht ausreichend pandemiekonforme Arbeitsplätze ein drängendes Problem. In diesem Kontext entdecken viele Verantwortliche die Heimarbeit als Ausweg.

Unter Heimarbeit verstehen wir das dauerhafte, zeitweise oder alternierende Arbeiten an einem dafür hergerichteten Arbeitsplatz in einer privaten, häuslichen Umgebung. Hiervon abzugrenzen ist das mobile Arbeiten, bei dem eben keine fest eingerichtete Umgebung existiert. Im Rahmen unserer Tätigkeit wurden wir zum einen mit Anfragen und Beratungsersuchen zur Heimarbeit mit personenbezogenen Daten konfrontiert, zum anderen haben wir leider auch einige Beschwerden erhalten und unzureichende Umsetzungen festgestellt. Hierdurch ist uns bewusst geworden, dass einige Verantwortliche schon mit der Identifizierung der zu regelnden Themenbereiche überfordert sind. Vor diesem Hintergrund und mit Blick auf die voraussichtlich länger andauernden Pandemiebeschränkungen haben wir die wichtigsten Anforderungen sowie die daraus resultierenden technischen und organisatorischen Maßnahmen zur Verarbeitung personenbezogener Daten in Heimarbeit in einer Handreichung zusammengefasst und als Hilfestellung für Unternehmen und Behörden in unserem Internetangebot veröffentlicht.

Zwei grundlegende Probleme bei der Umsetzung von Heimarbeit konnten wir immer wieder feststellen: Viele Verantwortliche orientieren sich an im Internet kursierenden, „fertigen“ Listen von Maßnahmen, streichen Unpassendes oder Unbequemes heraus und verwenden den Rest als „Heimarbeitskonzept.“ Ebenfalls beliebt ist der Ansatz, Verpflichtungserklärungen von Beschäftigten einzufordern, sie dann jedoch bei einem Großteil der praktischen Umsetzung allein zu lassen. Hieran lassen sich gleich zwei Kardinalfehler erkennen: Zunächst ist der datenschutzrechtlich Verantwortliche (also z. B. das Unternehmen oder die Behörde) auch für die Einhaltung der entsprechenden gesetzlichen Anforderungen bei der Heimarbeit verantwortlich. Seine Aufgaben reichen von einer lückenlosen Konzipierung über die Anschaffung der erforderlichen Hard- und Software sowie die Einbindung der in Heimarbeit befindlichen Beschäftigten bis hin zur Kontrolle der Heimarbeitsplätze. Zum anderen orientiert sich das oben geschilderte Vorgehen nicht an dem eigenen, unternehmensspezifischen Bedarf und behandelt somit auch nicht zwingend die Risiken der eigenen Geschäftstätigkeit. Da die bzw. der Beschäftigte in Heimarbeit Teil des Unternehmens bzw. der Behörde bleibt, muss auch der Heimarbeitsplatz als Teil der Arbeitsstätte aufgefasst werden. Daraus folgt, dass dort mindestens

die gleichen Risiken wie in der Betriebsstätte bzw. der Behörde zu adressieren sind. Insofern ist jeder in Heimarbeit stattfindende Prozess einer Risikobewertung zu unterziehen. Aus dieser sind entsprechende Maßnahmen zur Minimierung des zugrunde liegenden Risikos abzuleiten. Dies ist so lange zu wiederholen, bis ein hinreichend niedriges, beherrschbares Restrisiko vorliegt. Entsprechend müssen Verantwortliche auch die in der von uns veröffentlichten Handreichung zusammengestellten Anforderungen und Maßnahmen an die eigenen Bedürfnisse anpassen und ergänzen.

Unser Papier haben wir in die Themenkomplexe konzeptionelle Vorarbeiten, Einrichtung des häuslichen Arbeitsplatzes, Aufbewahrung und Transport, Hard- und Software-Management, Kommunikationsinfrastruktur sowie Kommunikation zwischen Beschäftigten und Unternehmen unterteilt. Zu jedem Themenkomplex wurden datenschutzrechtliche Anforderungen und Maßnahmen für normale und hohe Risiken identifiziert. Um Unklarheiten aufgrund eines nicht eindeutigen Sprachgebrauchs zu vermeiden, haben wir uns bei der Formulierung an den Publikationen des Bundesamtes für Sicherheit in der Informationstechnik zum IT-Grundschutz orientiert: Eine MUSS-Anforderung ist zwingend umzusetzen, eine SOLLTE-Anforderung ist zur Umsetzung empfohlen und kann nach eigenem Ermessen durch andere Maßnahmen ersetzt werden, die Umsetzung einer KANN-Anforderung ist optional. Nachfolgend geben wir eine kurze Zusammenfassung der wichtigsten Aspekte der einzelnen Themenkomplexe.

Im Hinblick auf konzeptionelle Vorarbeiten haben wir generelle Kriterien zur Umsetzung der Heimarbeit und Anforderungen bezüglich der Dokumentation aufgeführt. So werden Themen wie die Prüfung der Eignung von Verarbeitungstätigkeiten für Heimarbeit, die Einräumung von Kontrollrechten im häuslichen Bereich, die Schulung von Mitarbeiterinnen und Mitarbeitern, die Fortschreibung von Datenschutz- und IT-Sicherheitskonzepten sowie die Erforderlichkeit einer Datenschutz-Folgenabschätzung angesprochen. Der Verantwortliche muss durch eine individuelle Klärung dieser Fragen die Heimarbeit auf ein solides Fundament stellen.

Bei der Einrichtung des häuslichen Arbeitsplatzes sind Aspekte wie die grundsätzliche Eignung eines Raumes für Heimarbeit und die Trennung von Arbeits- und Privatbereich zu beachten sowie Fragen zum Perimeterschutz zu klären. Hierbei soll sichergestellt werden, dass die Beschäftigten den Heimarbeitsplatz als Teil der betrieblichen Arbeitsstätte wahrnehmen und an diesem auch so handeln.

Schnell übersehen werden der Transport von personenbezogenen Daten (z. B. in Akten oder auf elektronischen Datenträgern) zwischen Unternehmen oder Behörde und dem häuslichen Bereich sowie die Aufbewahrung der Daten am Heimarbeitsplatz – speziell außerhalb der Arbeitszeit. Die Risiken auf diesen Gebieten sind höher als bei einer Verarbeitung ausschließlich in den Räumlichkeiten des Verantwortlichen. Als wesentliche Maßnahme ist die Bereitstellung der entsprechenden Behältnisse durch Verantwortliche zu nennen, sodass der sichere Transport und die sichere Aufbewahrung der personenbezogenen Daten nicht allein den Beschäftigten überlassen wird.

Ab nach Hause! Home statt Office

Unter der Überschrift Hard- und Software-Management sprechen wir Fragestellungen zur Administration der Hardware, zur Nutzung von privaten Endgeräten, zur Freigabe der eingesetzten Software und zur Notwendigkeit von Verschlüsselung an. Hierbei war es uns besonders wichtig, erneut die Verantwortlichkeit des Unternehmens oder der Behörde in den Vordergrund zu stellen, eine klare Vorgabe zur Verwendung von unternehmens- oder behördeneigener Hard- und Software zu treffen und klarzustellen, dass private Geräte nur ausnahmsweise und unter ausreichender Kontrolle durch den Verantwortlichen genutzt werden können.

Der Themenkomplex Kommunikationsinfrastruktur trifft hauptsächlich Aussagen zu Anforderungen an die Anbindung der eingesetzten Hardware an die Unternehmensressourcen. Über allgemeine Grundlagen, wie eine sichere Transportverschlüsselung, haben wir hier Anforderungen an die eingesetzten Router mit aufgenommen, da ein Teil der für den Verbrauchermarkt konzipierten Geräte häufig Sicherheitsmängel aufweist, die nur zögerlich bereinigt werden.

Im Hinblick auf die Kommunikation zwischen den in Heimarbeit befindlichen Beschäftigten und Unternehmen oder Behörde wird zum einen die Schaffung von Richtlinien verlangt, die einen geordneten Austausch ermöglichen, zum anderen werden für wesentliche Kommunikationsmittel wie E-Mail oder Telefon die wichtigsten Maßnahmen festgehalten.

Wir hoffen, dass das Papier eine gute Orientierung zur datenschutzkonformen Ausgestaltung von Heimarbeit gibt und Verantwortliche in die Lage versetzt, eine Anpassung an ihre konkreten Verarbeitungsvorgänge und die spezifischen Risiken vorzunehmen sowie die erforderlichen technischen und organisatorischen Maßnahmen zu identifizieren und umzusetzen.

6 Empfehlungen zum Einsatz von Videokonferenzsystemen

Aufgrund der Corona-Pandemie und der durch die Bundes- und Landesregierungen beschlossenen Einschränkungen, insbesondere hinsichtlich direkter persönlicher Kontakte, entstand bei vielen Verantwortlichen die Notwendigkeit, virtuelle Treffen durchzuführen. Unternehmen und Behörden, Schulen und Hochschulen, Vereine und Privatpersonen setzten in großem Umfang Videokonferenzen ein – oder planten es zumindest, da oftmals die technischen Voraussetzungen noch geschaffen werden mussten. Hierzu gehört auch die Auswahl eines geeigneten, datenschutzgerecht zu betreibenden Videokonferenzsystems. Insofern erhielt die Landesbeauftragte im Berichtszeitraum sehr viele Anfragen und Beratungsersuchen zu diesem Thema. Weiterhin beschwerten sich auch immer wieder Teilnehmerinnen und Teilnehmer von Videokonferenzen, dass ein konkretes Produkt, ein Videokonferenzbetreiber oder ein genutzter Dienstleister eben nicht die datenschutzrechtlichen Anforderungen eingehalten hatte.

Die Landesbeauftragte führte keine eigenständige datenschutzrechtliche Prüfung von Produkten zur Durchführung von Videokonferenzsystemen oder von Anbietern entsprechender Dienstleistungen durch. Sie beteiligte sich dagegen an der Erarbeitung der „Orientierungshilfe Videokonferenzsysteme“ der Konferenz der

unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, die im September 2020 auch in unserem Internetangebot veröffentlicht wurde. Die Orientierungshilfe wird ergänzt durch eine Checkliste, in der die datenschutzrechtlichen Anforderungen in komprimierter Form zusammengefasst sind.

In der Orientierungshilfe wird insbesondere der Einsatz von Videokonferenzsystemen in Form einer sogenannten On-Premises-Lösung empfohlen, d. h. eines auf der eigenen IT-Infrastruktur laufenden Systems. Nur in diesem Fall hat der Betreiber der Videokonferenz auch alle datenschutzrechtlichen und technischen Angelegenheiten in seiner Hand und kann die Umsetzung der gesetzlichen Anforderungen eigenständig gewährleisten. Lässt sich eine solche Lösung nicht umsetzen, kann auch ein Dienstleister mit dem Betrieb des Videokonferenzsystems beauftragt werden. Dabei sind die Regelungen zur Auftragsverarbeitung (insbesondere zur Kontrolle des Dienstleisters) einzuhalten. Grundsätzlich sollten Dienstleister mit Sitz in Europa bevorzugt werden. Die Verwendung der anfallenden Daten für eigene Zwecke des Dienstleisters ohne rechtliche Grundlage ist genauso auszuschließen wie Datenabflüsse an den Hersteller des Videokonferenzsystems oder an Dritte. Aus den zuletzt genannten Gründen sind im Internet einfach zugängliche Online-Dienste für Videokonferenzen oftmals aus datenschutzrechtlicher Sicht kritisch zu bewerten.

Die Orientierungshilfe weist außerdem sehr deutlich auf die Beachtung der entsprechenden Rechtsgrundlagen hin. In Frage kommen grundsätzlich eine freiwillige, informierte Einwilligung der an der Videokonferenz Teilnehmenden, die Erforderlichkeit für die Erfüllung eines Vertrages oder zur Wahrnehmung einer öffentlichen Aufgabe oder zur Wahrung berechtigter Interessen des Verantwortlichen. Videokonferenzen im Beschäftigungskontext können auf § 26 Bundesdatenschutzgesetz bzw. § 26 Brandenburgisches Datenschutzgesetz gestützt werden. Die Erforderlichkeit der Übertragung von Bilddaten sollte dabei stets überprüft werden. Auch Kollektivvereinbarungen mit dem Betriebs- oder Personalrat können Videokonferenzen legitimieren. Nehmen Beschäftigte vom heimischen Arbeitsplatz aus an Videokonferenzen teil, sind Einblicke in ihre Privatsphäre oder das Erscheinen von Familienmitgliedern o. ä. zu verhindern. Sollen mit ei-

ner Videokonferenz auch besondere Kategorien personenbezogener Daten verarbeitet werden, ist die rechtliche Zulässigkeit gesondert zu prüfen.

Weitere Pflichten für den Betreiber einer Videokonferenz und damit Verantwortlichen nach der Datenschutz-Grundverordnung (DS-GVO) ergeben sich beispielsweise aus den Artikel 13 DS-GVO (Information über die Datenverarbeitung zur Gewährleistung der Transparenz), Artikel 25 DS-GVO (datenschutzfreundliche Voreinstellungen), Artikel 28 DS-GVO (Abschluss eines Auftragsdatenverarbeitungsvertrags), Artikel 30 DS-GVO (Führen eines Verzeichnisses der Verarbeitungstätigkeiten) und Artikel 32 DS-GVO (Umsetzung von technischen und organisatorischen Maßnahmen). Auch für Letzteres enthält die Orientierungshilfe viele Hinweise und Empfehlungen, z. B. hinsichtlich der Sicherheit der Übertragung durch Verschlüsselung, der Authentisierung der Teilnehmerinnen und Teilnehmer einer Videokonferenz oder das Erstellen eines entsprechenden Berechtigungskonzepts.

Werden im Zuge einer Videokonferenz personenbezogene Daten in Drittländer übertragen (z. B. zum Hersteller oder Anbieter des Systems), sind zusätzlich die Regelungen der Datenschutz-Grundverordnung für entsprechende Datentransfers einzuhalten. Hierbei ist auch das Schrems II-Urteil[2] des Europäischen Gerichtshofs vom 16. Juli 2020 zu beachten.

7 Einsatz von Videokonferenzsystemen bei der Online-Lehre an Hochschulen

Die Corona-Pandemie führte bereits im Sommersemester 2020 zu erheblichen Einschränkungen im Lehrbetrieb der brandenburgischen Hochschulen. Die sonst übliche Durchführung von Lehrveranstaltungen im Präsenzbetrieb war durch Kontaktbeschränkungen auf einmal nicht mehr ohne Weiteres möglich. Um die Lehre weiterhin gewährleisten zu können und gleichzeitig das Infektionsgeschehen an den Hochschulen zu minimieren, mussten sie kurzfristig auf Online-Varianten von Vorlesungen, Seminaren, Übungen usw. umstellen. Das Studium wurde so zu einem großen Teil in virtuelle Räume

2 siehe A V 2

sowie die eigenen vier Wände der Studierenden und des Lehrpersonals verlagert.

Um die Hochschulen bei einer datenschutzgerechten Durchführung der Online-Lehre unterstützen zu können, war es notwendig, dass wir uns zunächst einen Überblick über die eingesetzten Lehrmittel verschaffen. Daher führten wir eine Umfrage bei den staatlichen Universitäten und Fachhochschulen des Landes Brandenburg durch. Bereits vor dem Hintergrund der unterschiedlichen technischen Ausstattung und der Größe der jeweiligen Hochschulen ergaben sich bei der Umsetzung der Online-Lehre unterschiedliche Herausforderungen. Die kleinste Hochschule im Land Brandenburg hat beispielsweise ca. 850 Studierende bei ca. 350 Lehrveranstaltungen mit einer maximalen Größe von 100 Plätzen. Im Vergleich dazu hat die größte Hochschule des Landes ca. 21.000 Studierende bei ca. 2.900 Lehrveranstaltungen mit einer maximalen Größe von 666 Plätzen. Aber auch innerhalb einer einzelnen Hochschule gibt es keine einheitliche Umsetzung der Online-Lehre. Ein Grund hierfür ist die Freiheit von Forschung und Lehre, wonach die jeweiligen Lehrenden die Lehrmethode frei gestalten und selbst über die verwendeten Lehrmittel entscheiden können.

Bei der Bereitstellung der Lehrinhalte im Rahmen der Online-Lehre können grundlegend zwei Formen unterschieden werden. Bei der asynchronen Form werden die Lehrinhalte wie z. B. Vorlesungsskripte, Aufgabenblätter, Videoaufzeichnungen usw. auf den Lernplattformen der Hochschulen bereitgestellt. Eine direkte Interaktion zwischen den Lehrenden und den Studierenden findet hierbei typischerweise nicht statt. Diese asynchrone Bereitstellung der Lehrinhalte bereitet aus Sicht des Datenschutzes weniger Probleme. Zum einen ist diese Methode für Studierende datensparsam, zum anderen wird sie aus Sicht der Hochschulen schon seit längerer Zeit praktiziert.

Bei der synchronen Vermittlung der Lehrinhalte ist dagegen oftmals eine direkte Kommunikation zwischen den Lehrenden und den Studierenden erwünscht, zum Teil auch erforderlich. Am häufigsten werden hierfür Videokonferenzsysteme eingesetzt. Aufgrund der unterschiedlichen technischen Rahmenbedingungen und Anforde-

rungen kommen bereits innerhalb einer Hochschule oftmals zwei bis drei verschiedene Videokonferenzsysteme zum Einsatz. Einige dieser Systeme können durch die Hochschulen selbstständig betrieben werden. Allerdings werden auch Videokonferenzsysteme externer Anbieter genutzt. Weil die Hochschulen für diese Konferenzsysteme kaum technische Kapazitäten benötigen, sind diese oftmals schneller und leichter verfügbar.

Beim Einsatz von Videokonferenzsystemen im Rahmen der Online-Lehre ergibt sich aus Sicht des Datenschutzes eine Vielzahl von Herausforderungen. Neben dem Filmen im privaten Wohnraum und dem Aufzeichnen von Videokonferenzen samt der Beiträge der Teilnehmenden, kann insbesondere der Einsatz von externen Anbietern zu datenschutzrechtlichen Problemen führen. Hierbei handelt es sich in der Regel um eine Auftragsverarbeitung gemäß Artikel 28 Datenschutz-Grundverordnung. Die Hochschule bleibt der Verantwortliche für die Verarbeitung der personenbezogenen Daten und muss bereits vor dem Einsatz sicherstellen, dass der gewählte externe Anbieter alle gesetzlichen Anforderungen erfüllt. Die Details sind im Rahmen eines Vertrages zu dokumentieren. Verarbeitet der Anbieter die Daten auch zu eigenen Zwecken, benötigt er hierfür eine Rechtsgrundlage, genauso wie die Hochschule eine Rechtsgrundlage zur Übermittlung der Daten an ihn braucht.

Vereinzelt kamen in brandenburgischen Hochschulen im Sommersemester 2020 auch amerikanische Anbieter von Videokonferenzsystemen zum Einsatz, die die datenschutzrechtlichen Anforderungen nicht in vollem Umfang erfüllen. Insbesondere ist aufgrund des Schrems II-Urteils des Europäischen Gerichtshofs[3] die Übermittlung von personenbezogenen Daten in die USA nicht mehr ohne Weiteres zulässig und bedarf zusätzlicher Maßnahmen, um ein angemessenes Datenschutzniveau zu erreichen. Zu den im Rahmen von Videokonferenzen verarbeiteten personenbezogenen Daten zählen beispielsweise IP-Adressen, Benutzer- oder Anmeldedaten sowie die per Video- und Audiosignal übertragenen Inhalte, gegebenenfalls auch über dritte Personen.

3 siehe A V 2

Wir rieten den Hochschulen davon ab, auf Auftragsverarbeiter, bei denen es keine Rechtssicherheit und kein dem europäischen vergleichbares Datenschutzniveau gibt, zurückzugreifen. Insbesondere kann dem Argument einiger Hochschulen, dass diese Anbieter die einzigen seien, die eine stabil laufende Online-Lehre ermöglichen, aus datenschutzrechtlicher Sicht nicht gefolgt werden. Zwar können die Hochschulen bzw. die jeweiligen Lehrenden aufgrund der Freiheit der Lehre grundsätzlich selbst entscheiden, welche Form sie für die Vermittlung der Inhalte wählen und welche Medien sie hierfür einsetzen. Dabei müssen sie sich jedoch nach wie vor an geltendes Recht halten. Falls aus technischer oder rechtlicher Sicht der Einsatz von bestimmten Videokonferenzsystemen nicht zulässig oder möglich ist, muss ein alternatives System oder eine andere Lehrmethode eingesetzt werden. Inwiefern die Hochschulen unserem Rat gefolgt sind, werden wir im Frühjahr 2021 prüfen.

II Datenschutzverstöße: Maßnahmen und Sanktionen

1 Das Patientendaten-Schutz-Gesetz und die elektronische Patientenakte

Im Berichtszeitraum hat der Bundesgesetzgeber das Patientendaten-Schutz-Gesetz auf den Weg gebracht, um den Versicherten unter anderem die bereits lange angekündigte elektronische Patientenakte anzubieten. Das Gesetz sollte u.a. die technische Umsetzung des Vorhabens regeln. Datenschutzrechtliche Kritik blieb dabei auf der Strecke. Vielmehr beschloss der Deutsche Bundestag das Patientendaten-Schutz-Gesetz am 3. Juli 2020, ohne die Empfehlungen des Bundesrates für datenschutzrechtliche Verbesserungen vollständig umzusetzen.

In der Kritik stand vor allem die Regelung zum Zugriff auf die Inhalte der (freiwilligen) elektronischen Patientenakte. Zwar sollten die Versicherten dokumentenscharf festlegen können, welche Ärztinnen und Ärzte, Psychotherapeutinnen und Psychotherapeuten oder Apotheken welche Daten sehen können. Allerdings war für die erste Ausbaustufe vom 1. Januar 2021 bis zum 31. Dezember 2021 noch nicht vorgesehen, die Zugriffsrechte nach Dokumenten differenziert und feingranular zu vergeben. Erst nach dem 1. Januar 2022 sollten Versicherte, die hierfür ein Smartphone oder Tablet nutzen, so verfahren können. Patientinnen und Patienten, die nicht bereit oder in der Lage sind, ein mobiles Endgerät zu verwenden, sollte diese Möglichkeit auch nach dem 1. Januar 2022 weitgehend verwehrt bleiben. Hinzu kam, dass die ursprünglich vorgesehene Verpflichtung der Krankenkassen, Patiententerminals zur Verwaltung der elektronischen Patientenakte anzubieten, aus dem Gesetzentwurf gestrichen worden war.

Elektronische Patientenakte – entweder alles oder nichts

Im Ergebnis stehen die Patientinnen und Patienten insbesondere in der ersten Umsetzungsphase vor einer Alles-oder-nichts-Entscheidung – sie geben entweder allen Behandelnden alle Dokumente ihrer elektronischen Patientenakte zur Kenntnis oder eben gar keine. Auch können Versicherte, die kein Smartphone oder Tablet nutzen können oder möchten, einen dokumentenscharfen Zugriff erst ab 2022 und dann nur mit der Unterstützung einer Vertreterin oder eines Vertreters erreichen. Das

hat zur Folge, dass sie dieser oder diesem einen vollständigen Zugriff auf ihre Gesundheitsdaten einräumen müssen.

Für die Anmeldung der Patientinnen und Patienten in der elektronischen Patientenakte ist neben der Verwendung der elektronischen Gesundheitskarte noch ein weiteres, alternatives Verfahren gesetzlich vorgeschrieben worden. Das für die Apps auf mobilen Endgeräten angebotene alternative Authentifizierungsverfahren al.vi (alternative Versichertenidentität) ist jedoch nicht den Risiken der Verarbeitung angemessen. Es bietet nicht den erforderlichen, hohen Schutz vor Datenmissbrauch durch Unbefugte und kann daher nicht datenschutzgerecht eingesetzt werden.

Diese Einschränkungen widersprechen der vom Gesetzgeber selbst hervorgehobenen Bedeutung der Patientensouveränität. Sie wäre nur gewahrt, wenn von Anfang an eine feingranular ausgestaltete Zugriffsmöglichkeit auf Dokumente der elektronischen Patientenakte bestünde, und zwar so, dass die Versicherten selbst entscheiden können, wem sie welche Informationen zur Verfügung stellen. Mit dem lediglich grobgranularen Zugriffsmanagement werden die datenschutzrechtlichen Grundsätze der Datensparsamkeit, der Erforderlichkeit und der Zweckbindung außer Acht gelassen.

Am 19. August 2020 nahm die Landesbeauftragte gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie mit den Datenschutzaufsichtsbehörden zweier weiterer Länder an einer Bundespressekonferenz teil. In einer begleitenden Presseinformation forderte sie die Landesregierung Brandenburg auf, sich dafür einzusetzen, dass der Bundesrat seine weiteren Mitwirkungsrechte im Rahmen des Gesetzgebungsverfahrens ausschöpft. Wenig später wirkte sie im Rahmen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder an einer gemeinsamen Entschließung[4] mit. Diese Maßnahmen hatten zum Ziel, auf den Verstoß des Patientendaten-Schutz-Gesetzes gegen europäisches Recht aufmerksam zu machen und auf Nachbesserungen hinzuwirken.

4 Entschließung „Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig!“ vom 1. September 2020.

Die Landesbeauftragte wandte sich mit dieser Forderung auch unmittelbar an die Staatskanzlei und das Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz des Landes Brandenburg. Die Landesregierung erklärte jedoch, dass die elektronische Patientenakte zum 1. Januar 2021 freiwillig eingeführt werde. Versicherte, die unsere datenschutzrechtlichen Bedenken teilen, könnten sich auch für eine spätere Nutzung entscheiden. Eine Anrufung des Vermittlungsausschusses durch den Bundesrat erfolgte nicht mehr. Das Patientendaten-Schutz-Gesetz wurde am 19. Oktober 2020 veröffentlicht.[5]

Noch bevor das Gesetz veröffentlicht worden war, hatten wir uns an die beiden unserer Aufsicht unterstehenden Krankenkassen gewandt. Wir erkundigten uns, ob sie beabsichtigten, die Regelungen des Patientendaten-Schutz-Gesetzes unverändert umzusetzen oder darüber hinausgehend von Anfang an ein dokumentenscharfes Zugriffsmanagement, Patienten-Terminals sowie ein datenschutzgerechtes Authentifizierungsverfahren anzubieten.

Eine Krankenkasse hat daraufhin auf ihre gesetzliche Verpflichtung sowie auf ihre Abhängigkeit von der technischen Spezifikation der Lösung durch die gematik GmbH, die im Fünften Buch Sozialgesetzbuch vorgegeben ist, hingewiesen. Dabei betonte sie, sich im Gesetzgebungsverfahren für Verbesserungen bei den Versichertenrechten eingesetzt zu haben. Sie werde als zusätzliche Authentifizierungsmöglichkeit einen Zugang über die elektronische Gesundheitskarte mit einer PIN anbieten. Allerdings befürchte sie, dass diese Möglichkeit von den Versicherten als weniger nutzerfreundlich verworfen werden könnte.

Im Ergebnis hat die Landesbeauftragte gegenüber beiden Krankenkassen eine Warnung gemäß Artikel 58 Absatz 2 Buchstabe a Datenschutz-Grundverordnung bezüglich des Berechtigungsmanagements ausgesprochen. Nach dem aktuellen Stand der Technik ist es nicht nachvollziehbar, dass den Versicherten zunächst nur eine grobgranulare Zugriffssteuerung ermöglicht wird, die sie in ihren Rechten mehr als nötig einschränkt.

5 Patientendaten-Schutz-Gesetz vom 14. Oktober 2020 (BGBl. 2020 Nr. 46)

2 Videoüberwachung im Rahmen der Feierlichkeiten zum Tag der Deutschen Einheit (EinheitsEXPO)

Das Land Brandenburg war in diesem Jahr für die Ausrichtung der Feierlichkeiten zum Tag der Deutschen Einheit verantwortlich, da es in der Zeit vom 1. November 2019 bis zum 31. Oktober 2020 den Vorsitz im Bundesrat inne hatte. Die Staatskanzlei übernahm die Organisation der EinheitsEXPO. Bei diesen zentralen, in ihrem Umfang pandemiebedingt erheblich reduzierten, Feierlichkeiten in der Landeshauptstadt Potsdam präsentierten sich an insgesamt 30 Plätzen unter anderem die Bundesländer und die Bundesverfassungsorgane. Ihre Exponate wurden in sogenannten „Event Cubes“ ausgestellt. Dabei handelte es sich um gläserne Würfel, die eine Betrachtung der Exponate ausschließlich von außen erlaubten.

Die Staatskanzlei informierte die Landesbeauftragte erstmals Anfang August 2020 über Einzelheiten der anstehenden Veranstaltung, welche zwischen dem 5. September und dem 4. Oktober 2020 stattfinden sollte. Während der Veranstaltung sollten die ausgestellten Exponate in den Event Cubes ganztägig für 24 Stunden mittels Videoüberwachung vor Diebstahl, Beschädigung und Zerstörung geschützt werden. Mithilfe der Videoüberwachung – ausschließlich zur Echtzeitbeobachtung und ohne Speicherung der Videobilder – wollte die Staatskanzlei auch erreichen, dass Ansammlungen von Personen durch gezielte Lenkung vermieden und Sicherheitsabstände zum Schutz vor Übertragungen von Covid-19 eingehalten werden. Zusätzlich zu den vier Videokameras sollte Wachpersonal zur Erfüllung der vorgenannten Zwecke zum Einsatz kommen. Die Erfassungsbereiche jeder einzelnen Kamera zeigten neben den Event Cubes auch weiträumig Flächen des öffentlichen Straßenlandes.

Eine Videoüberwachung durch öffentliche Stellen, von der andere Personen betroffen sind, ist nach Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) nur zulässig, wenn alle Betroffenen eingewilligt haben oder die Überwachung auf eine gesetzliche Erlaubnisnorm gestützt werden kann. Als Erlaubnisnorm kam hier lediglich Artikel 6 Absatz 1 Buchstabe e DS-GVO i. V. m. § 28 Absatz 1 Brandenburgisches Datenschutzgesetz (BbgDSG) in Be-

tracht. Nach Artikel 6 Absatz 1 Buchstabe e DS-GVO ist die Verarbeitung personenbezogener Daten zulässig, soweit dies zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Gemäß Artikel 6 Absatz 2 DS-GVO hat der brandenburgische Gesetzgeber mit § 28 BbgDSG eine spezifische Vorschrift zur Videoüberwachung öffentlich zugänglicher Räume erlassen. Nach § 28 Absatz 1 BbgDSG dürfen öffentliche Stellen eine Videoüberwachung öffentlich zugänglicher Räume nur durchführen, soweit dies zur Erfüllung ihrer Aufgaben (Nummer 1), zur Wahrnehmung des Hausrechts (Nummer 2), zum Schutz des Eigentums oder Besitzes (Nummer 3) oder zur Kontrolle von Zugangsberechtigungen (Nummer 4) erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen.

Die Staatskanzlei konnte nach dem Dafürhalten der Landesbeauftragten ihre Videoüberwachung vor dem Hintergrund, dass sie die Exponate in den Event Cubes – also den Besitz – vor Diebstahl, Beschädigung oder Zerstörung schützen wollte, höchstens auf § 28 Absatz 1 Nummer 3 BbgDSG stützen. Eine Erforderlichkeit der Datenverarbeitung für diese Zwecke ist jedoch nur gegeben, wenn und soweit die konkrete Art und Weise der Überwachung geeignet ist, sie zu erreichen, und es keine andere, weniger in die Grundrechte und Grundfreiheiten betroffener Personen eingreifende Möglichkeit gibt (sogenanntes milderes Mittel). Für den Zweck des Besitzschutzes stellte die Videoüberwachung grundsätzlich ein geeignetes Mittel dar. Allerdings machte die Landesbeauftragte der Staatskanzlei mit Blick auf die Erforderlichkeit deutlich, dass eine Videoüberwachung nur zulässig ist, wenn die Verarbeitung personenbezogener Daten sowohl zeitlich als auch räumlich beschränkt wird. Demnach war eine Videoüberwachung mittels der vier Kameras nur zwischen 21:00 Uhr abends und 6:00 Uhr morgens zulässig und die Erfassungsbereiche der Kameras waren ausschließlich auf die Event Cubes zu begrenzen. Im Übrigen hätte nach Ansicht der Landesbeauftragten auch eine zahlenmäßige Erhöhung des Wachpersonals ein milderes Mittel zur Videoüberwachung dargestellt.

Im Rahmen der Interessenabwägung waren zu den Tageszeiten zwischen 6:00 Uhr morgens und 21:00 Uhr abends Anhaltspunkte gegeben, dass überwiegende schutzwürdige Interessen von betroffenen Personen der Videoüberwachung entgegenstanden. Es war davon auszugehen, dass zu diesen Uhrzeiten neben den Besuchern der EinheitsEXPO eine Vielzahl von Personen wie beispielsweise Berufstätige, Touristinnen und Touristen oder Schülerinnen und Schüler als Unbeteiligte von der Videoüberwachung mitbetroffen waren und deren Daten anlasslos sowie ohne Anknüpfung an einen konkreten Verdacht erhoben wurden.

Wir teilten der Staatskanzlei diese Einschätzung mit und forderten sie auf, die Videoüberwachung entsprechend zu begrenzen. Darüber hinaus wiesen wir auf die Informationspflichten nach § 28 Absatz 2 BbgDSG i. V. m. Artikel 13 DS-GVO zur Gewährleistung der Transparenz der Datenverarbeitung hin. Im Rahmen einer unangekündigten Kontrolle vor Ort stellten Beschäftigte der Landesbeauftragten jedoch Verstöße gegen diese Vorgaben fest. Daraufhin behob die Staatskanzlei diese Missstände, indem sie die Videoüberwachung auf die Nachtzeit beschränkte und die Hinweisschilder an die Anforderungen der Datenschutz-Grundverordnung anpasste.

Die für eine Videoüberwachung erforderlichen, umfangreichen Unterlagen mit technisch-organisatorischem Bezug nach Artikel 5 Absatz 2 DS-GVO i. V. m. Artikel 24 ff. DS-GVO und § 4 Absatz 1 BbgDSG, welche bereits vor Beginn einer Verarbeitung personenbezogener Daten mittels Videokameras vorhanden sein müssen, wurden der Landesbeauftragten trotz Aufforderung nicht bereitgestellt und auch später nicht nachgereicht.

Aufgrund der festgestellten datenschutzrechtlichen Verstöße im Hinblick auf die unzulässige Datenverarbeitung mittels der vier Videokameras, die unzureichende Hinweisbeschilderung und das Fehlen sämtlicher Unterlagen mit einem technisch-organisatorischen Bezug hat die Landesbeauftragte die Staatskanzlei nach erfolgter Anhörung nach Artikel 58 Absatz 2 Buchstabe b DS-GVO verwarnt. Dies ist die höchste Form der Sanktion, die der Landesbeauftragten im öffentlichen Bereich zur Verfügung steht.

3 Mängel bei der Antragstellung für Corona-Soforthilfen

Um kleine Unternehmen, Soloselbständige und Angehörige der Freien Berufe, die durch die Covid-19-Pandemie in eine existenzbedrohliche wirtschaftliche Schieflage und in Liquiditätsengpässe geraten waren, zu unterstützen, hatte das Ministerium für Wirtschaft, Arbeit und Energie des Landes Brandenburg im März 2020 eine Richtlinie zur Gewährung einer Soforthilfe[6] erlassen. Die Investitionsbank des Landes Brandenburg (ILB) war für die Umsetzung dieser Richtlinie zuständig. Zur Beantragung des Fördergeldes war ein Förderantrag samt Unterlagen wie Handelsregisterauszügen, Gewerbeanmeldung, Personalausweiskopie mit Vorder- und Rückseite, Lohnjournalen und Steuerbescheiden einzureichen. Das Antragsverfahren der ILB sah vor, ihr diese Unterlagen hauptsächlich per gewöhnlicher E-Mail zuzusenden.

Die zur Antragstellung übermittelten Daten konnten jedoch auch sensitive Informationen enthalten, aus denen z. B. die Bonität bzw. Kreditwürdigkeit einer Person hervorgeht. Bei einer Kenntnisnahme solcher Daten durch unbefugte Dritte kann dies zu Rufschädigungen, zur Verhinderung von Vertragsabschlüssen, aber auch zum wirtschaftlichen Ruin führen. Die übermittelten Daten sind außerdem auch besonders lukrativ für Kriminelle, um beispielsweise Identitätsdiebstahl zu betreiben und Fördergelder zu erschleichen. Artikel 25 und 32 Datenschutz-Grundverordnung (DS-GVO) sehen vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit personenbezogener Daten planen und umsetzen muss. Letztendlich stellt eine lediglich transportverschlüsselte E-Mail-Kommunikation aus unserer Sicht keinen geeigneten Schutz gegen eine unbefugte Kenntnisnahme derartiger Daten dar. In Bezug auf die genannten sensitiven Daten kann dagegen eine Ende-zu-Ende-Verschlüsselung für E-Mails die Risiken un-

6 Richtlinie des Ministeriums für Wirtschaft, Arbeit und Energie des Landes Brandenburg zur Gewährung einer Soforthilfe für von der Corona-Krise 2020 unter Berücksichtigung der Vollzugshinweise für die Soforthilfen des Bundes für die Gewährung von Überbrückungshilfen als Billigkeitsleistungen für von der Corona-Krise in ihrer Existenz bedrohte kleine Unternehmen und Soloselbständige vom 24. März 2020 (ABl. 2020 Nr. 14S, S. 312/3).

befugter Zugriffe wirksam senken. Aufgrund der Beschwerde eines Bürgers konnten wir frühzeitig auf die unzureichenden technischen Vorkehrungen der ILB reagieren und darauf hinwirken, dass die Möglichkeit einer angemessen geschützten Übertragung, z. B. durch Ende-zu-Ende verschlüsselte E-Mails, eingerichtet wurde.

Soforthilfe rechtfertigt keinen Datenschutzverstoß

Die Art und Weise der E-Mail-Übertragung war allerdings nicht der einzige Verstoß gegen die Datenschutz-Grundverordnung, den wir im vorliegenden Fall festgestellt haben. Das Antragsformular enthielt eine Formulierung, die als „Einwilligung“ in eine zukünftig unver-schlüsselte E-Mail-Kommunikation zu verstehen war. Unsere Kritik bezog sich zum einen darauf, dass eine Einwilligung gemäß Artikel 7 DS-GVO immer freiwillig und informiert erfolgen muss. Die Antragsunterlagen enthielten jedoch keinerlei Erläuterung, was mit der E-Mail-Kommunikation bewirkt werden sollte. Da sich der Text direkt im Förderantrag befand, war aus dem Zusammenhang heraus auch die Freiwilligkeit nicht ersichtlich. Zum anderen besteht aus unserer Sicht für betroffene Personen nicht die Möglichkeit, wirksam darin einzuwilligen, dass Verantwortliche auf notwendige technische und organisatorische Maßnahmen, wie hier das Verschlüsseln, verzichten. Durch eine Einwilligung wird die Rechtmäßigkeit einer Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe a DS-GVO sichergestellt. Jedoch müssen auch für eine solche Verarbeitung die Grundsätze der Verordnung eingehalten werden. Das Einwilligen in einen Verstoß gegen die rechtlichen Regelungen ist nicht möglich. Die unverschlüsselte E-Mail-Kommunikation widerspricht jedoch Artikel 25 und 32 DS-GVO, wonach der Verantwortliche geeignete technische und organisatorische Maßnahmen, wie zum Beispiel das Verschlüsseln zum Schutz der Vertraulichkeit und Integrität, planen und umsetzen muss.

Hinzu kam, dass einige Informationen bzgl. der Antragstellung teilweise einseitig, schwer auffindbar oder sogar widersprüchlich waren. Der Verantwortliche muss solche Informationen zur Datenverarbeitung jedoch klar und transparent darstellen. Obwohl beispielsweise ein postalischer Versand der Antragsunterlagen möglich gewesen wäre, waren die Informationen hierzu gegenüber denjenigen zum E-Mail-Versand deutlich unterrepräsentiert und somit schwer auf-

findbar. Zeitweise verwies die Bank sogar darauf, dass postalisch gestellte Anträge nicht bearbeitet werden können.

Weiterhin bemängelten wir, dass nicht alle erhobenen personenbezogenen Daten für die nachfolgende Verarbeitung erforderlich waren. Beispielsweise sollten die Lohnjournale dazu dienen, die Anzahl der bei dem Antrag stellenden Unternehmen beschäftigten Personen festzustellen, weil dies für die Berechnung des Förderbetrags erforderlich war. Nicht erforderlich war es jedoch, die Namen dieser Personen zu erheben. Aufgrund der Tatsache, dass die Namen der Beschäftigten Daten von Dritten waren, wäre die Datenverarbeitung selbst dann nicht rechtmäßig gewesen, wenn die den Antrag stellende Person in die Verarbeitung eingewilligt hätte. Die ILB hätte vielmehr geeignete Maßnahmen ergreifen müssen, um diese unrechtmäßige Datenverarbeitung einzuschränken. Beispielsweise hätte sie bereits bei der Antragsstellung klarstellen müssen, welche Informationen tatsächlich notwendig sind und welche geschwärzt werden müssen.

Positiv ist anzumerken, dass die Investitionsbank auf einige unserer Kritikpunkte reagierte und so einen Teil der Verstöße gegen den Datenschutz schnell beseitigte. Gleichwohl prüften wir die Einleitung weiterer Maßnahmen und die Verhängung einer Sanktion gemäß Artikel 58 Absatz 2 DS-GVO. Aufgrund der Vielzahl der Verstöße und des Umfangs der Verarbeitung sprachen wir gegen Ende des Berichtszeitraums eine Verwarnung aus.

4 Versand von Bonitätsdaten per E-Mail nur mit ausreichender Verschlüsselung

Ein Beschwerdeführer, der bei einem Vermittler einen Kredit beantragt hatte, bemängelte, dieses Unternehmen habe ihn per lediglich transportverschlüsselter E-Mail und unter Angabe seiner Bonitätsdaten (negative Schufa-Einträge) über die Ablehnung seines Kreditwunsches informiert.

Diese Datenübermittelung stellt einen Verstoß gegen die Vorgaben des Artikels 32 Datenschutz-Grundverordnung (DS-GVO) zur Sicherheit der Datenverarbeitung dar. Anstelle der Transportverschlüsse-

lung wäre eine Ende-zu-Ende-Verschlüsselung der E-Mail geeignet und angemessen gewesen, um den Zugriff unbefugter Dritter auf Bonitätsdaten zuverlässig zu verhindern. Solche Zugriffe bergen die Gefahr, dass der betroffenen Person ein erheblicher Schaden entsteht, beispielsweise könnte ihr der Abschluss eines Mietvertrages verwehrt, ihre wirtschaftliche Existenz gefährdet oder ihr Ansehen empfindlich gestört werden.

Bonitätsdaten sicher übermitteln

Nachdem wir an das Unternehmen herangetreten waren, teilte es uns mit, dass es beabsichtige, in gleichgelagerten Fällen auch weiterhin Bonitätsdaten per transportverschlüsselter E-Mail zu versenden, da Bonitätsdaten – wie das Unternehmen argumentiert – nicht in eine der durch Artikel 9 DS-GVO geschützten, besonderen Kategorien personenbezogener Daten fallen. Es verwies auf Ausführungen anderer Datenschutzaufsichtsbehörden, aus denen sich allerdings lediglich ergab, dass die nach Artikel 9 DS-GVO besonders sensitiven Daten per Ende-zu-Ende-Verschlüsselung übermittelt werden müssen. Der Umkehrschluss, dass für den Versand von Bonitätsdaten, die der genannten Vorschrift nicht unterfallen, eine Transportverschlüsselung ausreicht, ergab sich daraus keineswegs.

Im Ergebnis hat die Landesbeauftragte gegenüber dem Unternehmen eine Warnung nach Artikel 58 Absatz 2 Buchstabe a DS-GVO für den Fall der Fortführung seiner bisherigen Vorgehensweise ausgesprochen. Berücksichtigt haben wir dabei auch, dass es bereits über eine Plattform verfügt, die den Kundinnen und Kunden einen ausreichend gesicherten Zugang ermöglicht. Eine Alternative zum lediglich transportverschlüsselten Versand von E-Mails ist somit bereits vorhanden.

Auf Nachfrage des Unternehmens erläuterten wir, dass auch eine Einwilligung der betroffenen Person den Verzicht auf eine Ende-zu-Ende-Verschlüsselung nicht rechtfertigen kann. Eine datenschutzrechtliche Einwilligung bezieht sich ausschließlich auf die Frage, ob die eigenen personenbezogenen Daten zu einem bestimmten Zweck verarbeitet werden dürfen, kann aber nicht Vorschriften zur Art und Weise ihrer Verarbeitung aushebeln. Verantwortliche sind somit u. a. an die Regelungen des Artikels 32 DS-GVO gebunden. Sie müssen

die daraus resultierenden technisch-organisatorischen Verpflichtungen für eine sichere Datenübermittlung erfüllen und können sich durch eine Einwilligung davon nicht entbinden lassen.

5 Innenansichten einer Einliegerwohnung im Internet

Bewohner einer Einliegerwohnung beschwerten sich über die Internetveröffentlichung von Innenaufnahmen ihrer Wohnräume durch ein Maklerbüro. Hintergrund war die Absicht des Eigentümers, das Haus zu verkaufen. Er hatte zu diesem Zweck einen Makler beauftragt und diesem Fotoaufnahmen – unter anderem mit Innenansichten der von den Beschwerdeführern genutzten Wohnung – zur Verfügung gestellt. Im Rahmen einer eigenen Wohnungsbesichtigung sicherte der Makler den betroffenen Bewohnern zu, auf Innenaufnahmen zu verzichten, um deren Privatsphäre zu schützen.

Das Maklerbüro erklärte in seiner Stellungnahme, dass der Eigentümer ihm die Innenaufnahmen zum Zweck der Veröffentlichung zur Verfügung gestellt habe. Welche der Bilder die Einliegerwohnung und welche andere Innenräume des Hauses zeigten, sei nicht ersichtlich gewesen.

Die Innenaufnahmen der Wohnung ließen – unter anderem mit Kenntnis der Adresse der Betroffenen – eine personenbezogene Verknüpfung mit den Bewohnern zu. Somit handelte es sich um personenbezogene Daten im Sinne des Artikels 4 Nummer 1 Datenschutz-Grundverordnung (DS-GVO).

Private Einblicke nur mit Zustimmung

Nach unserer Auffassung hätte sich das Maklerbüro vor einer Veröffentlichung von Wohnungsaufnahmen Klarheit darüber verschaffen müssen, welche Bilder den Wohnraum der Betroffenen zeigen. Die Zusicherung des Maklers, selbst nur Außenaufnahmen fertigen zu wollen, ließ den Schluss zu, dass er bereits für die Datenschutzbelange der Bewohner sensibilisiert war. Umso mehr konnten diese erwarten, dass er ihre schutzwürdigen Interessen berücksichtigen und auf eine Veröffentlichung der Innenaufnahmen ohne ihre Zustimmung verzichten würde.

Die Veröffentlichung der Innenaufnahmen durch das Maklerbüro war rechtswidrig, weil keine der in Artikel 6 Absatz 1 DS-GVO genannten Voraussetzungen für eine Datenverarbeitung erfüllt war. Insbesondere lag kein überwiegendes berechtigtes Interesse des Verantwortlichen vor. Die Landesbeauftragte hat deshalb gegenüber dem Maklerbüro eine Verwarnung nach Artikel 58 Absatz 2 Buchstabe b DS-GVO ausgesprochen.

6 Recht auf Auskunft umfasst alle Unternehmensbereiche

Das Recht auf Auskunft nach Artikel 15 Datenschutz-Grundverordnung (DS-GVO) stellt, im Zusammenspiel mit den Informationspflichten aus Artikel 13 und 14 DS-GVO, das zentrale subjektive Datenschutzrecht dar. Es soll zunächst sicherstellen, dass sich die betroffene Person bewusst ist, ob überhaupt sie betreffende Daten verarbeitet werden. Soweit dies zu bejahen ist, soll sie erfahren können, welche konkreten Daten dies sind, zu welchen Zwecken sie verarbeitet werden, wer die Daten erhält und wie lange sie gespeichert werden. Das Auskunftsrecht stellt vor diesem Hintergrund eine unverzichtbare Voraussetzung für die Ausübung weiterer datenschutzrechtlicher Ansprüche wie des Rechts auf Löschung, Berichtigung oder Widerspruch dar und ist deshalb auch als „Magna Charta des Datenschutzes“ bezeichnet worden. Nur wenn die Betroffenen um die jeweilige Verarbeitung wissen, können deren Rechtmäßigkeit beurteilt und Transparenz erreicht werden.

Ungeachtet dessen erreichten uns auch in diesem Berichtszeitraum wieder eine Vielzahl an Beschwerden, wonach Auskunftsersuchen betroffener Personen nicht, nicht rechtzeitig oder inhaltlich nicht ausreichend bearbeitet worden sind.

In einem Fall wurde die Auskunft gegenüber einer selbstständigen Geschäftsstelle eines bundesweit tätigen Anbieters von Wirtschaftsinformationen und Inkassodienstleistungen begehrt. Anstatt die gewünschte Auskunft über die verarbeiteten Daten zu erteilen, leitete das Unternehmen die Anfrage an eine andere Gesellschaft des Unternehmensverbundes weiter, welche für die Erteilung von Bonitätsauskünften zuständig ist. Da zu der anfragenden Person bisher keine

Wirtschaftsinformationen vorlagen und eine Beurteilung der Bonität insoweit nicht erfolge, teilte das Unternehmen schlicht mit, dass keine Verarbeitung personenbezogener Daten stattfinde.

Kurz darauf wandte sich die betroffene Person an beide Unternehmen und betonte, dass es nicht um eine Wirtschaftsauskunft im Sinne einer Bonitätsüberprüfung gehe, sondern vielmehr um die Erteilung der Auskunft nach Artikel 15 DS-GVO. Ferner zog sie unter Bezugnahme auf ein vorangegangenes Inkassoverfahren bei der Antragsgegnerin in Zweifel, dass dort keine personenbezogenen Daten verarbeitet werden. Hierauf erfolgte zunächst keine Rückmeldung durch das verantwortliche Unternehmen.

Wir hörten das Unternehmen vor diesem Hintergrund zum vorgebrachten Sachverhalt an und erläuterten unter anderem, dass Verantwortliche nach Artikel 12 Absatz 3 DS-GVO verpflichtet sind, Informationen über die auf Antrag ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats zur Verfügung zu stellen haben. Nur ausnahmsweise könne die Frist im Einzelfall aufgrund besonderer Komplexität oder der Anzahl von Anträgen verlängert werden. Im Rahmen der Stellungnahme führte der Verantwortliche aus, dass das konkrete Auskunftsersuchen völlig unbekannt sei. Auch im Rahmen einer Befragung der Mitarbeiterinnen und Mitarbeiter hätte sich niemand an ein solches Auskunftsverlangen erinnern können. Nun erstmals damit konfrontiert habe man jedoch eine Datenbankrecherche durchgeführt, konnte jedoch wiederum keine auf die Antrag stellende Person bezogenen Daten auffinden.

Verantwortliche tun sich mit Auskünften schwer

Verwundert ob dieses Ergebnisses teilten wir dem Verantwortlichen das Aktenzeichen zu dem vorangegangenen Inkassoverfahren mit und baten um neuerliche Überprüfung. Dieses Verfahren wurde schließlich noch bis Ende 2019 aktiv betrieben und sodann eingestellt. Daraufhin räumte der Verantwortliche ein, dass doch Daten der Antrag stellenden Person im Zusammenhang mit dem Inkassovorgang verarbeitet würden. Man habe das Auskunftsersuchen fälschlicherweise zunächst nur auf den Unternehmensbereich „Erteilung von Bonitätsauskünften“ bezogen und, nachdem dort keine

Einträge gefunden werden konnten, jedenfalls nicht hinreichend sorgfältig im Inkassobereich gesucht.

Das verantwortliche Unternehmen sicherte schließlich zu, alle Beschäftigten, die mit der Bearbeitung von datenschutzrechtlichen Auskunftsersuchen betraut sind, nochmals umfassend und detailliert zu diesem Thema zu schulen, insbesondere hinsichtlich des Erfordernisses einer vollständigen Suche in allen Unternehmensbereichen. Die Auskunft an die betroffene Person wurde daraufhin letzten Endes noch erteilt.

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

7 Recht auf Auskunft unabhängig vom Verwendungszweck

Ein Autofahrer war in einen Verkehrsunfall verwickelt und erhielt anschließend von einem Autovermieter das Angebot für einen Leihwagen, um die Zeit des Ausfalls seines eigenen Fahrzeugs zu überbrücken. Um zu erfahren, auf welcher Rechtsgrundlage das gegnerische Versicherungsunternehmen seine Daten an den Autovermieter weitergegeben hatte, wandte sich ein Rechtsanwalt für den Fahrer an die Versicherung. Gleichzeitig stellte er einen Antrag auf Auskunft nach Artikel 15 Datenschutz-Grundverordnung (DS-GVO). Als dieser auch nach Fristablauf unbeantwortet blieb, beschwerte der Betroffene sich bei der Landesbeauftragten.

In ihrer Stellungnahme erklärte die Versicherungsgesellschaft, die Datenübermittlung lasse sich auf den Verhaltenskodex des Gesamtverbandes der Deutschen Versicherungswirtschaft zum einheitlichen und transparenten Umgang mit personenbezogenen Daten von Versicherten, Interessenten und Betroffenen (Code-of-Conduct-Datenschutz) stützen. Daraus ergebe sich eine rechtliche Verpflichtung,

die nach Artikel 6 Absatz 1 Buchstabe c DS-GVO eine Datenübermittlung erlaube.

Die ausgebliebene Beantwortung des Auskunftsantrags begründete das Unternehmen damit, dass der Rechtsbeistand des Betroffenen seine Bevollmächtigung nicht nachgewiesen habe. Außerdem habe der Rechtsanwalt beantragt, die Auskunft selbst zu erhalten und die Absicht kommuniziert, die beantragten Daten in einer nach Auffassung der Versicherung rechtsmissbräuchlichen Weise zum Zweck der Geltendmachung zivilrechtlicher Ansprüche verwenden zu wollen.

Die Weitergabe der Daten des Betroffenen an den Autovermieter hielten wir im Ergebnis unserer datenschutzrechtlichen Prüfung unter der Voraussetzung für akzeptabel, dass der geschädigte Autofahrer zuvor den Wunsch geäußert hat, einen Mietwagen in Anspruch zu nehmen. Ist eine solche Absicht nicht bekannt, verstößt die Datenübermittlung an den Autovermieter gegen das Gebot der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c DS-GVO. Die Datenübermittlung kann dann auch unter Berücksichtigung des Verhaltenskodex der Versicherungswirtschaft nicht auf Artikel 6 Absatz 1 Buchstabe c DS-GVO gestützt werden.

Keine künstlichen Hindernisse für Auskünfte!

Die verwehrte Auskunftserteilung über die personenbezogenen Daten und ihre Verarbeitung durch die Versicherungsgesellschaft haben wir als Verstoß gegen die Vorschriften des Artikels 12 Absätze 2 bis 4 DS-GVO gewertet. Danach ist der betroffenen Person die Ausübung des Auskunftsrechts so leicht wie möglich zu machen. Sofern eine Auskunftserteilung nicht erfolgt, muss der Verantwortliche den Antragsteller fristgerecht über die Gründe hierfür informieren. Das Unternehmen hätte also auf die fehlende Bevollmächtigung des Rechtsanwalts hinweisen und so eine erneute Geltendmachung des Auskunftsrechts unter Vorlage einer ausreichenden Vollmacht ermöglichen müssen. Auch hätte die Auskunft unmittelbar an die betroffene Person gerichtet werden können.

Das Recht auf Auskunft besteht ohne Begründungserfordernis. Gibt der Antragsteller dennoch eine Begründung ab, ist dies rechtlich un-

beachtlich. Eine Absicht, die auf dem Wege der Auskunft erhaltenen Daten zu einem späteren Zeitpunkt in einem Zivilprozess zu verwenden, kann dem Auskunft Begehrenden somit nicht entgegengehalten werden. Die Landesbeauftragte hat im Ergebnis gegenüber dem Versicherungsunternehmen eine Verwarnung nach Artikel 58 Absatz 2 Buchstabe b DS-GVO wegen des Verstoßes gegen die beschriebenen Modalitäten für die Ausübung des Auskunftsrechts ausgesprochen.

8 Bericht der Bußgeldstelle

Im Berichtszeitraum wurden wieder zahlreiche Ordnungswidrigkeitenverfahren eingeleitet. Geahndet wurden datenschutzrechtliche Verstöße insbesondere von Unternehmen sowie von Mitarbeiterinnen und Mitarbeitern öffentlicher Stellen.

In 16 Fällen schlossen wir das Verfahren mit der Festsetzung von einer oder mehreren Geldbußen ab. Häufige Verstöße stellten unter anderem die Versendung von E-Mails an viele Empfänger unter Nutzung des CC-Adressfeldes, nicht ordnungsgemäß abgeschlossene Auftragsverarbeitungsverträge und unzureichend getroffene technische und organisatorische Maßnahmen für die Sicherheit der verarbeiteten Daten dar. Vermehrt wurden auch wieder unbefugte Abrufe aus dienstlich bereitgestellten Datenbanken durch Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen, darunter Polizeibedienstete, geahndet.

An dieser Stelle sei noch einmal auf Folgendes hingewiesen: Auch wenn Informationssysteme zu den täglichen Arbeitsmitteln zählen und die darin gespeicherten Daten über die Zugriffsberechtigung grundsätzlich zugänglich sind, muss für jede Nutzung ein konkreter dienstlicher Anlass gegeben sein.

8.1 Technisch unsichere Auskunftserteilung durch Unternehmen

Die Datenschutz-Grundverordnung ermöglicht es jeder natürlichen Person, von Unternehmen, Behörden oder sonstigen Verantwortlichen Auskunft darüber zu verlangen, ob und wenn ja, welche perso-

nenbezogenen Daten über sie gespeichert sind sowie über weitere Einzelheiten der Datenverarbeitung.

Ein Unternehmen entschied sich dazu, Auskunftsanfragen per E-Mail zu beantworten. An die E-Mail war ein passwortgeschütztes PDF-Dokument mit den beantragten Auskünften angehängt. Um das PDF-Dokument öffnen zu können, erhielten die betroffenen Personen wenige Minuten später eine zweite E-Mail, die das Passwort im Klartext enthielt. Diese zweite E-Mail war lediglich mit der standardmäßig voreingestellten Transport Layer Security (TLS) verschlüsselt, wenn dies vom jeweiligen E-Mail-Anbieter unterstützt wurde. Dabei handelt es sich um eine Verschlüsselung, die nur den Transportweg der E-Mail sichert. Sowohl auf dem Mail-Server des Absenders als auch auf demjenigen der Empfängerin oder des Empfängers liegt die E-Mail unverschlüsselt, also das Passwort im Klartext vor. Darüber hinaus war das Passwort durch das Unternehmen recht schwach und nach einem einfachen System gebildet. Es erfüllte nicht die nach dem Stand der Technik maßgeblichen und z. B. durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Sicherheitskriterien.

Die Landesbeauftragte hatte das Unternehmen bereits in der Vergangenheit darauf hingewiesen, dass die Vorgehensweise der Auskunftserteilung nicht den Vorgaben der Datenschutz-Grundverordnung (DS-GVO) entspricht. Daraufhin änderte das Unternehmen für einen Teil der Kundinnen und Kunden seine Praxis in eine datenschutzkonforme Weise. Durch eine Beschwerde erhielten wir einige Zeit später Kenntnis davon, dass das Unternehmen für einen anderen Teil der Kundschaft die Passwörter weiterhin per einfacher, höchstens TLS-verschlüsselter E-Mail versandte und auch an der unzureichenden Sicherheit der Passwörter selbst festhielt. Daraufhin leiteten wir ein Bußgeldverfahren gegen das Unternehmen wegen Verstoßes gegen Artikel 32 DS-GVO ein. Die Vorschrift verpflichtet zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten.

Maßgeblich war hierbei insbesondere der enge zeitliche und inhaltliche Zusammenhang zwischen der Versendung der ersten E-Mail mit den passwortverschlüsselten Auskunftsdokumenten und der

zweiten, nicht hinreichend gesicherten E-Mail mit dem Passwort. Unberechtigte Dritte, die die E-Mail-Kommunikation zwischen dem Unternehmen und der die Auskunft beantragenden Person abgefangen hätten, hätten zwar mit dem passwortverschlüsselten Anhang zunächst nicht viel anfangen können. Wenige Minuten später hätten sie die Dokumente allerdings mit dem im Klartext übermittelten Passwort entschlüsseln können. Die zu erteilenden Auskünfte enthielten auch sensitive personenbezogene Daten, die das Unternehmen durch geeignete und angemessene Maßnahmen vor einem Zugriff unberechtigter Dritter zu schützen verpflichtet ist. Dies hätte etwa durch eine Ende-zu-Ende-Verschlüsselung sichergestellt werden können. Hierbei ist die E-Mail nicht nur auf dem Transportweg, sondern auch auf den jeweiligen Mail-Servern verschlüsselt. Durch die angemessene Verschlüsselung wäre eine hohe Sicherheit für die personenbezogenen Daten der betroffenen Personen erreicht worden. Alternativ hätte das Passwort z. B. auch telefonisch übermittelt werden können.

Da wir das Unternehmen bereits in der Vergangenheit darüber informiert haben, dass die Vorgehensweise gegen die Vorgaben der Datenschutz-Grundverordnung verstößt, es für einen Teil der Kundinnen und Kunden aber weiterhin datenschutzwidrig agierte, verhängte die Landesbeauftragte eine Geldbuße in sechsstelliger Höhe. Positiv hervorzuheben ist, dass das Unternehmen inzwischen auf eine Auskunftserteilung per E-Mail verzichtet und seinen Kunden in allen Verfahren einen gesicherten Zugang zu einem Portal anbietet, in dem die Auskünfte datenschutzkonform bereitgestellt werden.

8.2 Fotos Minderjähriger im Internet

Im Rahmen einer Beschwerde wurde die Landesbeauftragte von einem Vater darüber informiert, dass Bilder seiner minderjährigen Tochter ohne seine Erlaubnis im Internet abrufbar waren. Veröffentlicht hatte sie die Betreiberin einer Ballettschule, bei der seine Tochter Tanzunterricht nahm. Zur Sachverhaltsaufklärung wurden sowohl die Homepage als auch die Facebook-Fanpage der Betreiberin gesichtet und zahlreiche Fotos gesichert. Dort waren neben der Tochter des Beschwerdeführers viele weitere Bilder von meist minderjährigen Tanzschülerinnen veröffentlicht.

Im Rahmen des zunächst geführten aufsichtsrechtlichen Verwaltungsverfahrens entfernte die Betreiberin alle Bilder der Tochter des Beschwerdeführers von ihrer Homepage und der Facebook-Fanpage. Zudem holte sie für die Veröffentlichung von Fotos mit anderen Kindern die schriftlichen Einwilligungserklärungen der Sorgeberechtigten ein. Für die Vergangenheit hatte sie nicht nachweisen können, dass solche Erklärungen wirksam abgegeben worden waren.

Aufgrund der Betroffenheit von Minderjährigen und der damit einhergehenden schweren Verstöße wurde der Fall hausintern an die Bußgeldstelle der Landesbeauftragten abgegeben und im Ergebnis drei Bußgelder festgesetzt. Zwei Geldbußen wurden gemäß Artikel 83 Absatz 5 Buchstabe a Datenschutz-Grundverordnung (DS-GVO) i. V. m. Artikel 6 Absatz 1 DS-GVO für je ein konkret veröffentlichtes Bild der minderjährigen Tochter des Beschwerdeführers erhoben und eine weitere gemäß Artikel 83 Absatz 5 Buchstabe a DS-GVO i. V. m. Artikel 5 Absatz 1 und 2 und Artikel 7 Absatz 1 DS-GVO für die fehlende schriftliche Dokumentation der Rechtmäßigkeit der Verarbeitung für die übrigen Fotoveröffentlichungen der minderjährigen Tanzschülerinnen.

Eine Veröffentlichung von Bilddaten im Internet geht mit unkalkulierbaren Risiken für die betroffenen Personen einher. So können eine Weiterverwendung der Bilder durch Dritte nicht kontrolliert und Löschansprüche oft nicht wirksam durchgesetzt werden. Kinder sind deshalb nach dem gesetzgeberischen Willen besonders zu schützen. Im Vergleich zu Erwachsenen ist besonders die kindgerechte Persönlichkeitsentwicklung zu wahren. Kinder und Jugendliche haben ein erhebliches Interesse daran, dass Dritte keine Fotos, auf denen sie individuell erkennbar sind, ohne eine ausdrücklich erklärte Einwilligung der Eltern im Internet veröffentlichen. Im vorliegenden Fall war erschwerend zu berücksichtigen, dass die betroffenen Kinder zum Teil nur in Ballettkleidung abgebildet waren.

Nicht nur an die Wirksamkeit einer Einwilligung sind strenge Voraussetzungen zu knüpfen, auch die Pflicht zur Rechenschaft ist besonders zu beachten. Gemäß Artikel 5 Absatz 2 i. V. m. Artikel 5 Absatz 1 Buchstabe a DS-GVO hat der Verantwortliche den Nachweis der Rechtmäßigkeit der Verarbeitung zu führen. Daneben normiert auch

Artikel 7 Absatz 1 DS-GVO explizit die Verpflichtung des Verantwortlichen, die Einwilligung der betroffenen Person nachzuweisen.

Die Betreiberin der Ballettschule hätte deshalb das Datum und den Inhalt der Einwilligungserklärungen (insbesondere auch in Bezug auf ihren Umfang in Hinblick auf die Veröffentlichung der Fotos) sowie die Art ihrer Einholung in geeigneter Form dokumentieren müssen. Die Erfüllung dieser Pflicht hatte die Unternehmerin versäumt.

Im Tutu im Internet

Unter Berücksichtigung der konkreten Tatumstände wurden drei Geldbußen, die insgesamt eine vierstellige Höhe erreichten, als tat- und schuldangemessen betrachtet. Die Betreiberin hat die festgesetzten Geldbußen akzeptiert.

8.3 Verliebt am Arbeitsplatz

Eine Arzthelferin einer brandenburgischen Arztpraxis speicherte die dort hinterlegte Telefonnummer eines Patienten in ihrem Mobiltelefon und kontaktierte ihn daraufhin privat. Diese Vorgehensweise missfiel nicht nur der Ehefrau des Patienten, die von dem Chatverlauf Wind bekam, sondern auch der Landesbeauftragten – wenn auch aus anderen Gründen.

Wir leiteten ein Bußgeldverfahren gegen die Arzthelferin wegen der unrechtmäßigen Verarbeitung personenbezogener Daten ein. Nach Artikel 6 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) dürfen personenbezogene Daten nur verarbeitet werden, wenn einer der dort genannten Erlaubnistatbestände vorliegt. Denn im Datenschutzrecht gilt der Grundsatz, dass eine Datenverarbeitung verboten ist, es sei denn, sie ist ausdrücklich gesetzlich erlaubt oder die Betroffenen stimmen zu. Das heißt, der Patient hätte darin einwilligen müssen, dass die Telefonnummer, die er in der Praxis zu Behandlungszwecken hinterlegt hatte, von der Arzthelferin privat verwendet wird.

Eine solche Einwilligung lag nicht vor. Vielmehr wandte sich der Patient mit einer Beschwerde über das Verhalten der Arzthelferin an die Landesbeauftragte. Wer in einer Arztpraxis behandelt wird, muss

davon ausgehen können, dass die dort angestellten Personen rechtmäßig mit den persönlichen Daten umgehen. Da dieser Grundsatz durch die Arzthelferin missachtet wurde, verhängte die Landesbeauftragte gegen sie ein Bußgeld in dreistelliger Höhe.

8.4 Polizist ruft Daten eines Prominenten beim Einwohnermeldeamt ab

Aus Neugier nutzte ein Bediensteter der brandenburgischen Polizei die dienstlich zur Verfügung stehenden Informationssysteme für private Zwecke. Unter Verwendung seiner dienstlichen Anwenderkennung fragte er beim Einwohnermeldeamt der Landeshauptstadt Potsdam die gespeicherten Daten zu einem prominenten Potsdamer ab.

Wer vorsätzlich entgegen den Vorschriften der Datenschutz-Grundverordnung, des Brandenburgischen Datenschutzgesetzes (BbgDSG) oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten, personenbezogene Daten, die nicht offenkundig sind, abruft, handelt nach § 32 Absatz 1 Nummer 2, 1. Variante BbgDSG ordnungswidrig.

Neugier kostet

Bei den beim Einwohnermeldeamt Potsdam gespeicherten Informationen (u. a. Name, Geburtsdatum, Wohnanschriften) handelt es sich um personenbezogene Daten, da sie Einzelangaben über die persönlichen Verhältnisse von identifizierten oder identifizierbaren natürlichen Personen enthalten. Diese Daten sind nicht offenkundig, der Zugriff auf sie ist gesetzlich beschränkt. Indem der Bedienstete die gespeicherten Daten des Prominenten über die polizeiliche Suchmaske anforderte, rief er die Daten ab. Unerheblich war dabei im Übrigen, dass zu der abgefragten Person eine Auskunftssperre gemäß § 51 Bundesmeldegesetz vermerkt war und er die erhofften Informationen deshalb gar nicht bekam.

Der Abruf erfolgte unbefugt, denn Abrufe nicht offenkundiger Daten in Recherchesystemen der Polizei sind nach § 39 Absatz 1 Satz 1 Brandenburgisches Polizeigesetz (BbgPolG) nur dann zulässig, wenn sie zur Erfüllung der Aufgaben erforderlich sind, also jeweils ein

dienstlicher Anlass besteht. Ein solcher war nicht gegeben, denn der Bedienstete gab an, lediglich aus eigenem Interesse recherchiert zu haben, ob bekannte Persönlichkeiten in der Landeshauptstadt Potsdam wohnen würden.

Sein ausschließlich privat motiviertes Handeln stellte im Ergebnis einen mit Bußgeld bewehrten Verstoß dar. Unter Berücksichtigung der konkreten Tatumstände wurde eine Geldbuße in dreistelliger Höhe als tat- und schuldangemessen betrachtet, die der Polizeibedienstete akzeptierte.

Bei Verstößen dieser Art setzen wir regelmäßig ein Bußgeld fest, da sie in hohem Maße geeignet sind, das Vertrauen der Allgemeinheit in die Rechtmäßigkeit des Umgangs mit personenbezogenen Daten durch die damit befassten öffentlichen Stellen empfindlich zu beeinträchtigen.

III Anlasslose Prüfungen

1 Überprüfung der Webseiten von Kommunen auf Verschlüsselung

Im Berichtszeitraum prüften wir systematisch die Webseiten von Landkreisen, kreisfreien Städten, Ämtern, Städten und amtsfreien Gemeinden im Land Brandenburg. Diese verfügen häufig über Webformulare, mit denen Bürgerinnen und Bürger Kontakt zur Verwaltung aufnehmen können – die Spanne reicht von einfachen Gästebüchern über Anmeldungen zum Versand eines Newsletters oder zu Veranstaltungen bis hin zu Anträgen für Verwaltungsdienstleistungen. In der Regel sind dabei auch personenbezogene Daten anzugeben wie z. B. der Name, die Anschrift oder die E-Mail-Adresse. Uns fiel auf, dass mehrere Verwaltungen bei der Übertragung der so erhobenen Daten über das Internet auf eine Transportverschlüsselung z. B. mittels TLS-Protokoll (Transport Layer Security) verzichteten. Diese ist am Präfix https:// der Internetadresse erkennbar. Das zugehörige TLS-Zertifikat bestätigt, dass der Verantwortliche Betreiber der Webseiten ist.

Gemäß Artikel 32 Absatz 1 Datenschutz-Grundverordnung (DS-GVO) haben der Verantwortliche und gegebenenfalls der Auftragsverarbeiter unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Des Weiteren benennt Artikel 32 Absatz 1 Buchstabe a DS-GVO die Verschlüsselung als eine geeignete Maßnahme. Klar ist, dass eine unverschlüsselte Übertragung personenbezogener Daten über das Internet (z. B. mittels unverschlüsselter Webformulare) Risiken für die Vertraulichkeit und die Integrität der Daten mit sich bringt und einen Verstoß gegen Artikel 32 DS-GVO darstellt. Dies kann vermieden werden, indem die Daten bei der Übertragung gemäß dem Stand der Technik, z. B. mittels TLS, verschlüsselt werden. Hinweise zur Verwendung von TLS können der Technischen Richtlinie TR-02102-2 des Bundesamtes für Sicherheit in der Informationstechnik entnommen werden.

Die Webseiten der Verwaltungen prüften wir einzeln hinsichtlich des Einsatzes einer Transportverschlüsselung. Darüber hinaus stellten wir fest, ob dort Formulare enthalten waren, mit denen personenbezogene Daten erhoben wurden und ob die Übermittlung dieser Daten verschlüsselt erfolgte.

Insgesamt fanden wir 38 Kommunalverwaltungen, die keine verschlüsselte Übertragung personenbezogener Formulardaten implementiert hatten. Wir wiesen die Verantwortlichen auf den damit verbundenen Verstoß gegen datenschutzrechtliche Vorschriften hin und forderten sie auf, einen rechtskonformen Zustand herzustellen. Hierfür unterbreiteten wir ihnen zwei Vorschläge: Entweder sie beendeten jegliche Erhebung personenbezogener Daten über Formulare auf ihren Webseiten oder sie rüsteten eine Transportverschlüsselung per TLS nach.

Im Laufe der Antwortfrist erhielten wir viele Bestätigungen, dass die geforderten Anpassungen nun umgesetzt seien, kleinere Rückfragen und positive Rückmeldungen von Administratoren, welche sich in ihrer jeweiligen Verwaltung schon lange für eine Verschlüsselung ausgesprochen hatten, hierfür jedoch keine offenen Ohren fanden. Einige Verantwortliche meldeten sich zwar nicht zurück, hatten aber am Ende der von uns gesetzten Frist dennoch alle Anforderungen umgesetzt. Lediglich eine Amtsverwaltung hatte weder auf unsere Schreiben geantwortet noch die erforderlichen Änderungen vorgenommen. Bei einem Telefonat mit dem Amtsdirektor gab dieser an, die Umsetzung einer TLS-Verschlüsselung bereits angeordnet zu haben. Zu einer praktischen Implementierung war es allerdings bis zum gegebenen Zeitpunkt nicht gekommen, sodass er eine Nachbesserung ankündigte, die wir Anfang 2021 überprüfen werden.

2 Kreditinstitute: Der Auftraggeber bleibt in der Verantwortung

Aufgrund zahlreicher Meldungen von Datenschutzverletzungen gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) innerhalb eines Jahres entschloss sich die Landesbeauftragte, ein Kreditinstitut in Brandenburg vor Ort zu prüfen. Im Fokus der im September 2020 durchgeführten Kontrolle standen das Druckerkonzept, die Datenvernichtung, Schulungen und allgemeine Verhaltensregelungen des

Kreditinstituts (z. B. der typische Verlauf beim Postversand). Die Prüfung folgte auf ein im März 2020 geführtes Beratungsgespräch und diente insbesondere der Kontrolle der erzielten Ergebnisse. An zwei Standorten verschafften wir uns einen Überblick darüber, wie einzelne Beschäftigte des Kreditinstituts personenbezogene Daten in ihrem Alltagsgeschäft verarbeiten, z. B. beim Umgang mit datenschutzgerecht zu vernichtenden Papierunterlagen oder dem PIN-gesteuerten Ausdruck von Dokumenten.

Im Rahmen der Prüfung stellten wir fest, dass sich an allen Arbeitsplätzen Papierkörbe befanden, welche ausschließlich für den datenschutzrelevanten Papiermüll vorgesehen waren. Dieser wurde einmal täglich durch einen Dienstleister, der mit der Reinigung beauftragt war, in Müllsäcken gesammelt und in einem für die Öffentlichkeit unzugänglichen Bereich der Geschäftsstelle bis zur Abholung zwischengelagert. Hierbei handelte es sich um einen Archivraum, in dem gleichzeitig Bonitätsdaten der Kundinnen und Kunden so gelagert wurden, dass das Reinigungspersonal diese Daten auch hätte zur Kenntnis nehmen können.

Darüber hinaus wurden in einigen Fällen auch vertrauliche Daten in öffentlich zugänglichen Papiercontainern entsorgt und getroffene Weisungen der Bank somit in mehreren Fällen nicht eingehalten. Auch das Kreditinstitut als Verantwortlicher prüfte insofern nicht hinreichend, ob das Reinigungsunternehmen die Aufträge korrekt durchführte.

Die Landesbeauftragte empfahl, die datenschutzkonforme Entsorgung von Papierunterlagen in allen Teilschritten besser zu koordinieren und zu überwachen, um Fehler zu vermeiden. Zudem musste das Archiv umgehend vor möglichen Zugriffen unberechtigter Dritter, z. B. Mitarbeiterinnen und Mitarbeitern des Reinigungspersonals, gesichert werden. Wir machten gegenüber der Bank deutlich, dass bestehende Sicherheitslücken zu Lasten des Verantwortlichen gehen, weshalb ein eingesetzter Auftragsverarbeiter, wie z. B. ein Reinigungsunternehmen, hinsichtlich der Einhaltung getroffener Verpflichtungen durch den Verantwortlichen stetig zu kontrollieren ist.

Aufgrund zahlreicher Meldungen der Bank gemäß Artikel 33 DS-GVO, aus denen hervorging, dass Dokumente an falsche Empfängerinnen und Empfänger versandt wurden, prüften wir das bestehende Druckerkonzept und die Praktikabilität der Druckfunktionen. Es war davon auszugehen, dass der Fehlversand von Dokumenten auch darauf zurückzuführen war, dass Ausdrucke anderer Kolleginnen oder Kollegen noch im Drucker lagen, mitgegriffen und ohne weitere Kontrolle verschickt wurden – häufig als Folge von Stresssituationen im Arbeitsalltag. Wir haben daher empfohlen, Druckaufträge ausschließlich per PIN-Funktion an den Drucker zu senden. Diese Funktion verlangt bei jedem Druckauftrag die Vergabe einer PIN. Erst nach Eingabe dieser Nummer am Drucker wird der Druck ausgelöst. Das Risiko, Dokumente im Drucker zu vergessen und ausgedruckte Dokumente zu vertauschen, wird dadurch verringert.

Ohnmacht bei der Auftragsvergabe

Bisher konnten die Beschäftigten den PIN-Druckauftrag auf einem wenig anwenderfreundlichen Weg einstellen; verpflichtend war dies jedoch nicht. In der Regel wurde die Anwendung aus Praktikabilitätsgründen nicht genutzt. Die Landesbeauftragte hat deshalb eine zwingende Voreinstellung empfohlen. Die Bank problematisierte daraufhin, dass nur der beauftragte IT-Dienstleister eine derartige Umstellung vornehmen könne. Dieser ist jedoch bundesweit für eine Gruppe von Kreditinstituten aktiv und systemseitige Änderungen würden sich auf alle Auftraggeber auswirken. Wir machten deutlich, dass der Verantwortliche und nicht der Auftragsverarbeiter über technische Details der Datenverarbeitung bestimmen können muss.

Die Bank teilte uns mit, dass sie Änderungen in ihren Geschäftsprozessen prüft, um die festgestellten Mängel abzustellen. Die Bank stellte zudem die Klärung der Problematik zur Auftragsverarbeitung durch den Dienstleister in Aussicht. Wir werden uns im Frühjahr 2021 über die Fortschritte informieren. Hinsichtlich der Absicherung des Archivs mit den Bonitätsdaten wurden Schutzmaßnahmen umgesetzt.

IV Ausgewählte Fälle

1 Nachweis von Masernimpfungen der Schülerinnen und Schüler

Das am 1. März 2020 in Kraft getretene Masernschutzgesetz[7] sieht unter anderem vor, dass Schülerinnen und Schüler den Nachweis über einen ausreichenden Impfschutz gegen Masern erbringen müssen. Seit Einführung dieser Verpflichtung erreichten uns zahlreiche Beschwerden und Anfragen von Eltern zum Umgang der Schulen mit den vorgelegten Impfnachweisen. Diese wurden teilweise einfach in Kopie zur Schülerakte genommen.

Die Art und Weise, wie der Nachweis für einen ausreichenden Impfschutz der Schülerinnen und Schüler an den Schulen zu dokumentieren ist, geht aus einem Rundschreiben des Ministeriums für Bildung, Jugend und Sport hervor.[8] Es enthält als Anlage eine Musterbescheinigung. Eltern können diese verwenden, um den Impfschutz durch die Ärztin bzw. den Arzt oder durch das Gesundheitsamt bestätigen zu lassen. Ebenso ist es möglich, dass die Schule die Bescheinigung ausfüllt, nachdem die Eltern ihr die Impfdokumentation bzw. den Impfausweis des Kindes vorgelegt haben. Die ausgefüllte Bescheinigung wird dann in beiden Fällen als Bestätigung des Impfschutzes zur Schülerakte genommen.

Kopien der Impfdokumentation bzw. des Impfausweises selbst dürfen weder von den Sorgeberechtigten verlangt, noch von der Schule angefertigt oder in der Schülerakte abgelegt werden. Die Impfdokumentation bzw. der Impfausweis enthalten in der Regel medizinische Informationen, deren Datenumfang über die Nachweispflicht für die Masernimpfung hinausgeht. Diese zusätzlich zu speichern, ist nicht erforderlich und widerspricht dem Grundsatz der Datenminimierung. Auch mit Einwilligung der Eltern ist eine solche Datenspeicherung unzulässig.

---

7 Gesetz für den Schutz vor Masern und zur Stärkung der Impfprävention (Masernschutzgesetz) vom 10. Februar 2020 (BGBl. I, Nr. 6 vom 13. Februar 2020, S. 148).

8 Rundschreiben 7/20 vom 18. März 2020 zum Nachweis gemäß § 20 Absatz 9 des Infektionsschutzgesetzes über einen ausreichenden Impfschutz gegen Masern bei Schülerinnen und Schülern (ABl. MBJS 2020, Nr. 11).

Vor dem Hintergrund der bei uns eingegangenen Anfragen und Beschwerden haben wir den staatlichen Schulämtern empfohlen, die Schulen auf das Erfordernis einer datenschutzgerechten Dokumentation der Impfnachweise hinzuweisen. An der Erarbeitung dieser Hinweise haben wir uns schließlich mit konkreten Änderungs- und Ergänzungsvorschlägen beteiligt.

2 Auskunft zu Datenübermittlungen so konkret wie möglich

Artikel 15 Absatz 1 Buchstabe c Datenschutz-Grundverordnung (DS-GVO) enthält unter anderem ein Recht auf Auskunft über die „Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden“. Von diesem Recht wollte ein Beschwerdeführer gegenüber dem Landesbetrieb Landesvermessung und Geobasisinformation Gebrauch machen und stellte einen entsprechenden Antrag auf Auskunft.

Hintergrund der Datenverarbeitung, um die es in dem Fall ging, war die Vorschrift des § 10 Brandenburgisches Vermessungsgesetz. Danach übermittelt der Landesbetrieb unter bestimmten Voraussetzungen personenbezogene Geobasisinformationen an öffentliche oder nicht öffentliche Stellen. So verfuhr er auch mit den Daten zum Grundstück des Beschwerdeführers. Dieser hatte anschließend einen begründeten Anlass zu erfragen, an welche Empfängerinnen und Empfänger der Landesbetrieb seine personenbezogenen Grundstücksdaten weitergegeben hat.

Blackbox Datenempfänger

In seiner Antwort ging der Landesbetrieb davon aus, dass es genügte, dem Antragsteller lediglich die Kategorien von Datenempfängerinnen und -empfängern mitzuteilen. Als Kategorien sind beispielsweise Angaben wie „Kaufinteressierte“, „Maklerinnen“ bzw. „Makler“ oder „Behörden des Landkreises“ zu verstehen. Der Landesbetrieb beschränkte seine Auskunft auf solche Kategorien, obwohl er Angaben zu den genauen Empfängerinnen und Empfängern gespeichert hatte. Dies begründete er mit der Formulierung des Artikels 15 Absatz 1 Buchstabe c DS-GVO: Angesichts der Verbin-

dung durch den Begriff „oder“ enthalte die Vorschrift keine Rangfolge. Es bestehe sozusagen eine freie Auswahl, ob die Kategorien von Datenempfängerinnen und Datenempfängern oder die konkreten Stellen benannt werden.

Diese Auffassung teilten wir nicht. Wir sind vielmehr der Ansicht, dass die Kenntnis der Identität der konkreten Datenempfängerinnen und Datenempfänger neben der allgemeinen Information der betroffenen Person auch dazu dient, die Rechtmäßigkeit der Datenübermittlung zu überprüfen. Zweck der Vorschrift ist es, der betroffenen Person zu ermöglichen, die Weitergabe ihrer Daten auch über längere Übermittlungsketten hinweg nachzuvollziehen. Nur so kann sie bei allen Stellen, die ihre Daten erhalten haben, weitere Auskunftsansprüche stellen oder andere Betroffenenrechte wie beispielsweise die Löschung bzw. Berichtigung ihrer Daten oder die Einschränkung der Verarbeitung bewirken. Dieser Normzweck wird verfehlt, wenn eine auskunftspflichtige Stelle trotz vorliegender Angaben über die konkreten Datenempfängerinnen und -empfänger lediglich die Kategorien nennt.

Die Begriffe „Empfänger“ und „Kategorien von Empfängern“ stehen in der oben zitierten Vorschrift also nicht alternativ nebeneinander. Werden konkrete Empfängerinnen und Empfänger gespeichert und ist die Weitergabe dieser Angaben nicht durch eine anderweitige gesetzliche Regelung (z. B. durch § 11 Brandenburgisches Datenschutzgesetz) ausgeschlossen, muss die Auskunft immer die konkreten Angaben enthalten. Die Beschränkung der Auskunft auf Kategorien kommt nur für den Ausnahmefall infrage, dass zulässigerweise ausschließlich Angaben zu diesen Kategorien vorliegen.

Im Ergebnis kam der Landesbetrieb unserer Aufforderung nach, die konkreten Empfängerinnen und Empfänger gegenüber dem Beschwerdeführer zu benennen. Zwar bemängelte der Beschwerdeführer anschließend, ihm seien die Zwecke der Datenspeicherung bei den Empfängerinnen oder Empfängern vorenthalten worden. Wir teilten ihm jedoch mit, dass diese dem Auskunftsanspruch an die übermittelnde Stelle nicht unterfallen und er einen entsprechenden Antrag an die Daten empfangenden Stellen richten muss.

3 Nutzung von Drohnen durch ein Immobilienunternehmen

Ein Immobilienunternehmen fertigte zur besseren Vermarktung eines mit einem Einfamilienhaus bebauten Grundstücks Luftaufnahmen von der örtlichen Lage an. Dafür setzte es eine Kameradrohne ein, die ein Wohngebiet, in dem das in Rede stehende Grundstück lag, mehrmals überflog. Die so erstellten Aufnahmen wurden dem Exposé beigefügt und anschließend auf der gewerblichen Webseite des Unternehmens veröffentlicht. Zu erkennen war auf den Bildern sowohl das eigentlich zu vermarktende Objekt als auch die angrenzenden Grundstücke. So wurden beispielsweise die privaten Gärten und Sonnenterassen aus der Nachbarschaft im Internet gezeigt. Dies führte dazu, dass eine Anwohnerin ihr Privatgrundstück wiedererkannte und die Bilder umgehend von der Seite entfernt haben wollte.

Aus der Abbildung eines Grundstückes in seinen Einzelheiten lassen sich personenbeziehbare Daten ableiten, sodass mittels der Aufnahmen einer Kameradrohne solche Daten verarbeitet werden. Zudem ermöglicht ein Überflug, selbst schwer zugängliche Orte zu filmen. Das ist für Private besonders belastend, da sie versuchen, durch Zäune, Hecken oder sonstige Abtrennungen den Einblick auf ihren privaten Bereich zu verhindern oder zu erschweren. Diese Vorkehrungen werden mittels einer Kameradrohne umgangen.

Um diese Risiken zu vermeiden, wurden in der Luftverkehrsordnung (LuftVO) spezielle Vorschriften geschaffen, die den Einsatz von Drohnen an strenge Vorgaben knüpfen. So sieht § 21b Absatz 1 Ziffer 7 LuftVO ein Verbot des Betriebs einer Drohne vor, wenn diese elektronische Bildaufnahmen anfertigen kann, Wohngrundstücke überfliegt und die betroffenen Eigentümerinnen und Eigentümer oder sonstige Nutzungsberechtigte dem Überflug nicht ausdrücklich zugestimmt haben. Daneben sind die Vorschriften der Datenschutz-Grundverordnung (DS-GVO) zu beachten. Für Privatpersonen bedeutet das, dass der Einsatz auf dem eigenen Grundstück erlaubt ist, solange das Nachbargrundstück nicht miterfasst wird. In unserem Fall bezweckte das Unternehmen mit den Aufnahmen eine bestmögliche Vermarktung des Grundstücks. Der Einsatz war der gewerblichen Tätigkeit des Unternehmens zuzuordnen, sodass es für die

Verarbeitung der personenbezogenen Daten einer Rechtsgrundlage bedurfte. Als Rechtsgrundlage kam Artikel 6 Absatz 1 Buchstabe f DS-GVO in Betracht. Nach dieser Regelung ist die Verarbeitung personenbezogener Daten zulässig, wenn dies zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Die Landesbeauftragte verneinte bereits die Erforderlichkeit der Luftaufnahmen der weiteren Grundstücke für eine Vermarktung des Objektes. Die Erforderlichkeit ist nur anzunehmen, wenn und soweit die konkrete Art und Weise der Überwachung geeignet ist, den Zweck zu erreichen, und es keine andere, weniger in die Grundrechte und Grundfreiheiten eingreifende Möglichkeit gibt (sogenanntes milderes Mittel). Zwar waren die angefertigten Luftaufnahmen grundsätzlich geeignet, das Objekt grafisch ansprechend abzubilden. Jedoch hätte sich das Unternehmen im Vorfeld mit alternativen Darstellungsformen auseinandersetzen müssen. Denkbar wäre es gewesen, das Grundstück mit einem Lageplan, auch in einem 3D-Format, genau auszuweisen. Mit dieser Darstellung hätte das Unternehmen auch weniger in die Rechte der betroffenen Personen eingegriffen und das Grundstück dennoch maßstabsgetreu abbilden können.

Bei Drohnen wachsam sein

Im Ergebnis ist das Recht der Betroffenen u. a. an einer räumlichen Rückzugsmöglichkeit auf ihrem Grundstück zu wahren. Nicht genehmigte Luftaufnahmen des eigenen Grundstücks durch Dritte sind unzulässig. Im Laufe unseres Verfahrens nahm das Unternehmen freiwillig die Aufnahmen von der Webseite.

Die Landesbeauftragte sprach gegenüber dem Unternehmen dennoch einen rechtlichen Hinweis gemäß Artikel 58 Absatz 1 Buchstabe d Datenschutz-Grundverordnung (DS-GVO) aus. Ihm sollte verdeutlicht werden, dass es beim Einsatz einer Kameradrohne datenschutzrechtliche Bestimmungen einzuhalten hat. Betreiberinnen und Betreiber von Drohnen, die mit einer Videokamera ausgerüstet sind, müssen auch beachten, dass ihnen bei der Verarbeitung perso-

nenbezogener Daten Hinweispflichten nach Artikel 12 ff. DS-GVO sowie technische und organisatorische Maßnahmen gemäß Artikel 32 DS-GVO auferlegt werden. Weitere Informationen können der Orientierungshilfe Videoüberwachung durch nicht öffentliche Stellen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) oder dem Positionspapier der Datenschutzkonferenz, in dem sie ihre Rechtsauffassung zur Nutzung von Kameradrohnen durch nicht öffentliche Stellen darlegt, entnommen werden. Beide Papiere stehen in unserem Internetangebot zur Verfügung.

4 Sicherheitsvorfälle und Datenschutzverletzungen im Zusammenhang mit der Schul-Cloud Brandenburg

Bereits in vergangenen Tätigkeitsberichten hatten wir über datenschutzrechtliche Aspekte bei der Nutzung von Lernplattformen im Allgemeinen[9] und über die vom Potsdamer Hasso-Plattner-Institut (HPI) entwickelte Schul-Cloud im Besonderen[10] berichtet. Nachdem für das Jahr 2020 ursprünglich die Nutzung der HPI-Schul-Cloud in ca. 50 brandenburgischen Schulen geplant war, kam es durch die Notwendigkeit des Distanzlernens während der Corona-Pandemie zu einer raschen Erhöhung dieser Zahl. Gegen Ende des Berichtszeitraums nutzten fast 600 Schulen in Brandenburg das Angebot. Aus datenschutzrechtlicher Sicht sind sie hierbei Verantwortliche im Sinne der Datenschutz-Grundverordnung (DS-GVO). Das HPI agiert als Auftragnehmer einer Auftragsverarbeitung und hat verschiedene Unterauftragnehmer z. B. zur Erbringung von Rechenzentrumsdienstleistungen oder zur Einbindung von Lerninhalten.

Im Mai 2020 gab es in den Medien nacheinander Berichte über drei Sicherheitslücken in der Schul-Cloud. Diese wurden durch Journalistinnen und Journalisten zunächst an andere deutsche Aufsichtsbehörden herangetragen, welche uns kollegial informierten. Zum Teil wandten sich die Medien auch das HPI selbst und stellten kritische Nachfragen. Konkret ging es um unberechtigte Registrierungen neu-

9 Tätigkeitsbericht 2016/2017, B 13.1.1.
10 Tätigkeitsbericht Datenschutz 2019, A II 2.

er Nutzerkonten in der Schul-Cloud, um die öffentliche Einsehbarkeit von Tickets zur Beseitigung von Fehlern in der Lernplattform sowie um die fehlerhafte Konfiguration eines allgemeinen Chat-Raumes. Alle Lücken führten zu einer Verletzung der Vertraulichkeit personenbezogener Daten und somit auch zu einer Verletzung des Datenschutzes.

Die unberechtigten Registrierungen neuer Nutzerkonten wurden durch eine Verkettung mehrerer Fehler ermöglicht. Für manche Schulen war in der Schul-Cloud die Selbstregistrierung von Nutzerinnen und Nutzern vorgesehen. Hierzu war ein schulweit einheitlicher Registrierungslink zu verwenden. Die Selbstregistrierung diente eigentlich der Vereinfachung der Administration, da nicht alle Schülerinnen und Schüler zentral von einer verantwortlichen Lehrkraft angelegt werden mussten. Einige Schulen publizierten den Registrierungslink jedoch im Internet, wodurch insbesondere seine Struktur öffentlich wurde. Teil des Links war auch eine eindeutige, einfach bestimmbare Schulnummer. Durch Manipulation der Internetadresse konnten Unberechtigte sich einen gültigen Registrierungslink für andere Schulen erzeugen und dort – falls diese Form der Nutzerregistrierung freigeschaltet war – neue Nutzerkonten anlegen. Die Schulen prüften offenbar nicht, ob zu jedem neuen Konto auch tatsächlich eine berechtigte natürliche Person gehörte. Über das unberechtigt registrierte Nutzerkonto war es anschließend möglich, Nutzergruppen (Teams) in der Schul-Cloud anzulegen, wenn diese Option für die Schule aktiviert war. In diesem Zusammenhang hatten die Unbefugten Zugriff auf Namen, Vornamen und Klassenzugehörigkeit aller Nutzerinnen und Nutzer der jeweiligen Schule.

Missbräuchliche Registrierungen unberechtigter Personen in der Schul-Cloud wurden deutschlandweit bei insgesamt 13 Schulen festgestellt. Die Anzahl der Personen, deren Daten eingesehen werden konnten, variierte je nach Anzahl der für die jeweilige Schule angelegten Nutzerinnen und Nutzer. In Brandenburg waren drei Schulen mit Echtdaten betroffen, weitere sogenannte Testschulen hatten keine echten Daten hinterlegt. Das HPI schloss die Sicherheitslücke kurzfristig, indem die Funktion zur Selbstregistrierung über einen schulweiten Registrierungslink abgeschaltet wurde. Des Weiteren durchsuchte das Institut die Datenbank nach auffälligen Nutzer-

konten anhand der zur Registrierung verwendeten E-Mail-Adressen, sicherte diese Konten und löschte sie anschließend. Ferner hat das HPI alle am Projekt teilnehmenden Schulen über den Vorfall informiert und sie gebeten, zusätzlich eigenständig die bei ihnen angelegten Nutzerkonten auf verdächtige und bisher unerkannte Personen zu untersuchen. Weiterhin wurden die Schulen sensibilisiert, bei entsprechenden Funden ihrer zuständigen Datenschutzaufsichtsbehörde gemäß Artikel 33 DS-GVO eine Verletzung des Datenschutzes zu melden. Für die betroffenen brandenburgischen Schulen geschah dies.

Die zweite Sicherheitslücke bezog sich auf das vom HPI selbst betriebene Ticketsystem der Schul-Cloud. Über dieses System können Nutzerinnen und Nutzer die Softwareentwickler über Fehler in der Plattform informieren. Durch einen Mangel in der Konfiguration waren Teile des Ticketsystems öffentlich einsehbar. Da Tickets grundsätzlich auch personenbezogene Daten (zumindest der bzw. des Meldenden) enthalten und in zwei Fällen sogar Listen mit personenbezogenen Daten anderer Nutzerinnen und Nutzer der Schul-Cloud eingebettet waren, lag auch hier eine Datenschutzverletzung vor. Konkret ging es um 21 Tickets und 68 betroffene Personen, deren Namen, E-Mail-Adressen und z. T. Telefonnummern öffentlich wurden.

Informationssicherheit als kontinuierliche Aufgabe

Das HPI bestätigte den Vorfall und gab wegen seiner eigenen datenschutzrechtlichen Verantwortlichkeit eine Meldung nach Artikel 33 DS-GVO an uns als zuständige Aufsichtsbehörde ab. Der Fehler selbst war allerdings im Rahmen regelmäßiger Projektarbeiten bereits vor der Veröffentlichung in den Medien aufgefallen und zeitnah geschlossen worden. Im Ergebnis konnten nur noch berechtigte Personen auf das Ticketsystem zugreifen. Sie wurden außerdem durch das HPI darüber belehrt, keine zusätzlichen personenbezogenen Daten in Tickets aufzunehmen.

Auch der dritte Vorfall resultierte aus einer Fehlkonfiguration. Das in der Schul-Cloud integrierte Chat-System hatte einen allgemeinen Chat-Raum, in dem sich alle Nutzerinnen und Nutzer Nachrichten schreiben konnten. Dieser Raum war bei der Ersteinrichtung durch das HPI zentral deaktiviert worden. Als im Zuge eines planmäßigen

Updates auch das Chat-System aktualisiert wurde, versäumten die Verantwortlichen jedoch die erneute Deaktivierung des allgemeinen Chat-Raumes. Aus diesem Grund war es Unbefugten seit diesem Zeitpunkt möglich, durch eine gezielte Manipulation der Internetadresse zum Aufruf dieses Chat-Raums die Namen und Vornamen anderer Nutzerinnen und Nutzer einzusehen, aber nicht deren E-Mail-Adressen oder Chat-Beiträge. Das HPI hat den Fehler umgehend behoben.

Im Rückblick ist positiv hervorzuheben, dass das HPI stets sehr offen und transparent mit allen Informationen im Hinblick auf die Sicherheitsvorfälle und Datenschutzverletzungen umgegangen ist. Die Öffentlichkeit wurde immer aktuell auf dem Laufenden gehalten und konnte alle Erkenntnisse und Aktivitäten über das Weblog der Schul-Cloud verfolgen. Das Institut handelte stets schnell und koordinierte alle Tätigkeiten über einen eigens eingerichteten Krisenstab. Darüber hinaus wurde uns mitgeteilt, dass auch unabhängig von den konkreten Vorfällen bereits mit externen IT-Sicherheitsaudits der Schul-Cloud begonnen worden war, durch die einige weitere Sicherheitslücken festgestellt und beseitigt werden konnten. Das HPI hat auch Maßnahmen für ein verbessertes Informationssicherheitsmanagement sowie zur Sensibilisierung der Projektmitarbeiterinnen und -mitarbeiter für Fragen des Datenschutzes und der Informationssicherheit ergriffen.

5 Cloud-Lösungen von Microsoft im Schuleinsatz?

Durch den Hinweis eines Schülers eines brandenburgischen Oberstufenzentrums wurden wir auf eine Datenschutzverletzung in mehreren Schulen des Landkreises Potsdam-Mittelmark aufmerksam. Von seinem schulischen Nutzerkonto in der Microsoft Office 365-Umgebung konnte der Schüler nicht nur auf personenbezogene Daten seiner Schule zugreifen, sondern auch diejenigen anderer Schulen einsehen, manipulieren oder sogar löschen. Neben Kontaktinformationen von Lehrkräften, Schülerinnen und Schülern (wie Namen, Telefonnummern und E-Mail-Adressen) umfassten diese Daten auch E-Mail-Inhalte, persönliche Kalender, schulinterne Dokumente, Unterrichtsvorbereitungen sowie zum Teil private Korrespondenz

von Lehrkräften untereinander. So konnte der Schüler beispielsweise die Sammlung finanzieller Mittel für ein Hochzeitsgeschenk im Kollegium einer Schule mitverfolgen und in diesem Kontext auch private Kontoinformationen einsehen.

Daten aus der Cloud – frisch geklaut

Schnell stellte sich heraus, dass der Landkreis als Schulträger den betroffenen Schulen die cloudbasierte Microsoft-Umgebung als digitale Lernplattform zur Verfügung gestellt hatte und es vermutlich im Rahmen von Umstrukturierungen sowie Datenmigrationen zu einem Fehler in der Konfiguration gekommen war. Dieser ermöglichte die schulübergreifenden Zugriffe auf personenbezogene Daten. Darüber hinaus hatten mehrere Lehrkräfte Einstellungen zum Zugriffsschutz in von ihnen betreuten Benutzergruppen von „privat“ auf „öffentlich“ geändert. Das erhöhte jedoch nicht nur den Komfort, sondern gestattete auch unbefugten Personen den Zugriff auf die jeweils in der Gruppe bearbeiteten Daten und Dokumente.

Manche Schulen hatten den Vorfall gar nicht selbst bemerkt und erfuhren davon erst durch unsere Information oder durch Presseberichte. Zwar gaben alle eine entsprechende Meldung zu der Datenschutzverletzung gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) ab, allerdings blieben auch danach wesentliche Fragen zur Erfüllung der datenschutzrechtlichen Anforderungen durch die Schulen bzw. den Landkreis offen. Wir wandten uns deshalb schriftlich an die Verantwortlichen und baten sie um Aufklärung.

Nach § 65 Absatz 2 Brandenburgisches Schulgesetz dürfen Schulen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern, Lehrkräften und dem sonstigen Schulpersonal verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Erziehungs- und Bildungsauftrages der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. Sie müssen dabei die Anforderungen der Datenschutz-Grundverordnung, des Brandenburgischen Datenschutzgesetzes sowie der Datenschutzverordnung Schulwesen einhalten. Da das Brandenburgische Schulgesetz keine ausdrückliche gesetzliche Ermächtigung zur Verarbeitung personenbezogener Daten von Schülerinnen und Schülern mittels digitaler Lernplattformen enthält,

bedarf es in diesem Zusammenhang einer Einwilligung nach Artikel 7 DS-GVO. Sie muss freiwillig und in informierter Weise abgegeben werden sowie mit Wirkung für die Zukunft widerrufbar sein. Die Schule ist verpflichtet (gegebenenfalls gemeinsam mit dem Schulträger), sowohl die Grundsätze des Datenschutzes aus Artikel 5 Absatz 1 DS-GVO wie Rechtmäßigkeit, Transparenz, Zweckbindung und Datenminimierung einzuhalten, als auch die Verfahrensvorschriften sowie technische und organisatorische Anforderungen z. B. aus Artikel 24, 25, 30, 32 DS-GVO umzusetzen und dafür den Nachweis zu erbringen. Falls ein externer Dienstleister einbezogen wird, sind die Anforderungen zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO zu beachten. Und letztlich verlangt die umfangreiche Verarbeitung personenbezogener Daten von Kindern mittels digitaler Lernplattformen auch die Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO. Mit dieser ist nachzuweisen, dass durch geeignete und angemessene Maßnahmen dem gesetzlich normierten, besonderen Schutzbedürfnis Minderjähriger Rechnung getragen und die durch die Verarbeitung für sie entstehenden Risiken hinreichend reduziert werden.

Im vorliegenden Fall mussten wir feststellen, dass wesentliche Defizite hinsichtlich der Aufteilung der datenschutzrechtlichen Verantwortlichkeiten zwischen Schulträger und Schulen bestanden. Eine klare Regelung gab es hierzu nicht. Keine der beteiligten Stellen konnte darüber hinaus einen Vertrag zur Auftragsverarbeitung vorweisen. Selbst wenn man annimmt, dass die allgemeinen Vertragsbedingungen für Online-Dienste von Microsoft und deren Anhang zum Datenschutz Anwendung finden sollten, bleibt festzuhalten, dass diese Unterlagen nach unserer Auffassung die Mindestanforderungen von Artikel 28 Absatz 3 DS-GVO nicht in vollem Umfang erfüllen.[11] Auch für die Erledigung von Wartungsaufgaben durch einen weiteren Dienstleister gab es keinen Auftragsverarbeitungsvertrag.

Weiterhin haben wir Zweifel, dass in den vorliegenden Fällen die Einwilligungen der Schülerinnen und Schüler bzw. der Sorgeberechtigten in die Verarbeitung personenbezogener Daten in der Cloud-Umgebung rechtskonform waren. Unsere Bedenken beziehen sich zum einen auf die Freiwilligkeit der Einwilligung, da Einführung und

11 siehe A V 1.5

Nutzung der Microsoft-Produkte in der Regel auf einem Beschluss der Schulkonferenz beruhen und natürlich auch ein gewisser „Gruppenzwang“ besteht, diese Werkzeuge gerade in der Phase des pandemiebedingten Distanzlernens zu verwenden. Nicht in jedem Fall war zudem gewährleistet, dass alternative Angebote verfügbar waren, falls keine Einwilligung erteilt wurde. Zum anderen sind wir skeptisch, dass die Einwilligungen in informierter Weise erteilt wurden und eine hinreichende Transparenz der Verarbeitung personenbezogener Daten bestand. Unklar ist beispielsweise, welche Telemetrie- und Diagnosedaten (etwa durch die Beobachtung des Nutzungsverhaltens und das Protokollieren von Tätigkeiten, insbesondere in Verbindung mit Identitätsdaten, Gerätekennungen, Zeitstempeln und Ortsangaben) an den Hersteller Microsoft für eigene Geschäftszwecke übermittelt werden, wie lange das Unternehmen diese Daten verarbeitet und welche Risiken dadurch für die Rechte und Freiheiten der betroffenen Schülerinnen, Schüler und Lehrkräfte entstehen.

Hinzuweisen ist auch darauf, dass nach dem Schrems II-Urteil des Europäischen Gerichtshofes[12] Datenübermittlungen in die USA, dem Hauptsitz des Microsoft-Konzerns, besonderer Sorgfalt hinsichtlich der rechtlichen Begründung ihrer Zulässigkeit sowie ergänzender vertraglicher, organisatorischer oder technischer Sicherheitsmaßnahmen bedürfen, da das Datenschutzniveau im Zielland des Datentransfers nicht dem europäischen Niveau entspricht.

Darüber hinaus stellten wir fest, dass für das in Rede stehende Verfahren keine Datenschutz-Folgenabschätzung durchgeführt und somit auch kein Nachweis erbracht wurde, dass die Risiken der Datenverarbeitung durch geeignete und angemessene Maßnahmen hinreichend reduziert wurden.

Im Ergebnis forderten wir die betroffenen Schulen auf, die Nutzung der cloudbasierten Microsoft-Umgebung solange auszusetzen, bis ein vollständig rechtskonformer Zustand erreicht und nachgewiesen ist. Eine Schule hat daraufhin gegen Ende des Berichtszeitraums überarbeitete Unterlagen eingereicht, deren Bewertung durch uns

12 siehe A V 2

aktuell vorgenommen wird. Die Ergebnisse werden wir anschließend mit der Schulleitung erörtern.

6 Datenschutzverletzungen durch Sicherheitslücken im Webauftritt

Content-Management-Systeme (CMS) werden von Verantwortlichen häufig eingesetzt, um Inhalte ihrer Webauftritte (wie beispielsweise Texte, Bilder, multimediale Inhalte, Kontakt- und Anmeldeformulare) zu erstellen, zu pflegen und zu verwalten. Bei bekannten Content-Management-Systemen wie WordPress, Drupal oder TYPO3 werden immer wieder Sicherheitslücken entdeckt. Die Betreiberinnen und Betreiber der jeweiligen Websites können schnell Opfer von Angriffen werden, wenn sie diese Lücken nicht rechtzeitig schließen. Bereits in unserem letzten Tätigkeitsbericht[13] informierten wir über einen Fall, in dem ein Verantwortlicher die notwendigen Updates für sein CMS über einen längeren Zeitraum nicht einpflegte und so eine Verletzung des Schutzes personenbezogener Daten verursachte.

Im Februar 2020 meldeten uns der brandenburgische Landesverband sowie mehrere Kreisverbände einer überregional tätigen Hilfs- und Wohlfahrtsorganisation eine Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO). Ursache war auch hier eine nicht geschlossene Sicherheitslücke im verwendeten Content Management System. Dieses war durch einen externen Dienstleister eigens für die Organisation entwickelt worden. Mittels eines als „SQL Injection“ bezeichneten Angriffs gelang es Unbefugten, direkt auf die hinter dem Webauftritt liegende Datenbank mit einer Vielzahl personenbezogener Daten zuzugreifen. Im Falle eines Kreisverbands war eine sechsstellige Anzahl von Datensätzen betroffen, im Falle anderer Kreisverbände und des Landesverbands eine fünfstellige Anzahl. Die Datensätze enthielten neben dem Namen und der Wohnadresse von Personen zum Teil auch Daten über ihren Gesundheitszustand.

Aufgrund der Meldungen hörte die Landesbeauftragte die jeweiligen Verantwortlichen an und bat um nähere Auskünfte und eine Stellungnahme. Im Falle eines Kreisverbands konnte ermittelt werden,

13 Tätigkeitsbericht Datenschutz 2019, A III 5.

dass ihm die Sicherheitslücke bereits seit November 2019 bekannt war. Schon zu diesem Zeitpunkt konnte ein Hacker auf die Datenbank zugreifen, nutzte dies jedoch nicht für eigene Zwecke aus, sondern informierte den Betreiber. Dieser dokumentierte den Vorfall zwar, meldete ihn jedoch nicht an uns als zuständige Datenschutzaufsichtsbehörde, da er das Risiko für die Rechte und Freiheiten der betroffenen Personen durch unbefugte Zugriffe als gering einschätzte. Bei der Bereinigung der Sicherheitslücke vergaß der Kreisverband, dass eine zweite Website mit identischen Inhalten existierte und versäumte die Korrektur des Fehlers dort. Die auf der zweiten Website weiter bestehende Lücke wurde im Februar 2020 prompt erneut ausgenutzt – nun erhielten auch wir eine entsprechende Information des Verantwortlichen.

Die Aufklärung des gesamten Sachverhalts gestaltet sich – auch wegen der Einschränkungen der Corona-Pandemie – schwierig und dauert an. Zu klären ist etwa noch, warum wir entgegen der Pressemitteilung des Landesverbandes nicht in allen genannten Fällen eine Meldung einer Datenschutzverletzung erhalten haben. Darüber hinaus fiel im Rahmen der Recherche auf, dass weitere Kreisverbände das in Rede stehende CMS nutzten, jedoch auch diese keine Meldung nach Artikel 33 DS-GVO abgaben. Hintergrund für die Schwierigkeiten der Aufklärung sind zudem Unklarheiten bezüglich der Organisationsstrukturen der Verbände, der Verantwortlichkeiten und der Beauftragung von Unternehmen. Wir werden in jedem Fall prüfen, ob die Einleitung eines Ordnungswidrigkeitenverfahrens gegen die Verantwortlichen wegen Verstoßes gegen Artikel 32 und 33 DS-GVO angezeigt ist. Die verwundbaren Websites wurden im Übrigen mittlerweile auf eine neue technische Basis gestellt.

7 Kundendatenbank ungesichert im Internet

Während des Berichtsjahres wurden wir anonym über eine Datenschutzverletzung bei einem Tourismusunternehmen informiert. Konkret ging es darum, dass eine MongoDB-Datenbank dieses Unternehmens mit personenbezogenen Daten von Kundinnen und Kunden sowie von Gastgeberinnen und Gastgebern ungesichert im Internet erreichbar war.

MongoDB ist ein dokumentenorientiertes Datenbankmanagementsystem. Im Gegensatz zu herkömmlichen relationalen Datenbankmanagementsystemen erfolgt die Speicherung von Einträgen nicht in miteinander verknüpften Tabellen, sondern in hierarchisch strukturierbaren Kollektionen von Dokumenten. Dokumente können unterschiedliche Einträge enthalten wie Name-Wert-Paare, Texte, Listen von Einträgen oder Verweise auf andere Dokumente. Im fraglichen Fall enthielt die Datenbank über 3.000 Einträge vermutlich zu Kundinnen und Kunden – unter anderem mit deren Namen, Reisen und Interessen. Außerdem waren über 600 Einträge vermutlich zu Gastgeberinnen und Gastgebern gespeichert – unter anderem mit Kontoinformationen und verschlüsselten Passwörtern.

Nachdem wir uns selbst im Rahmen einer ersten Untersuchung und Beweissicherung davon überzeugt hatten, dass die Datenschutzverletzung andauerte, wandten wir uns an das Unternehmen. Der Verantwortliche versicherte uns, dass er in der Zwischenzeit die Erreichbarkeit der Datenbank aus dem Internet unterbunden und die interne IT-Abteilung mit einer umfangreichen Nachforschung beauftragt hatte. Gleichwohl hatten wir eine Reihe von Nachfragen. Insbesondere wollten wir in Erfahrung bringen, welche technischen und organisatorischen Maßnahmen gemäß Artikel 32 Datenschutz-Grundverordnung (DS-GVO) im konkreten Fall umgesetzt wurden, warum diese die Datenschutzverletzung nicht verhinderten sowie welche Konsequenzen seitens des Verantwortlichen daraus gezogen wurden. Weiter interessierten uns die Umstände, unter denen das Unternehmen von der ungesicherten Datenbank erfuhr, warum es keine Meldung nach Artikel 33 DS-GVO abgegeben hatte, wie das Risiko für die Rechte und Freiheiten der betroffenen Personen im Zuge des Vorfalls eingeschätzt wurde und ob deren Information nach Artikel 34 DS-GVO geplant war.

Sich um Daten kümmern, bevor es andere tun.

Die Stellungnahme des Unternehmens beantwortete unsere Fragen nur zum Teil. Im Rahmen unserer Prüfung ergaben sich auch neue Fragen, z. B. zum Passwort- und Zugriffsmanagement in der Anwendung, zu Einzelheiten des Datenabflusses und zur Benachrichtigung der betroffenen Personen. Eine weitere Besonderheit resultierte daraus, dass der Verantwortliche plante, die bisherige Datenbank zu

migrieren und dabei ein ausschließlich cloudbasiertes Angebot eines amerikanischen Anbieters zu verwenden. Vor allem hinsichtlich des Speicherortes der Daten in dieser Cloud-Lösung und der Gestaltung der Auftragsverarbeitung verlangten wir vor dem Hintergrund des Schrems II-Urteils des Europäischen Gerichtshofes[14] detailliertere Informationen.

Der Vorgang ist noch nicht abgeschlossen. Aufgrund der bisherigen Sachlage prüfen wir wegen der festgestellten Verstöße gegen die Datenschutz-Grundverordnung die Einleitung eines Ordnungswidrigkeitenverfahrens durch die Bußgeldstelle unserer Behörde.

8 Citrix-Sicherheitslücke bei öffentlichen Stellen

Über Citrix-Terminalserver können Behörden oder Unternehmen sichere Fernzugriffe auf Serverdienste (z. B. E-Mail- oder Dateidienste) oder auf andere interne Softwaresysteme ermöglichen. Die Anwendungssoftware muss nicht mehr lokal auf dem PC der Nutzerin bzw. des Nutzers installiert sein – ein lokaler Citrix-Client holt sich lediglich deren Bilddaten vom Server und gibt Tastatur- oder Mauseingaben dorthin zurück. Da Citrix-Serversysteme oft über das Internet erreichbar sind, ist es besonders wichtig, diese stets auf dem aktuellen Stand zu halten und auf mögliche Sicherheitsprobleme sofort zu reagieren.

Mitte Dezember 2019 wurde eine kritische Lücke in einer Citrix-Komponente, dem Application Delivery Controller (ADC), bekannt. Er bildet das Zugangstor, um von außen per Fernzugriff auf interne Anwendungen zugreifen zu können. Über die Lücke war es möglich, auch ohne entsprechende Berechtigungen Schadcode nachzuladen und beliebige Programme auszuführen. Viele Unternehmen und öffentliche Stellen waren hiervon betroffen. Zum Zeitpunkt des Bekanntwerdens der Lücke gab es noch keinen Patch, um sie zu schließen. Allerdings veröffentlichte der Hersteller Empfehlungen für technische Sofortmaßnahmen, die das Angriffsrisiko senken sollten. In einschlägigen Publikationen wurde vor der Sicherheitslücke gewarnt und geraten, die Maßnahmen umzusetzen.

14 siehe A V 2

Die genannte Sicherheitslücke trat auch in mehreren brandenburgischen Kommunen auf. Besonders gravierend waren die Auswirkungen in der Landeshauptstadt Potsdam. Die Stadtverwaltung wurde am 15. Januar 2020 durch einen Dienstleister in Kenntnis gesetzt, dass ihre Citrix-Installation angreifbar ist. Daraufhin beauftragte sie unverzüglich ein externes Unternehmen mit einer Analyse der Systeme. Aufgrund der hohen Auftragsdichte konnte das Unternehmen jedoch erst mehrere Tage später mit den Arbeiten beginnen. Im Rahmen der Analyse wurde schon früh festgestellt, dass tatsächlich ein unbefugter Zugriff auf den Citrix ADC der Landeshauptstadt stattgefunden hatte.

Sicherheitshalber wurden die betroffenen Systeme deshalb am 22. Januar 2020 heruntergefahren, vom Netz und zusätzlich von der Stromversorgung getrennt. Hierdurch wurde der lokale Cache im Arbeitsspeicher gelöscht, weshalb dieser nicht für weitere Analysen zur Verfügung stand. Auch die Verbindung der Stadtverwaltung zum Landesverwaltungsnetz wurde vorsorglich getrennt.

Am gleichen Tag berief die Stadtverwaltung einen Krisenstab ein, der das weitere Vorgehen koordinieren sollte. Dieser hat in der Folgezeit ca. 30-mal getagt. Weiterhin ersuchte die Stadt das Hasso-Plattner-Institut (HPI) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) um Unterstützung. Auf Grund der hohen Auslastung des BSI kam allerdings nur das HPI der Bitte nach. Unsere Behörde wurde weiterhin im Rahmen einer vorsorglichen Meldung einer Datenschutzverletzung nach Artikel 33 Datenschutz-Grundverordnung informiert und beim Landeskriminalamt Anzeige gegen Unbekannt erstattet.

Die stadtinterne technische Analyse beschränkte sich nicht nur auf den Citrix ADC; einbezogen waren auch die Proxy- und Firewall Systeme. Dabei wurde festgestellt, dass es sich bei dem Angriff nicht um eine gezielte Attacke gegen die Stadtverwaltung Potsdam gehandelt hatte. Vielmehr war das Vorgehen der Angreifer automatisiert, um zunächst von der Sicherheitslücke betroffene Systeme zu identifizieren. Der Versuch, unberechtigte Zugriffe auf das Dateisystem durchzuführen und Schadcode nachzuladen, konnte jedoch durch die Firewall-Systeme der Stadtverwaltung verhindert werden. An-

haltspunkte für größere Schäden oder auch eventuelle Datenschutzverletzungen gab es nicht.

Dennoch förderten die Untersuchungen Mängel in der Organisation der Informationssicherheit der Stadtverwaltung Potsdam zutage. So wurde beispielsweise festgestellt, dass die Tageslageberichte des Computer Emergency Response Teams Brandenburg (CERT-BB) nicht zeitnah ausgewertet wurden. Das CERT-BB ist beim Brandenburgischen IT-Dienstleister eingerichtet und gibt u. a. aktuelle Informationen zu Sicherheitslücken und möglichen Gegenmaßnahmen heraus. Das geschah auch zu der hier in Rede stehenden Citrix-Lücke. Die Beachtung dieser Informationen und das rechtzeitige Einleiten von Maßnahmen (wie z. B. die Umsetzung der technischen Sofortmaßnahmen des Herstellers) hätte die Attacke im vorliegenden Fall verhindern können. Weiterhin fiel auf, dass die Dokumentation der Systemlandschaft und der umgesetzten Maßnahmen zur Gewährleistung der Informationssicherheit Lücken aufwiesen. Dies erschwerte und verzögerte die Analyse des Vorfalls. Beide Aufgaben oblagen dem behördlichen Informationssicherheitsbeauftragten. Die Stadtverwaltung hat die Mängel erkannt und begonnen, die erforderlichen Änderungen umzusetzen. Dabei wird auch eine bessere organisatorische Anbindung der bzw. des neuen Informationssicherheitsbeauftragten (gegebenenfalls als Stabsstelle direkt beim Oberbürgermeister) angestrebt.

Systeme patchen - Sicherheit gewinnen

Die bei der Aufarbeitung des Vorfalls festgestellten Mängel wirken noch immer nach. Die Stadtverwaltung kann insbesondere die Lücken in der Dokumentation nur schrittweise beseitigen und somit die verbundenen Systemdienste und Softwareanwendungen erst nach und nach wieder bereitstellen. Auch der ADC wurde zwar komplett neu aufgesetzt, befand sich jedoch zum Ende des Berichtszeitraums noch nicht wieder im Betrieb.

Die Landesbeauftragte sah in dem konkreten Fall davon ab, gegenüber der Stadtverwaltung Potsdam eine Sanktion nach Artikel 58 Absatz 2 Datenschutz-Grundverordnung zu verhängen. Hintergrund ist, dass es tatsächlich nicht zu einer Verletzung des Datenschutzes kam, die Verwaltung schnell reagierte und die erforderlichen Maßnahmen

ergriff bzw. für die Zukunft plant. Eine Kontrolle zu einem späteren Zeitpunkt behalten wir uns vor. Außerdem wurde die dringende Empfehlung ausgesprochen, die Aufgaben der bzw. des Informationssicherheitsbeauftragten auf ein Informationssicherheitsmanagementteam zu verteilen, eine stärkere Koordinierung der Arbeiten auf diesem Gebiet zwischen den verschiedenen Organisationseinheiten der Verwaltung durchzusetzen und eine regelmäßige Berichterstattung der bzw. des Beauftragten oder des Teams zum aktuellen Stand der Informationssicherheit bei der Leitung zu etablieren.

9 Datenschutzverletzungen bei der Nutzung von E-Mails

9.1 Verteilung von Schadsoftware

Immer wieder erreichten uns auch in diesem Berichtsjahr Meldungen zu Datenschutzverletzungen gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO). Häufig informierten uns Behörden und Unternehmen über die Infektion von Rechnern mit Schadsoftware durch die E-Mail-Nutzung. Die Schadsoftware variiert in Funktion und Schadensausmaß: Manchmal wird nur Aufregung verursacht, z. B. indem einzelne Buchstaben oder Textteile verschwinden oder Bildschirmfenster geöffnet bzw. geschlossen werden. Manchmal werden E-Mail-Adressen gezielt an Angreifende übermittelt, die diese wiederum an Dritte verkaufen. Manchmal verschickt die Schadsoftware auch selbst E-Mails im Namen des angegriffenen Unternehmens unter Bezugnahme auf eine vorherige echte E-Mail. Bei einer weiteren häufig anzutreffenden Form verschlüsselt die Schadsoftware gespeicherte Daten bei der angegriffenen Institution und versucht, ein „Lösegeld“ für die Entschlüsselung zu erpressen. Und sehr weitreichende Formen von Schadsoftware versuchen, unbemerkt eine Hintertür auf den Rechnern der Institution zu etablieren, durch die auch später noch Schadfunktionen ausgeführt werden können.

Exemplarisch sowohl für die Ursachen als für auch das Schadenspotenzial einer Infektion mit Schadsoftware sind die folgenden drei Fälle aus dem Berichtsjahr.

Im ersten Fall hatte ein Beschäftigter eines mittelständischen Unternehmens den Dateianhang einer E-Mail geöffnet. Die E-Mail wirkte authentisch, Ungereimtheiten gab es nicht. Es kam zur Infektion mit einer Schadsoftware. Diese ist darauf spezialisiert, E-Mail-Adressen auszulesen und sich selbst als Anhang an diese Adressen zu versenden – bestenfalls wieder in echt wirkenden E-Mails (sogenanntes Outlook Harvesting). Die jeweiligen Empfänger sollen ihrerseits die Anhänge öffnen und so nach einer Infektion zu weiteren Absendern werden. Dies führt zu einer exponentiellen Verbreitung der Schadsoftware. Die IT-Abteilung des fraglichen Unternehmens konnte sie in diesem Fall zwar in der eigenen Infrastruktur wieder entfernen. Unklar blieb jedoch, ob auch alle Empfänger die Infektion verhindern konnten oder bereits selbst an der Weiterverbreitung der Schadsoftware mitwirkten. Ursache der Infektion waren in diesem Fall nicht hinreichende technische Maßnahmen zur Prüfung von Mailanhängen auf Schadcode.

Vor dem Schaden klug sein!

In einem zweiten Fall kam es zur Infektion mehrerer Server in einem Unternehmen mit einer sogenannten Ransomware. Diese verschlüsselte die Datenbestände und erpresste das Unternehmen anschließend über ein automatisiertes Verfahren. Es sollte Geld an eine anonyme Adresse – ein Bitcoin-Wallet– überweisen, bevor ihm der Schlüssel zum Entschlüsseln der Daten übermittelt wird. Das Unternehmen zahlte nicht. Es verfügte über eine aktuelle Datensicherung und konnte den Datenbestand zum größten Teil wieder herstellen. Die Infektionsursache blieb jedoch ungeklärt. Da anscheinend die getroffenen Schutzmaßnahmen nicht ausreichend waren, versicherte das Unternehmen, eine Überarbeitung des IT-Sicherheitskonzeptes vornehmen zu wollen.

Auf zwei Dinge möchten wir in diesem Zusammenhang hinweisen: Zum einen besteht keine Garantie dafür, den Schlüssel für das Entschlüsseln der Daten zu erhalten, auch wenn auf die Forderung zur Zahlung eines Geldbetrages eingegangen wird. Und zum anderen drohen manche mit Ransomware Angreifende, die Daten, die sie vor der Verschlüsselung aus dem betroffenen Unternehmen oder der Behörde ausgeleitet haben, zu veröffentlichen. Dies verdeutlicht, wie wichtig es ist, nicht nur eine aktuelle Datensicherung zu haben,

sondern auch alle anderen technischen und organisatorischen Maßnahmen umzusetzen, die eine Infektion mit Ransomware sowie unbefugte Datenzugriffe und Datenübermittlungen verhindern.

Im dritten Fall leitete ein Beschäftigter eines Unternehmens eine private E-Mail mit Anhang an seine Firmen-E-Mail-Adresse weiter. Die Schutzmaßnahmen des Unternehmens waren nicht in der Lage, den schädlichen Anhang der besagten E-Mail zu identifizieren und zu bereinigen. Deshalb kam es auch hier dazu, dass E-Mail-Kontakte ausgelesen und unautorisiert von der Schadsoftware benutzt wurden, um sich selbst zu versenden und weiterzuverbreiten. Allerdings konnte der Vorfall auf das in Rede stehende Unternehmen begrenzt werden, da er schnell erkannt und die Schadsoftware ausschließlich die geschäftlichen E-Mail-Adressen der anderen Beschäftigten auslesen konnte. Personenbezogene Daten von Dritten waren nicht betroffen. Als Reaktion etablierte das Unternehmen eine weitere Schutzebene auf den lokalen Computern der Beschäftigten und erließ ein Verbot der privaten Nutzung der IT-Infrastruktur.

In allen drei Fällen sind nicht ausreichende technische und organisatorische Schutzmaßnahmen Ursache der Infektionen mit Schadsoftware und damit der Verletzungen des Datenschutzes. Artikel 32 DS-GVO schreibt vor, dass Verantwortliche solche Maßnahmen treffen müssen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Die Maßnahmen müssen dem Stand der Technik entsprechen, für die Schutzzwecke geeignet und den Risiken angemessen sein. Ein nicht vorhandener, nicht ausreichender oder nicht aktueller Schutz vor Schadsoftware erfüllt diese Anforderungen nicht. Und letztlich ist auch an die Sensibilisierung der Beschäftigten zu denken, kritisch mit E-Mail-Anhängen oder in E-Mails versandten Internetlinks umzugehen sowie Geschäftliches und Privates nicht zu vermischen.

9.2 Unüberlegte Nutzung der CC-Funktion

Eine weitere Art der Datenschutzverletzung, die uns im Berichtszeitraum sehr oft gemeldet wurde, ist der Versand von E-Mails in Kopie an viele Personen, wobei die E-Mail-Adressen der Empfängerinnen und Empfänger in das CC-Feld (Carbon Copy) anstatt in das BCC-

Feld (Blind Carbon Copy, auch BC – Blind Copy) eingetragen wurden. Entscheidender Unterschied der beiden Varianten ist, dass die im BCC-Feld eingetragenen Adressen gegenüber den anderen Empfängerinnen und Empfängern nicht offenbart werden, diejenigen im CC-Feld jedoch schon. Somit kann es bei Nutzung des CC-Feldes schnell zu einer ungewollten Offenbarung von mehreren hundert E-Mail-Adressen an Dritte kommen. Da E-Mail-Adressen oftmals Vor- und Nachnamen natürlicher Personen enthalten, werden damit auch personenbezogene Daten unbefugt übermittelt. Dies stellt eine Verletzung der Vertraulichkeit dar.

Verantwortlichen raten wir regelmäßig, Maßnahmen zu ergreifen, die derartige Pannen bereits im Vorfeld vermeiden. An erster Stelle ist die Sensibilisierung der Beschäftigten zu nennen, die auf eine korrekte Verwendung von CC- und BCC-Feld achten müssen. Eine technische Maßnahme kann die Einholung einer expliziten Bestätigung vor dem beabsichtigten Versenden von E-Mails mit Adresseinträgen im CC-Feld sein. Denkbar wäre etwa, durch Ankreuzen einer Checkbox oder Einblenden einer Warnmeldung in einem neuen Fenster zu bestätigen, dass eine Nutzung des CC-Feldes tatsächlich beabsichtigt ist. Dadurch könnten Fälle, die zum Beispiel aus Unachtsamkeit oder Eile entstehen, vermutlich oftmals verhindert werden. Die Lösung müsste allerdings für das jeweilige E-Mail-Programm bereitstehen oder entwickelt werden.

Eine andere Methode, welche wir des Öfteren empfehlen, ist die Einrichtung eines Vier-Augen-Prinzips in Abhängigkeit von der Größe des Empfängerkreises. Der Verantwortliche könnte beispielsweise bei einem Empfängerkreis ab 50 Personen festlegen, dass neben der Absenderin bzw. dem Absender der E-Mail eine weitere Person – z. B. eine Kollegin oder ein Kollege – den korrekten Versand überprüfen und bestätigen muss. Dies sollte in einer organisatorischen Regelung (wie einer Dienst- oder Geschäftsanweisung) festgehalten werden. Alternativ könnte die bzw. der Datenschutzbeauftragte auch eine Checkliste für den Versand von E-Mails mit einem großen Empfängerkreis erarbeiten, bei der die Prüfung der korrekten Verwendung des Adressfeldes ein Punkt ist, der aktiv geprüft und bestätigt werden muss.

Die große Gefahr bei dieser Art von Datenschutzverletzungen ist nicht, dass hier besonders sensible personenbezogene Daten betroffen wären, sondern die unter Umständen sehr hohe Zahl von betroffenen Personen durch nur ein einziges falsch befülltes Adressfeld. Wir können daher allen Verantwortlichen nur dringend empfehlen, sich Gedanken über den Umgang mit dem CC- und BCC-Feld beim E-Mail-Versand zu machen und geeignete, vorbeugende Maßnahmen zu treffen.

9.3 Unsicherer E-Mail-Versand von Sozialdaten durch Jugendämter

Der externe Datenschutzbeauftragte eines freien Trägers der Jugendhilfe informierte uns darüber, dass Jugendämter im Land Brandenburg häufig nicht die erforderlichen technischen Maßnahmen für eine sichere E-Mail-Kommunikation umsetzen. So sei es oft gängige Praxis, dass Entwicklungspläne, Hilfepläne, Gutachten und andere Dokumente mit sensitiven personenbezogenen Daten unverschlüsselt zwischen den Jugendämtern und den leistungserbringenden freien Trägern versandt werden. Weiter verfüge nur ein Teil der Jugendämter über die Möglichkeit, Ende-zu-Ende-verschlüsselte E-Mails zu empfangen. Er bat uns darauf hinzuwirken, dass die sozial- und datenschutzrechtlichen Anforderungen bei der elektronischen Kommunikation durch die Jugendämter eingehalten werden.

Darüber hinaus erreichten uns im Berichtszeitraum Meldungen von Datenschutzverletzungen gemäß Artikel 33 Datenschutz-Grundverordnung (DS-GVO) zu fehlgeleiteten, unverschlüsselten E-Mails von Jugendämtern. Diese machten deutlich, dass neben der Sorgfalt bei der Angabe der Adressatin oder des Adressaten und der Umsetzung geeigneter technischer Verschlüsselungsmaßnahmen auch das Gebot der Datensparsamkeit bei der E-Mail-Kommunikation nicht in jedem Fall beachtet wurde. So können vermeintlich harmlos wirkende E-Mails mit Informationen über den Wechsel einer Fachkraft oder der Terminanfrage für das nächste Hilfeplangespräch die Identifizierung der konkreten Person ermöglichen. Eine unbefugte Kenntnisnahme der E-Mail-Inhalte kann insofern zu erheblichen Risiken für die Rechte und Freiheiten der Betroffenen führen.

Bei den genannten personenbezogenen Daten handelt es sich um Sozialdaten. Diese unterliegen dem Sozialgeheimnis gemäß § 35 Absatz 1 Satz 1 Erstes Buch Sozialgesetzbuch. Danach hat jeder einen Anspruch darauf, dass die ihn betreffenden Sozialdaten von Leistungsträgern nicht unbefugt verarbeitet werden. Hierzu gehört auch, dass Dritten die Daten nicht unbefugt offenbart werden dürfen. Werden sie per E-Mail übertragen, sind durch den Verantwortlichen (und gegebenenfalls den Auftragsverarbeiter) gemäß Artikel 32 Absatz 1 DS-GVO geeignete technische und organisatorische Maßnahmen umzusetzen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Buchstabe a dieser Norm nennt ausdrücklich die Verschlüsselung als geeignete Maßnahme.

Im Regelfall ist bei der Übermittlung personenbezogener Daten per E-Mail mindestens eine Transportverschlüsselung einzusetzen. Für besonders schutzbedürftige Sozialdaten ist nach unserer Auffassung eine Ende-zu-Ende-Verschlüsselung zu nutzen. Da diese jedoch die Betreffzeile einer E-Mail nicht schützt, muss die Absenderin oder der Absender auch darauf achten, dort keine Sozialdaten zu verwenden. Ist eine Ende-zu-Ende-Verschlüsselung des kompletten Inhalts einer E-Mail nicht möglich, sind zumindest die sensitiven personenbezogenen Daten nach dem Stand der Technik zu verschlüsseln, z. B. in Form eines verschlüsselten E-Mail-Anhangs. Der Schlüssel muss dann über einen anderen Kommunikationsweg, z. B. telefonisch, mitgeteilt werden.

Obacht bei Übermittlung von Sozialdaten

Die Verantwortung für die Zulässigkeit der Übermittlung von Sozialdaten – einschließlich des Schutzes vor unbefugter Kenntnisnahme – trägt gemäß § 67d Abs. 1 Satz 1 Zehntes Buch Sozialgesetzbuch (SGB X) die übermittelnde Stelle. Ein Sozialleistungsträger kann sich dieser gesetzlichen Verpflichtung nach unserer Auffassung nicht dadurch entziehen, dass er die betroffenen Personen allgemein auf die Risiken der Nutzung unsicherer Kommunikationswege hinweist und deren Einwilligung einholt, solche Wege verwenden zu dürfen. Antragstellerinnen und Antragsteller bzw. Hilfesuchende sind in vielfältiger Weise auf die Gewährung von Sozialleistungen angewiesen. Gerade im Hinblick auf dieses besondere Abhängigkeitsverhältnis sind die hohen Anforderungen des Sozialdatenschutzes konsequent

zu beachten. Eine Einwilligung gemäß § 67b Absatz 2 SGB X i. V. m. Artikel 7 DS-GVO kann zwar eine Verarbeitung von Sozialdaten an sich legitimieren, wenn sie tatsächlich freiwillig und in informierter Weise abgegeben wurde sowie widerrufbar ist. Durch sie können aber nicht die nach Artikel 32 DS-GVO notwendigen technischen und organisatorischen Maßnahmen ausgehebelt werden.

Im Berichtszeitraum wurden wir mehrfach auf Fälle hingewiesen, in denen die betroffenen Personen selbst ausdrücklich den unverschlüsselten Versand von z. B. Therapie- und Schulberichten mit sensitiven Daten verlangten und Beschäftigte des Jugendamts dieser Bitte trotz der Unzulässigkeit der Nutzung des unsicheren Kommunikationsweges nachgaben.

Aufgrund des hohen Aufklärungsbedarfes haben wir im Juni 2020 ein Rundschreiben zu der Thematik verfasst und an alle Jugendämter der Landkreise und kreisfreien Städte versandt. Einige Datenschutzbeauftragte der Behörden mussten durch uns nachträglich in Kenntnis gesetzt werden. Wir baten sie, für eine datenschutzkonforme Umsetzung in den entsprechenden Ämtern zu sorgen. Insbesondere verwiesen wir in dem genannten Rundschreiben auf die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ des Arbeitskreises Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 13. März 2020 mit ergänzenden Erläuterungen. Die Orientierungshilfe steht in unserem Internetangebot zur Verfügung.

Darüber hinaus haben wir vorgeschlagen, Schulungen zur Sensibilisierung der Beschäftigten der Jugendämter für Belange der Datensparsamkeit, des technischen Datenschutzes sowie zu datenschutzrechtlichen Einwilligungen im Sozialleistungsbereich und ihren Rechtsfolgen durchzuführen. Weiterhin sollten im Rahmen einer Dienstanweisung Regelungen zur E-Mail-Nutzung, insbesondere zur Verschlüsselung, festgehalten und jede Mitarbeiterin bzw. jeder Mitarbeiter ausdrücklich dazu schriftlich belehrt werden.

V Ausgewählte Beratungen

1 Beratungen im öffentlichen Bereich

1.1 Die Registermodernisierung und das Problem der Personenkennziffer

In ihrer Funktion als Vorsitzende des Arbeitskreises Verwaltung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) war die Landesbeauftragte in den Jahren 2019 und 2020 an dem Projekt zur Registermodernisierung beteiligt. Dieses wird von der Bundesregierung als wesentlich für die Umsetzung des Onlinezugangsgesetzes angesehen. Gemeinsam mit Kolleginnen und Kollegen anderer Länder und des Bundes wirkten wir in verschiedenen Arbeitsgruppen mit.

Das Bundesministerium des Innern, für Bau und Heimat und der IT-Planungsrat hatten als Zielvorgabe gesetzt, die deutsche Registerlandschaft innerhalb kurzer Zeit so zu ertüchtigen, dass sie es ermöglicht, etwa 560 Leistungen des Staates in guter Qualität rein online abzuwickeln. Ein Problem hierbei war, dass die Datenqualität in den die Leistungen unterstützenden Registern der öffentlichen Verwaltung als nicht gut genug eingeschätzt wurde. So ist in vielen Fällen eine Zuordnung von Datensätzen eines oder mehrerer Register zu einer Person nur mit Mühe möglich, weil etwa die Schreibweise zwischen den Registern oder mit den vorliegenden Informationen nicht übereinstimmt.

Darüber, wie die Datensätze zu derselben Person in allen betroffenen Registern verbunden werden sollten, bestand Uneinigkeit zwischen dem Bundesministerium und einigen anderen Behörden, zu denen auch wir gehörten. Das Ministerium legte sich früh auf eine zentrale Personenkennziffer, im inzwischen vorliegenden Gesetzentwurf Identifikationsnummer genannt, fest. Diese sollte als Ordnungsmerkmal dem jeweiligen Datensatz in allen Registern hinzugefügt werden und für eine übergreifende Verknüpfbarkeit sorgen. Hierfür war die beim Bundeszentralamt für Steuern geführte Steuer-Identifikationsnummer der betroffenen Person vorgesehen. Gegen beide Komponenten dieses Plans äußerte die Landesbeauftragte durchgreifende Bedenken:

Die Einführung der Personenkennziffer ermöglicht es technisch grundsätzlich, sämtliche über eine Person vorhandenen Daten ohne größeren Aufwand zusammenzuführen und damit ein tiefgehendes Persönlichkeitsprofil zu erstellen. Das Bundesverfassungsgericht hatte in seinem für den Datenschutz grundlegenden Volkszählungsurteil[15] die Einführung eines – hier vorliegenden – einheitlichen Personenkennzeichens bereits als „entscheidende[n] Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und katalogisieren" bezeichnet. Bereits die Möglichkeit einer solchen Zusammenführbarkeit dürfte verfassungsrechtlich bedenklich sein.

Die Nutzung der Steuer-Identifikationsnummer als einheitliches Ordnungsmerkmal ist nach Überzeugung der Datenschutzkonferenz mit dem Recht auf informationelle Selbstbestimmung nicht zu vereinbaren. In seinem Urteil vom 18. Januar 2012 hat der Bundesfinanzhof[16] die Feststellung der Verfassungsmäßigkeit der Steuer-Identifikationsnummer ausdrücklich auf deren zweckgebundene Nutzung allein zur Abwicklung steuerlicher Sachverhalte gestützt. Die Aufhebung dieser Zweckbindung lässt somit nicht nur ihre Nutzung als Personenkennziffer, sondern auch diejenige zu steuerlichen Zwecken als verfassungswidrig erscheinen.

Personenkennziffer nicht verfassungskonform

Die Aufsichtsbehörden des Bundes und der Länder hatten sich dagegen für eine dezentrale Lösung nach dem Vorbild des österreichischen Systems eingesetzt, welches durch Trennung von Kennziffern u. a. nach Einsatzzweck die unzulässige Zusammenführung personenbezogener Daten effektiv verhindert. Wir sind mit diesem Vorschlag jedoch ebenso wenig durchgedrungen wie mit dem Hinweis, dass über ein rechtliches Verbot einer nicht erforderlichen Zusammenführung hinaus weitere strukturelle Hemmnisse die Zusammenführung von Daten zumindest tatsächlich erschweren müssten.

Ungeachtet der verfassungsrechtlichen Zweifel erstellte das Bundesministerium des Innern, für Bau und Heimat einen Entwurf für ein Registermodernisierungsgesetz. Darin finden sich die datenschutzrechtlich fragwürdigen Aspekte des ursprünglichen Plans faktisch

15 Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983, 1 BvR 209/83.

16 Urteil des Bundesfinanzhofes vom 18. Januar 2012, II R 49/10.

unverändert wieder. Die Datenschutzkonferenz verabschiedete am 26. August 2020 eine Entschließung unter dem Titel „Registermodernisierung verfassungskonform umsetzen!“, die wir auf unserer Webseite veröffentlichen. Weiterhin haben wir die Landesregierung Brandenburg auf unsere Rechtsauffassung aufmerksam gemacht. Es steht zu hoffen, dass im verbleibenden Verfahren noch Verbesserungen erfolgen, weil die Nutzung einer einheitlichen Personenkennziffer als Ordnungsmerkmal einer Vielzahl von Registern der öffentlichen Verwaltung mit dem Grundrecht auf Datenschutz, wie es das Bundesverfassungsgericht ausgestaltet hat, nicht vereinbar ist.

1.2 Aufenthaltserlaubnis zur Erwerbstätigkeit per Internet

Die Umsetzung des Onlinezugangsgesetzes und die damit verbundene Verpflichtung für Bund und Länder, ihre Verwaltungsleistungen bis Ende 2022 elektronisch über Verwaltungsportale anzubieten, stellt auch Brandenburg vor große Herausforderungen. Gemäß den Beschlüssen des IT-Planungsrates sollen die Dienstangebote gebündelt in insgesamt 14 Themenfeldern arbeitsteilig von einzelnen Ländern und dem Bund entwickelt und anschließend bundesweit nachgenutzt werden („Einer für alle“-Prinzip). Das Land Brandenburg hat gemeinsam mit dem Auswärtigen Amt die Federführung im Themenfeld „Ein- und Auswanderung“ übernommen und koordiniert somit die dortigen Aktivitäten.

Im Berichtszeitraum wurde in einer ersten Projektphase unter Leitung des Ministeriums des Innern und für Kommunales des Landes Brandenburg eine Pilotanwendung für die elektronische Beantragung eines „Aufenthaltstitels zur Erwerbstätigkeit“ entwickelt. Ziel dieses Fachdienstes soll es sein, Personen aus Nicht-EU-Staaten die Beantragung eines entsprechenden Titels über einen internetbasierten Zugang zur Verwaltung anzubieten und auf diese Weise ein zügigeres technikunterstütztes Antragsverfahren zu ermöglichen.

In Zusammenarbeit mit dem Brandenburgischen IT-Dienstleister sowie drei Modellkommunen (Landkreis Elbe-Elster, Landkreis Teltow-Fläming und Landeshauptstadt Potsdam) hat das verantwortliche Ministerium auf Grundlage der in einem „Digitalisierungslabor“ analysierten Prozessschritte die Entwicklung des Fachdienstes im

Berichtszeitraum stetig vorangetrieben. Mit Abschluss der Entwicklungsarbeit, die unter Einbeziehung externer Dienstleistungen erfolgte, soll das Vorhaben produktiv gesetzt und unter datenschutzrechtlicher Verantwortlichkeit der drei Pilotkommunen betrieben werden.

Die Landesbeauftragte wurde von den Projektverantwortlichen bereits frühzeitig eingebunden und konnte so datenschutzrechtliche und technische Aspekte bei der Konzeption und Entwicklung des Dienstangebots einbringen. Kontinuierlich – zum Teil mehrfach pro Woche – erfolgte die Erörterung der Projektinhalte in Arbeitsgruppen mit den Produktentwicklerinnen und -entwicklern sowie den fachlich zuständigen Stellen. Die rechtzeitige Beteiligung unserer Dienststelle hat sich bereits in vorangegangenen Digitalisierungsprojekten des Landes bewährt und ermöglichte auch in diesem Verfahren einen strukturierten sowie lösungs- und ergebnisorientierten Austausch zwischen den beteiligten Institutionen.

Innerhalb des bisherigen Projekts konnte noch nicht die Gesamtheit aller aufenthaltsrechtlichen Fragen betrachtet werden. Der entwickelte Fachdienst, ein webbasierter Antragsassistent, sowie die zugehörigen rechtlichen und technischen Dokumentationen beschränken sich auf die Erstbeantragung eines Aufenthaltstitels zur Erwerbstätigkeit – nicht mehr und nicht weniger. Eine Schwierigkeit lag darin, dass zwar die Vertreterinnen und Vertreter der fachlich zuständigen Stellen (z. B. der Ausländerbehörden der Landkreise) und die mit der Entwicklung beauftragten Personen den Geltungsbereich der rechtlichen Regelungen und den zukünftigen Einsatzbereich der Lösung detailliert kannten, innerbehördlichen Beteiligten wie IT-Systembetreuerinnen und -betreuern, Datenschutzbeauftragten dieses Spezialwissen jedoch zum Teil fehlte.

Im Antragsverfahren werden, vereinfacht dargestellt, die erforderlichen personenbezogenen Daten der Antrag stellenden Person über einen auf den Web-Seiten der verantwortlichen Stelle als Komponente eingebetteten Web-Service erhoben und an das jeweilige besondere elektronische Behördenpostfach übermittelt, das beim Brandenburgischen IT-Dienstleister betrieben wird. Die Pilotanwendung betrachtet nur die Erhebung, Speicherung und Übertragung

der personenbezogenen Antragsdaten bis zum Eingang in dieses Postfach. Der Abruf des jeweiligen Antrages, die Übernahme der Antragsdaten in die Fachanwendung sowie die weitere Bearbeitung und Entscheidung über den Antrag ist durch die zuständige, datenschutzrechtlich verantwortliche Stelle selbstständig zu realisieren. Für die Weiterverarbeitung sind die datenschutzrechtlichen und technischen Anforderungen jeweils in eigener Zuständigkeit zu erfüllen.

Verwaltungsdienste online – ein steiniger Weg …

Zwar wurde der Fachdienst „Aufenthaltstitel zur Erwerbstätigkeit“ im Zusammenhang mit dem Onlinezugangsgesetz entwickelt, jedoch kann er in seiner jetzigen minimalen Umsetzung die Konformität zu den gesetzlichen Anforderungen nicht umfassend gewährleisten. Hintergrund sind die mangelnden Möglichkeiten, die Antrag stellende Person rechtssicher über das Internet zu identifizieren. Sie muss deshalb bei der zuständigen Stelle persönlich erscheinen und ihre Identität nachweisen. Ein vollständig medienbruchfreier Antragsprozess ist somit noch nicht möglich. Gleiches gilt für die Vorlage weiterer für die Antragstellung erforderlicher Dokumente. Diese können zwar über den webbasierten Antragsassistenten übermittelt werden, müssen jedoch auch bei einem verpflichtenden Vor-Ort-Termin der Behörde vorgelegt werden.

Aus datenschutzrechtlicher und technischer Sicht konnten wir im Rahmen des Projektes insbesondere Fragen der Datensparsamkeit, der Erfüllung der Informationspflichten zur Herstellung der Transparenz der Datenverarbeitung, der Ermittlung und Bewertung möglicher Risiken für die Rechte und Freiheiten betroffener Personen, der Erforderlichkeit einer Datenschutz-Folgenabschätzung, der Umsetzung technischer und organisatorischer Maßnahmen sowie der Abgrenzung der Zuständigkeiten der teilnehmenden Stellen klären.

Der Fachdienst „Aufenthaltstitel zur Erwerbstätigkeit“ ist als minimal funktionsfähige Produktversion anwendungsbereit implementiert und hinreichend dokumentiert. Er wurde den verantwortlichen Stellen übergeben. Mit der Bereitstellung der Servicevereinbarung und damit auch der Regelung zur Auftragsverarbeitung erklärte der Brandenburgischen IT-Dienstleister gegenüber den Pilotkommunen die

Betriebsbereitschaft. Auf dieser Grundlage erfolgte zum Ende des Berichtszeitraums durch die Landkreise Elbe-Elster und Teltow-Fläming die datenschutzrechtliche Freigabe gemäß § 4 Absatz 1 Brandenburgisches Datenschutzgesetz.

Die Landesbeauftragte wird sowohl die Implementierung der Ergebnisse aus der ersten Projektphase in anderen brandenburgischen Landkreisen als auch die Fortentwicklung des vorliegenden bzw. die Neuentwicklung zusätzlicher Fachdienste im Themenfeld „Ein- und Auswanderung“ weiter begleiten.

Weiterhin ist eine Reihe datenschutzrechtlicher Fragen im Zusammenhang mit der länderübergreifenden Bereitstellung bzw. Nutzung von Online-Diensten zu klären, die nach dem „Einer für alle“-Prinzip entwickelt und bundesweit genutzt werden. Dabei geht es insbesondere um die datenschutzrechtliche Verantwortlichkeit, die Zulässigkeit von Datenübermittlungen und vertragliche Regelungen zwischen beteiligten Stellen.

1.3 Personenbezogene Daten in Beschlussvorlagen und Niederschriften

Im Berichtszeitraum beschwerten sich viele Bürgerinnen und Bürger darüber, dass ihre Gemeinden Unterlagen im Ratsinformationssystem veröffentlicht hatten, die ihre personenbezogenen Daten enthielten und eigentlich für die Beratungen in den Gemeindevertretungen gedacht waren. Die große Anzahl solcher Beschwerden nehmen wir zum Anlass, die Rechtslage erneut darzustellen.[17]

Die Befugnis zur Weitergabe personenbezogener Daten in Sitzungsunterlagen an die Gemeindevertretung ergibt sich in den meisten Fällen aus Artikel 6 Absatz 1 Buchstabe e und Absatz 3 Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 5 Brandenburgisches Datenschutzgesetz und § 54 Absatz 1 Nummern 1 und gegebenenfalls 2 sowie Absatz 2 Brandenburgische Kommunalverfassung (BbgKVerf). Danach dürfen der Gemeindevertretung personenbezogene Daten – beispielsweise als Anlage zu Beschlussvorlagen – zur

17 Über diese Problematik hatten wir bereits mehrfach berichtet: Tätigkeitsbericht 2014/2015, B 11.5, sowie Tätigkeitsbericht 2016/2017, B 11.3.

Verfügung gestellt werden, soweit dies für die Beschlussvorbereitung oder die Information der Gemeindevertretung sowie gegebenenfalls zur späteren Ausführung der Beschlüsse erforderlich ist. Personenbezogene Daten, die über den erforderlichen Umfang hinausgehen, dürfen nicht Bestandteil der Sitzungsunterlagen werden. Das Prinzip der Datensparsamkeit gilt auch für die Abfassung der Formblätter der Beschlussvorlagen.

Soweit Angelegenheiten in öffentlicher Sitzung behandelt werden, besteht vor der Sitzung nach § 36 Absatz 4 BbgKVerf ein allgemeines Recht, die Beschlussvorlagen der in öffentlicher Sitzung zu beratenden Tagesordnungspunkte einzusehen. Da Tagesordnungspunkte, bei denen persönliche oder wirtschaftliche Verhältnisse bestimmbarer natürlicher Personen öffentlich gemacht würden (beispielsweise individuelle Grundstücksangelegenheiten, arbeitsrechtliche Fragen oder die Teilnahme an Bieterverfahren), grundsätzlich in den nicht öffentlichen Sitzungsteil gehören, wird, neben der datensparsamen Erstellung der Formblätter, ein weiterer gewichtiger Teil der personenbezogenen Daten in Beschlussvorlagen der Einsichtnahme nach § 36 Abs. 4 BbgKVerf entzogen. Diese Daten stehen in der Regel nur den Gemeindevertreterinnen und Gemeindevertretern zum Zweck ihrer Aufgabenerfüllung zur Verfügung. Diese unterliegen insoweit der Verschwiegenheitspflicht nach § 21 BbgKVerf.

Sitzungsunterlagen datensparsam erstellen

Für die Veröffentlichung personenbezogener Daten in Sitzungsunterlagen außerhalb des Anwendungsbereichs von § 36 Absatz 4 BbgKVerf gilt Folgendes: Werden diese ohne Personenbezug veröffentlicht, ist dies datenschutzrechtlich völlig unproblematisch. Für die Veröffentlichung personenbezogener Daten in Sitzungsunterlagen, die nicht Beschlussvorlagen sind, besteht zwar keine unmittelbare gesetzliche Rechtsgrundlage. Nach § 13 BbgKVerf unterrichtet die Gemeinde die betroffenen Einwohnerinnen und Einwohner aber als eigene Aufgabe in wichtigen Gemeindeangelegenheiten. Die Zulässigkeit der Veröffentlichung bemisst sich daher nach dem bereits erwähnten Grundsatz der Erforderlichkeit zur Information der Einwohnerinnen und Einwohner. Sie ist danach zulässig, sofern aus-

schließlich die zum Verständnis unbedingt erforderlichen personenbezogenen Daten enthalten sind.

In jedem Einzelfall sind dabei die schutzwürdigen Interessen der Betroffenen sorgfältig zu prüfen. Die Namen der betroffenen Personen stellen in aller Regel keine Information dar, die für das Verständnis des Sachverhalts notwendig sind. Besondere gesetzliche Geheimhaltungspflichten wie das Sozial- und Steuergeheimnis sowie die ärztliche Schweigepflicht stehen einer Veröffentlichung in jedem Fall entgegen. Soweit die Unterlagen sich auf einen nicht öffentlich beratenen Tagesordnungspunkt beziehen, ist die personenbezogene Veröffentlichung grundsätzlich zu unterlassen. Insgesamt wird die Erforderlichkeit, personenbezogene Daten in einem Ratsinformationssystem für die Öffentlichkeit bereitzustellen, nur in wenigen Ausnahmefällen zu erkennen sein. Dies bringt es mit sich, dass dann Schwärzungen erfolgen müssen, bevor die Sitzungsunterlagen der Allgemeinheit zur Verfügung gestellt werden können.

Nach § 39 Absatz 3 BbgKVerf sind Beschlüsse der Gemeindevertretung oder deren wesentlicher Inhalt in ortsüblicher Weise der Öffentlichkeit zugänglich zu machen, soweit nicht im Einzelfall aus Gründen des öffentlichen Wohls oder zur Wahrung von Rechten Dritter etwas anderes beschlossen wird. Daraus folgt die Pflicht, Beschlüsse vor der Veröffentlichung so weit zu anonymisieren, wie ihr wesentlicher Inhalt, also die Tragweite des Beschlusses, noch erkennbar bleibt. In jedem Fall zu anonymisieren sind personenbezogene Daten in Beschlüssen, zu deren Schutz bereits der Ausschluss der Öffentlichkeit erfolgt war. Die Prüfung, ob ein Beschluss zu kürzen ist, ist aber auch dann erforderlich, wenn Beschlüsse in öffentlicher Sitzung getroffen wurden, ausnahmsweise aber personenbezogene Daten enthalten.

Ähnlich wie im Falle der Sitzungsunterlagen enthält die Brandenburgische Kommunalverfassung keine ausdrückliche Rechtsgrundlage für die Veröffentlichung der Niederschriften. Eine Verpflichtung hierzu gibt es also nicht. Wiederum ist die Gemeinde allerdings nach § 13 BbgKVerf verpflichtet, die Einwohnerinnen und Einwohner in wichtigen Gemeindeangelegenheiten zu unterrichten, sodass auch die Veröffentlichung personenbezogener Daten in der Niederschrift bei Erforderlichkeit zu diesem Zweck nicht ausgeschlossen ist.

Nach § 42 Absatz 1 BbgKVerf muss die Niederschrift einer Sitzung der Gemeindevertretung einen gewissen Mindestinhalt aufweisen – beispielsweise die Namen der Teilnehmerinnen und Teilnehmer. Dazu gehören jedoch ausschließlich solche Personen mit einem aktiven Teilnahmerecht im kommunalverfassungsrechtlichen Sinn.

Die Veröffentlichung von Niederschriften mit dem beschriebenen – auch personenbezogenen – Mindestinhalt ist unter dem Gesichtspunkt der Erforderlichkeit für die Aufgabenerfüllung der Gemeinde (Unterrichtung der Einwohnerinnen und Einwohner nach § 13 Satz 1 BbgKVerf) immer zulässig. Dazu gehört auch die Zuordnung der Teilnehmerinnen und Teilnehmer zu deren Beiträgen und Wortmeldungen. Nur so können die Interessierten das Handeln der Gemeindevertretung sowie der Verwaltung verstehen und ihre Wahlentscheidung treffen.

Weitere personenbezogene Daten können nur aufgenommen werden, wenn dies zur Unterrichtung der Einwohnerinnen und Einwohner im Einzelfall erforderlich ist. In den meisten Fällen ist es das nicht. Beispielsweise spielt es keine Rolle, welche Bürgerinnen oder Bürger über die genannten, offiziellen Teilnehmerinnen und Teilnehmer hinaus an einer Gemeindevertretersitzung teilgenommen haben. Entsprechende Anwesenheitslisten dürfen in der Regel nicht Inhalt der Niederschrift werden. Auch ist die namentliche Bezeichnung von Bürgerinnen und Bürgern, die sich im Rahmen einer Einwohnerfragestunde zu Wort gemeldet haben, für das Verständnis der Angelegenheit in aller Regel irrelevant. Soweit die Namen bzw. Anschriften der Fragestellenden für eine spätere Beantwortung erforderlich sein sollten, ist dies separat und nicht in der Niederschrift zu vermerken.

In den meisten von uns bearbeiteten Fällen haben die Gemeinden es versäumt, zwischen den Voraussetzungen für die Weiterleitung von personenbezogenen Sitzungsunterlagen an die Gemeindevertretung und an die Öffentlichkeit über das Ratsinformationssystem zu unterscheiden. Oftmals stellten sie dieselben Dokumente zuerst den Vertretungen und anschließend unverändert der Öffentlichkeit zur Verfügung, ohne zu berücksichtigen, dass für diese beiden Schritte unterschiedliche Voraussetzungen bestehen. Allerdings gelang es uns in diesen Fällen, die datenschutzgerechte Schwärzung

der Unterlagen zu erreichen, da die jeweiligen Gemeinden selbst gar keinen Grund für eine personenbezogene Veröffentlichung sahen.

1.4 Handlungsempfehlung zur E-Mail-Kommunikation von Lehrkräften

Die elektronische Kommunikation von Lehrkräften untereinander sowie mit Schülerinnen, Schülern und Eltern ist heute alltäglich. Bislang nutzten brandenburgische Lehrerinnen und Lehrer hierbei ganz unterschiedliche E-Mail-Adressen: zum Teil wurden diese von der Schule selbst eingerichtet, manchmal kümmerte sich der Schulträger darum und in einigen Fällen verwendeten Lehrkräfte auch ihre private E-Mail-Adresse, mit der sie sich bei einem der zahlreichen E-Mail-Anbieter registriert hatten. Diese Heterogenität führte in der Vergangenheit immer wieder zu Verwirrungen, erschwerte die Handhabbarkeit und Administration und sorgte in Einzelfällen auch für meldepflichtige Verletzungen des Datenschutzes. Im Berichtsjahr stellte das Ministerium für Bildung, Jugend und Sport des Landes Brandenburg jeder Lehrkraft eine persönliche dienstliche E-Mail-Adresse bereit und baute eine zentrale technische Infrastruktur für die E-Mail-Kommunikation der Lehrerinnen und Lehrer untereinander sowie mit Dritten – insbesondere mit Schülerinnen, Schülern und Eltern – im schulischen Kontext auf. Die staatlichen Schulämter haben in diesem Zusammenhang eine „Handlungsempfehlung zur Nutzung der Dienst-Mail“ erstellt und mit unserer Behörde abgestimmt.

Das Dokument enthält zunächst einige grundsätzliche Hinweise zur Zulässigkeit, Erforderlichkeit und Sicherheit der E-Mail-Kommunikation und gibt anschließend Empfehlungen für einzelne spezielle Konstellationen der Datenverarbeitung.

In der Regel ist der Versand personenbezogener Daten per E-Mail zulässig, soweit unter Berücksichtigung der Art der Daten die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes umgesetzt werden. Personenbezogene Daten, von deren Verarbeitung besondere Risiken für die Rechte und Freiheiten betroffener Personen ausgehen (sogenannte sensitive Daten), verlangen einen besonderen Schutz, also weitergehende Maßnahmen. Solche sensitiven, besonders schützenswerten

Daten im schulischen Kontext sind z. B. Noten, Aussagen zur individuellen Leistung und zum Verhalten von Schülerinnen und Schülern, konkrete Informationen zu Erziehungs- und Ordnungsmaßnahmen oder auch Gesundheitsdaten (ärztliche Atteste, Förderausschussprotokolle). Während dienstliche E-Mails mit personenbezogenen Daten grundsätzlich mindestens auf dem Transportweg zu verschlüsseln sind, erfordern solche mit sensitiven Daten zusätzlich eine Ende-zu-Ende-Verschlüsselung. Darüber hinaus ist bei jeder E-Mail-Kommunikation das Prinzip der Datenminimierung zu beachten, also gemessen am Zweck sind nur die unbedingt notwendigen personenbezogenen Daten zu übermitteln. Die Betreffzeile einer E-Mail sollte gar keine personenbezogenen Daten enthalten.

Lehrkräfte können allgemeine E-Mail-Anfragen von Eltern oder bloße Bitten um Terminabsprachen ohne weitere personenbezogene Daten auch per E-Mail beantworten. Erhalten sie jedoch von Eltern, Schülerinnen oder Schülern E-Mails mit sensitiven personenbezogenen Daten ohne hinreichende Sicherung, sollten sie lediglich den Empfang der Daten bestätigen und gleichzeitig auf die Unsicherheit des Kommunikationswegs sowie sichere Formen des Versands hinweisen. Selbst verschicken dürfen Lehrerinnen und Lehrer sensitive personenbezogene Daten per E-Mail nur dann, wenn eine Ende-zu-Ende-Verschlüsselung gewährleistet ist. Dies kann auch durch die Auslagerung der Daten in einen verschlüsselten E-Mail-Anhang erfolgen. Das jeweilige Passwort bzw. der jeweilige Schlüssel zur Entschlüsselung muss der empfangenden Person über einen zweiten Kommunikationskanal (z. B. telefonisch) mitgeteilt werden.

Weiterhin ist vor dem Versand einer E-Mail stets die Richtigkeit der Adressen der Empfängerinnen und Empfänger zu überprüfen. Die Gefahr einer Fehladressierung ist bei E-Mails besonders hoch – insbesondere wegen der automatischen Vervollständigung von Namensbestandteilen während der Eingabe bei den meisten Mailprogrammen. Die Übermittlung von E-Mails an falsche Personen kann eine nach Artikel 33 Datenschutz-Grundverordnung meldepflichtige Datenschutzverletzung darstellen. Gleiches gilt auch, wenn eine E-Mail an viele Personen versandt werden soll und deren Adressdaten nicht im BCC-Feld des E-Mail-Kopfes eingetragen werden, sondern im CC-Feld. In diesem Fall werden alle (meist personenbe-

zogenen) E-Mail-Adressen an alle Empfängerinnen und Empfänger offenbart, wofür in der Regel weder ein Bedarf noch eine Rechtsgrundlage existieren.

1.5 Weiter Klärungsbedarf zum Einsatz von Microsoft Cloud-Diensten, insbesondere Microsoft 365

Die datenschutzrechtlichen Rahmenbedingungen beim Einsatz von Cloud-Diensten des Unternehmens Microsoft, insbesondere von Microsoft 365 (bisher: Microsoft Office 365), stehen weiter im Fokus vieler Anfragen und Beratungsersuchen an unsere Behörde. Gerade vor dem Hintergrund der Corona-Pandemie und der Notwendigkeit der verstärkten Nutzung von Heimarbeit bei Behörden und Unternehmen sowie des Distanzlernens in Schulen und Hochschulen planten viele Verantwortliche, mit den genannten Produkten die Kommunikation und Kooperation besser zu unterstützen. Allerdings darf hierbei trotz der Ausnahmesituation die Einhaltung der grundlegenden gesetzlichen Regelungen des Datenschutzes, speziell im Hinblick auf die Einbeziehung von Microsoft als Dienstleister, nicht hintanstehen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) hatte schon vor geraumer Zeit eine Arbeitsgruppe eingesetzt, die insbesondere die Einhaltung der Regelungen zur Auftragsverarbeitung personenbezogener Daten gemäß Artikel 28 Datenschutz-Grundverordnung (DSGVO) beim Einsatz von Microsoft 365 in öffentlichen Stellen prüfen sollte. Die Arbeitsgruppe wurde im Arbeitskreis Verwaltung der Konferenz etabliert, der durch unsere Behörde geleitet wird.

Im Berichtszeitraum standen die Prüfung der Online Service Terms für Microsoft Online-Dienste sowie ihrer Ergänzung zum Datenschutz (Data Processing Addendum) im Mittelpunkt der Aktivitäten der Arbeitsgruppe. Da Microsoft in der Vergangenheit immer wieder Änderungen der Papiere vorgenommen hatte und die datenschutzrechtlichen Prüfungen damit stets von neuem beginnen mussten, legte die Gruppe die Fassung vom Januar 2020 zu Grunde, um die Vereinbarkeit der durch Microsoft als Dienstleister zur Verfügung gestellten Unterlagen mit den Anforderungen von Artikel 28 Absatz

3 DS-GVO zu untersuchen. Im Ergebnis wurde eine Reihe von Kritikpunkten formuliert und in Form eines Arbeitspapiers zusammengefasst:

- Die Art und der Zweck der Verarbeitung sowie die Kategorien personenbezogener Daten, die bei Microsoft im Auftrag verarbeitet werden, können nicht hinreichend detailliert beschrieben werden.

- Es bestehen Zweifel hinsichtlich der Tragfähigkeit der Rechtsgrundlagen sowie des Umfangs der Verarbeitung von personenbezogenen Daten der Auftraggeberinnen und Auftraggeber durch Microsoft für eigene Geschäftszwecke.

- Fraglich sind weiter die Auswirkungen amerikanischer Gesetze in Bezug auf Anforderungen zur Herausgabe von personenbezogenen Daten, die bei Microsoft als Dienstleister verarbeitet werden.

- Auftraggeberinnen und Auftraggeber haben vor Vertragsabschluss keine Möglichkeit, die beim Dienstleister Microsoft umgesetzten technischen und organisatorischen Maßnahmen einzusehen und können demzufolge nicht einschätzen, ob das erreichte Sicherheitsniveau für die Verarbeitung der Daten im Auftrag ausreicht.

- Es bestehen Unklarheiten hinsichtlich der Löschfristen für die von Microsoft in eigener Verantwortung und für die eigenen Geschäftszwecke verarbeiteten Daten.

- Die Information über Unterauftragnehmerinnen und Unterauftragnehmer, die von Microsoft bei der Verarbeitung einbezogen werden, ist unzureichend.

Da Microsoft mit den Vertragsunterlagen die gesetzlichen Anforderungen nach Auffassung der Arbeitsgruppe (und des Arbeitskreises) nicht in vollem Umfang erfüllt, ist die Nutzung der Online-Dienste des Unternehmens auf dieser Basis datenschutzrechtlich kritisch zu

sehen. Diese Einschätzung nahm die Datenschutzkonferenz im September 2020 mit knapper Mehrheit zustimmend zur Kenntnis.

Gleichzeitig richtete die Konferenz eine neue Arbeitsgruppe unter Vorsitz des Bayerischen Landesamtes für Datenschutzaufsicht und unserer Behörde ein, die weitere Gespräche mit Microsoft hinsichtlich der erforderlichen Anpassungen der vertraglichen Unterlagen an die gesetzlichen Anforderungen führen soll. Die oben genannten Kritikpunkte wurden dem Unternehmen mit der Bitte übersandt, hierzu Stellung zu nehmen und anhand der aktuellen Vertragsdokumente nachzuweisen, dass die Regelungen der Datenschutz-Grundverordnung eingehalten werden. Ein weiteres Thema der neu eingerichteten Arbeitsgruppe sind die Auswirkungen des Schrems-II-Urteils des Europäischen Gerichtshofs[18] auf die Auftragsverarbeitung im Rahmen von Microsoft Online-Diensten. Ein besonderes Augenmerk wird dabei auch auf die Bewertung der ergänzenden Maßnahmen zu legen sein, die das Unternehmen trifft, um ein angemessenes Datenschutzniveau bei der Auftragsverarbeitung auch im Zielland zu gewährleisten.

Microsoft zeigt sich gesprächsbereit, sodass ein erster Termin für den Austausch mit Vertreterinnen und Vertretern der Datenschutzaufsichtsbehörden für Mitte Dezember 2020 vereinbart wurde. Es ist allerdings gegenwärtig noch nicht abzusehen, ob und gegebenenfalls wann die vollständige Erfüllung der datenschutzrechtlichen Anforderungen von den Aufsichtsbehörden festgestellt werden kann. In der Zwischenzeit bleibt es jedem Verantwortlichen, der die genannten Produkte einsetzen möchte, unbenommen, eigene Vereinbarungen mit dem Dienstleister zu treffen, ergänzende technische und organisatorische Maßnahmen umzusetzen und einen umfassenden Nachweis für die rechtskonforme Nutzung eigenständig zu erbringen.

18 siehe A V 2

2 Beratungen im nicht öffentlichen Bereich

Internationale Datenverarbeitung nach dem „Schrems II-Urteil“ des Europäischen Gerichtshofs

Das Urteil des Europäischen Gerichthofs vom 16. Juli 2020 („Schrems II“, Rechtssache C-311/18) gilt in Fachkreisen als das bedeutendste Datenschutzurteil des Jahres 2020. Mit der Entscheidung stellt der Europäische Gerichthof – nun schon zum zweiten Mal[19] – klar, dass personenbezogene Daten in den USA allein durch Absprachen wie das EU-US-Privacy-Shield (im Folgenden Privacy Shield) oder Standarddatenschutzklauseln nicht ausreichend vor staatlichen Zugriffen durch US-Behörden geschützt werden. Das Urteil stellt sowohl Unternehmen als auch Vereine vor erhebliche Herausforderungen, da mit der Entscheidung die Grundlage für eine Vielzahl von Drittlandübermittlungen entfallen ist. Entsprechend erreichten uns in dessen Folge auch diverse Anfragen nicht öffentlicher Stellen zum Umgang mit der Entscheidung.

Datenübermittlungen in Drittländer (Länder außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums) sind zulässig, wenn neben den sonstigen Anforderungen der Datenschutz-Grundverordnung (DS-GVO) auch eine der Grundlagen für die Drittlandübermittlung der Artikel 44 bis 50 DS-GVO erfüllt ist. Soweit kein wirksamer Angemessenheitsbeschluss der Europäischen Kommission gemäß Artikel 45 DS-GVO vorliegt, kommen unter anderem geeignete Garantien gemäß Artikel 46 DS-GVO, vor allem die dort unter Absatz 2 Buchstabe c genannten Standarddatenschutzklauseln sowie verbindliche interne Datenschutzvorschriften innerhalb einer Organisation gemäß Artikel 47 DS-GVO oder bestimmte Ausnahmefälle gemäß Artikel 49 DS-GVO als Rechtfertigung für die Übermittlung in Frage. Auf Grundlage einer sektorspezifischen Angemessenheitsentscheidung der EU-Kommission wurden Datenübermittlungen in die USA in der Vergangenheit vor allem über eine

19 Siehe Urteil des Europäischen Gerichtshofs vom 6. Oktober 2015, Rechtssache C-362/14, “Schrems“, durch das dieser bereits den Kommissionsbeschluss zu Safe Harbour, den Vorgänger des EU-US Privacy Shield, für ungültig erklärte.

Zertifizierung von US-Unternehmen im sogenannten Privacy Shield gerechtfertigt.[20]

Mit der Entscheidung „Schrems II“ erklärte der Europäische Gerichtshof diesen allerdings für ungültig und stellte generell in Frage, unter welchen Voraussetzungen eine Datenübermittlung in die USA zulässig ist. Ausschlaggebend hierfür war, dass nach dessen Ansicht die nach den dortigen Rechten bestehenden Eingriffsmöglichkeiten der US-Regierung in Bezug auf die Daten von Bürgerinnen und Bürgern der EU unverhältnismäßig seien. Kritisiert wurde zudem das Fehlen einer gerichtlichen Kontrolle, also explizit der fehlende Rechtsschutz vor staatlichen Maßnahmen. Das Gericht stellte dabei fest, dass die im Kommissionsbeschluss zum Privacy Shield festgelegten Maßnahmen, wie z. B. ein Ombudsmechanismus, sich nicht eigneten, um ein angemessenes Datenschutzniveau herzustellen. Aufgrund dieser Wertung bestehen auch Zweifel, ob andere Rechtfertigungstatbestände wie Standarddatenschutzklauseln oder verbindliche interne Datenschutzvorschriften geeignet sind, eine Datenübermittlung in die USA oder gegebenenfalls andere Drittstaaten zu rechtfertigen. Denn auch wenn der Europäische Gerichtshof den für die Standarddatenschutzklauseln geltenden Beschluss 2010/879 der Europäischen Kommission als gültig bewertete, merkte das Gericht an, dass zusätzliche Maßnahmen erforderlich seien, um ein angemessenes Schutzniveau im Drittland zu gewährleisten. Dies gilt grundsätzlich für alle Datenübermittlungen in Drittländer, wenn für das jeweilige Land kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Neben den USA sind das vor allem auch Russland oder China.

Drittländer müssen angemessenes Datenschutzniveau bieten

Um Verantwortliche und Auftragsverarbeiter als Datenexporteure dabei zu unterstützen, geeignete Maßnahmen zu finden, hat der Europäische Datenschutzausschuss ein Papier mit Empfehlungen zur Prüfung von Datenübermittlungen in Drittstaaten veröffentlicht,[21] das in englischer Sprache auch in unserem Internetangebot bereit-

20 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016.

21 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

steht. Die Empfehlungen sehen sechs Schritte für die Prüfung eines solchen Transfers vor:

- Bestandsaufnahme: Erfassung, in welchen Fällen personenbezogene Daten in ein Drittland übermittelt werden.

- Bestimmung der Rechtsgrundlage für die Drittlandübermittlung: Festlegung, welches Mittel zur Rechtfertigung der Drittlandübermittlung in Betracht kommt, zum Beispiel ein Angemessenheitsbeschluss der EU-Kommission nach Artikel 45 DS-GVO, geeignete Garantien gemäß Artikel 46 DS-GVO (u. a. Standarddatenschutzklauseln oder verbindliche interne Datenschutzvorschriften gemäß Artikel 47 DS-GVO) und Ausnahmeregelungen gemäß Artikel 49 DS-GVO.

- Einschätzung des Rechts im Drittland: Wenn die Übermittlung auf Grundlage geeigneter Garantien gemäß Artikel 46 DS GVO erfolgt, muss zusätzlich geprüft werden, ob sich aus dem Recht bzw. den Praktiken des Drittlands Einschränkungen ergeben, die dazu führen, dass trotz der gewählten Mittel kein angemessenes Schutzniveau gewährleistet werden kann.

- Ergreifen zusätzlicher Maßnahmen: Wenn in Schritt 3 Einschränkungen festgestellt werden konnten, muss geprüft werden, ob Maßnahmen in Betracht kommen, die das Datenschutzniveau auf den EU-Standard heben.

- Umsetzung formaler Schritte: Wenn die Übermittlung auf Grundlage geeigneter Garantien stattfinden soll, müssen die formalen Vorgaben aus Artikel 46 DS-GVO beachtet werden, z. B. eine Konsultation der zuständigen Aufsichtsbehörde.

- Regelmäßige Überprüfung: Um dem Grundsatz der Rechenschaftspflicht nachzukommen, ist es erforderlich, in angemessenen Zeitabständen das Schutzniveau für personenbezogene Daten im Drittland neu zu bewerten und Entwicklungen zu beobachten, die sich darauf auswirken können.

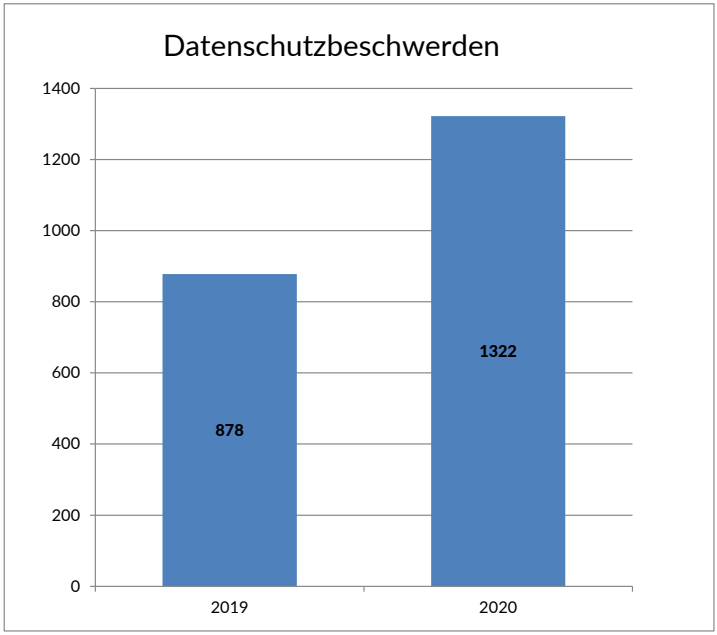
In Anlage 2 des Papiers werden darüber hinaus diverse technische, organisatorische und vertragliche Maßnahmen genannt, die im Rahmen von Schritt 4 herangezogen werden können.

Auf Grundlage der Empfehlungen des Europäischen Datenschutzausschusses wird sich allerdings nicht jede Datenübermittlung in ein Drittland rechtfertigen lassen. Wenn die Standarddatenschutzklauseln bei einer Drittlandübermittlung nicht eingehalten werden oder nicht eingehalten werden können und der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht durch andere Mittel gewährleistet werden kann, muss die Übermittlung ausgesetzt oder beendet werden. Andernfalls sind wir als Aufsichtsbehörde nach dem Urteil des Europäischen Gerichtshofs verpflichtet, diese Übermittlung zu untersagen.

VI Zahlen und Fakten

1 Beschwerden

Im Berichtszeitraum gingen bei der Landesbeauftragten 1.322 Beschwerden ein. Diese wurden von natürlichen Personen eingereicht, die der Ansicht waren, dass die Verarbeitung ihrer personenbezogenen Daten sie in ihren Rechten verletzt und gegen das Datenschutzrecht verstößt.

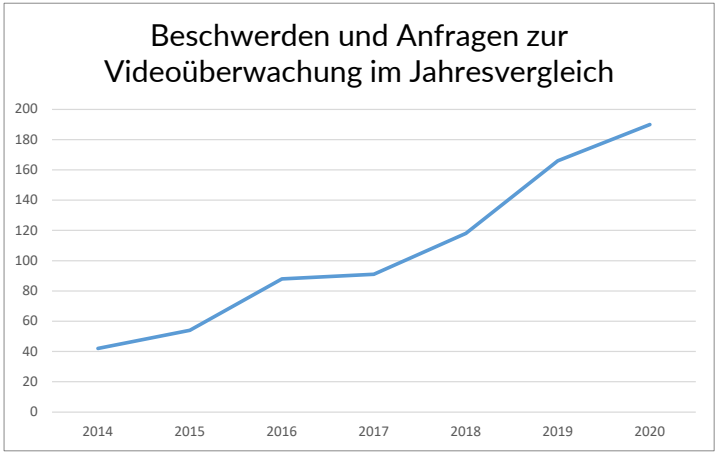


2 Videoüberwachung: Beschwerden und Anfragen

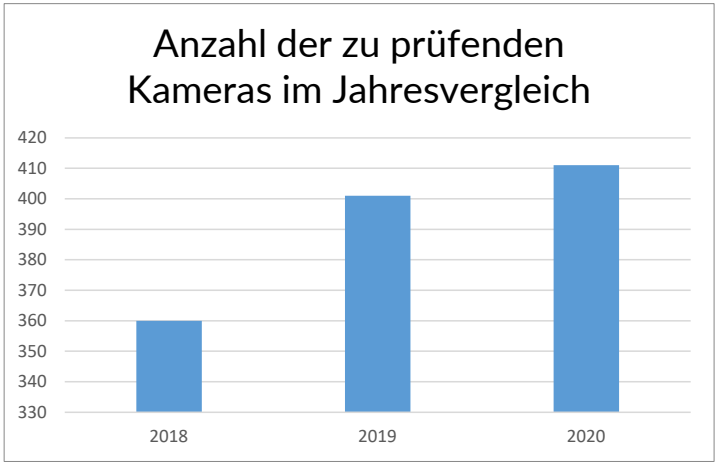
Videokameras sind weit verbreitet; sie werden unter anderem in Unternehmen, in Ladengeschäften, Restaurants und Cafés sowie in Freizeitstätten eingesetzt. Gemeinden möchten beispielsweise die Fahrradparkplätze am Bahnhof überwachen, das Justizzentrum Potsdam seine Gebäude und Kitas ihre Eingangsbereiche. Viele Bürgerinnen und Bürger möchten mit Videokameras ihre Grundstücke und Häuser schützen. Auch in Fahrzeugen werden sie als sogenannte Dashcams vermehrt installiert.

In vielen Fällen wenden sich Beschwerdeführerinnen und Beschwerdeführer an uns, weil sie sich durch die Videoüberwachung im öffentlich zugänglichen Raum einem Überwachungsdruck ausgesetzt und dadurch in ihren Persönlichkeitsrechten verletzt fühlen.

Seit Jahren verzeichnet die Landesbeauftragte eine Zunahme von Beschwerden und schriftlichen Anfragen zur Videoüberwachung durch Privatpersonen, Unternehmen und öffentliche Stellen. Wurden im Jahr 2014 lediglich 42 Beschwerden und Anfragen an uns gerichtet, stieg deren Zahl im Jahr 2019 auf 166. Im Berichtszeitraum erhöhten sich die Beschwerden und Anfragen auf 190. Die zahlreichen telefonischen Auskünfte haben wir nicht statistisch erfasst.



Mit jeder Videoüberwachung ist in der Regel der Einsatz mehrerer Kameras verbunden. Insofern waren im Jahr 2018 insgesamt 360 Videokameras, im Folgejahr 401 und im Berichtszeitraum 411 Kameras auf ihre rechtliche Zulässigkeit und auf technisch-organisatorische Maßnahmen zu überprüfen.



Die Zulässigkeitsprüfung verlangt, dass die Landesbeauftragte alle für die datenschutzrechtliche Bewertung erheblichen Aspekte der Datenverarbeitung, beispielsweise den Zweck der Verarbeitung, den Erfassungsbereich oder die technischen Gegebenheiten, kennt. Dies kann nicht immer im schriftlichen Verfahren erreicht werden. Häufig erfordern die Umstände des Einzelfalles eine Prüfung vor Ort. Der Zeitaufwand hierfür ist in einem Flächenland wie Brandenburg sehr groß. Dadurch kommt es zu erheblichen Engpässen bei der Bearbeitung der Beschwerden und Anfragen. Ergibt die Bewertung, dass die Verarbeitungsmodalitäten nicht im Einklang mit den Rechtsvorschriften stehen, ergreift die Landesbeauftragte entsprechende Abhilfemaßnahmen. Artikel 58 Absatz 2 Datenschutz-Grundverordnung stellt einen umfassenden Katalog zur Verfügung. Beispielsweise kann sie den Verantwortlichen anweisen, die Videoüberwachung in Einklang mit der Datenschutz-Grundverordnung zu bringen oder eine Einschränkung der Verarbeitung anordnen.

3 Beratungen

Neben der Bearbeitung von Beschwerden gehört auch die Beratung zu Datenschutzfragen zu den Aufgaben der Landesbeauftragten. Sie hat betroffene Personen, Verantwortliche im öffentlichen und nicht öffentlichen Bereich sowie die Landesregierung bei Rechtssetzungsverfahren in insgesamt 688 Fällen schriftlich beraten. Hinzu kommt eine Vielzahl telefonischer Beratungen, die nicht statistisch erfasst werden. Wie auch im Falle von Beschwerden zeigt sich, dass die Zahl der schriftlichen Beratungen im Berichtszeitraum um mehr als 50 % gestiegen ist.

4 Meldungen von Datenschutzverletzungen

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

Im Berichtszeitraum erhielt die Landesbeauftragte insgesamt 409 Meldungen von Datenschutzverletzungen. Das bedeutet erneut eine spürbare Steigerung gegenüber dem Vorjahr, in welchem 362 Meldungen eingingen. Die Datenschutzverletzungen passierten sowohl im öffentlichen (190 Meldungen) als auch im nicht öffentlichen Bereich (218 Meldungen).

Fast die Hälfte aller Meldungen betraf den Fehlversand von Unterlagen (insgesamt 198 Fälle). Hiervon umfasst sind sowohl Fehlkuvertierungen von Briefpost, versehentlicher E-Mail-Versand an einen offenen Verteilerkreis, Namensverwechslungen oder die Beifügung

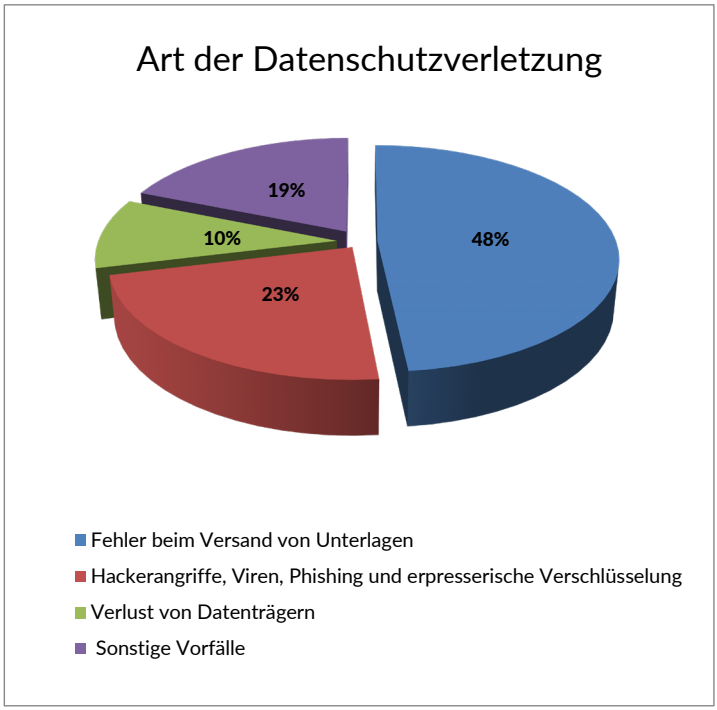
von Unterlagen unbeteiligter Dritter. So verschickte etwa ein Verantwortlicher versehentlich die Mitteilung einer arbeitsrechtlichen Maßnahme an den falschen Mitarbeiter. Und ein anderer Verantwortlicher ordnete aufgrund eines fehlerhaften E-Mail-Versands die coronabedingte Isolation des Empfängers an – nur handelte es sich hierbei nicht um die richtige Person.

Einen signifikanten Anteil der Meldungen machten auch die 93 Datenschutzverletzungen aus, die auf technischen Mängeln beruhen und insofern Virenbefall, Phishing, Hackerangriffe, unberechtigte Zugriffe Dritter und erpresserische Verschlüsselungen von Datensätzen ermöglichen. Hieran wird deutlich, dass Verantwortliche dem Einsatz und der Aktualität der technischen und organisatorischen Datenschutzmaßnahmen verstärkt Aufmerksamkeit widmen müssen.

Ein Abhandenkommen physischer Datenträger, etwa Diebstähle durch Einbrüche in Räume des Verantwortlichen oder durch den Verlust auf dem Postweg, wurde der Landesbeauftragten in 41 Fällen gemeldet.

Eine bunte Mischung aus 77 Datenschutzverletzungen fällt in die Kategorie „Sonstiges“. Beispielhaft hierfür sind die Fälle, in denen Papierdokumente mit personenbezogenen Daten versehentlich im Hausmüllcontainer entsorgt wurden, anstatt sie datenschutzkonform zu vernichten. Besonders brisant waren die gemeldeten Fälle eines Verantwortlichen mit Publikumsverkehr, bei dem Abhörgeräte gefunden wurden und eines anderen Verantwortlichen, der Bausparverträge an falsche Empfänger ausgezahlt hatte.

In der weit überwiegenden Anzahl betrafen die einzelnen Datenschutzverletzungen nur wenige Personen gleichzeitig. Dies ist vermutlich, ebenso wie im Vorjahr, mit der hohen Anzahl an fehlversandten Unterlagen zu erklären. Datenschutzverletzungen mit mehr als 1.000 Betroffenen wurden der Landesbeauftragten 22 Mal gemeldet.


Art der Datenschutzverletzung
19%
10%
48%
23%
Fehler beim Versand von Unterlagen
Hackerangriffe, Viren, Phishing und erpresserische Verschlüsselung
Verlust von Datenträgern
Sonstige Vorfälle

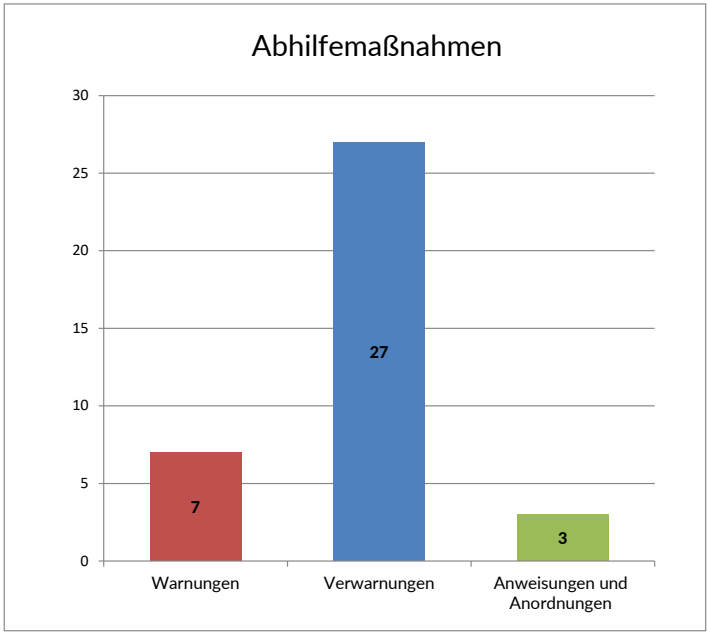
5 Abhilfemaßnahmen

5.1 Warnungen, Verwarnungen, Anweisungen und Anordnungen

Gemäß Artikel 58 Absatz 2 Datenschutz-Grundverordnung (DS-GVO) 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 passiert, würde aber verwirklicht, wenn der Verantwortliche sein Handeln unverändert fortführt.

Eine Maßnahme fasst dabei häufig mehre Einzelfälle oder Verstöße zusammen. So kann beispielsweise bei einem großflächigen Areal mit einer hohen Anzahl von Kameraüberwachungseinrichtungen eine Vielzahl unterschiedlich zu bewertender Überwachungsszenarien vorliegen. Hier könnte jeweils gegen jede einzelne Kameranutzung eine gesonderte Anordnung ausgesprochen werden. Erfolgt jedoch die Bewertung des Betriebs mehrerer Kameras in einer Maßnahme, muss trotzdem jede für sich geprüft und rechtlich beurteilt werden. Die bloße Zahl der Maßnahmen spiegelt daher nur teilweise die tatsächlich vorgefundenen Umstände wider.

Die Landesbeauftragte sprach im Berichtszeitraum sieben Warnungen, 27 Verwarnungen und drei Anordnungen aus. Mit letzteren wurden Verantwortliche zum konkreten Tun oder Unterlassen angewiesen. Hinzu kommen die im folgenden Abschnitt behandelten Bußgeldverfahren.



5.2 Geldbußen

Im Berichtszeitraum wurden der Bußgeldstelle der Landesbeauftragten 70 Sachverhalte wegen Verstößen gegen datenschutzrechtliche Vorgaben zur Kenntnis gegeben. Dies bedeutete eine spürbare Steigerung im Vergleich zu den im Vorjahr eingegangenen 47 Fällen. Die im Jahr 2020 betriebenen Verfahren wurden zu einem großen Anteil, nämlich in 56 Fällen, von den zuständigen Polizeibehörden oder Staatsanwaltschaften an unsere Bußgeldstelle weitergeleitet. Einen kleineren Anteil stellten insgesamt 9 Sachverhalte dar, die von aufsichtsbehördlich tätigen Mitarbeiterinnen und Mitarbeitern der Landesbeauftragten an die Bußgeldstelle abgegeben wurden. Die übrigen 5 Fälle folgten aus Abgaben anderer Aufsichtsbehörden mangels eigener dort bestehender Zuständigkeit.

Alle eingegangenen Verfahren waren nach der aktuellen Rechtslage unter Geltung der Datenschutz-Grundverordnung zu beurteilen.

Im Berichtszeitraum hat die Bußgeldstelle insgesamt 68 Verfahren abgeschlossen, die sich sowohl gegen nicht öffentliche Stellen als auch gegen Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen richteten. Knapp die Hälfte der abgeschlossenen Verfahren war davon im vorangegangenen Berichtszeitraum eröffnet worden.

In 16 Fällen verhängte die Landesbeauftragte wegen der festgestellten datenschutzrechtlichen Verstöße ein Bußgeld. Die Gesamtsumme der festgesetzten Bußgelder betrug 331.200 Euro. In den übrigen Fällen wurde entweder kein Ordnungswidrigkeitenverfahren eingeleitet, das Verfahren eingestellt oder mangels Zuständigkeit an die entsprechende Verfolgungsbehörde abgebeben.

6 Europäische Verfahren

Die Artikel 60 ff. Datenschutz-Grundverordnung (DS-GVO) sehen vor, dass bei grenzüberschreitender Datenverarbeitung eine europaweite Zusammenarbeit der Datenschutzaufsichtsbehörden erfolgen muss. Eine solche grenzüberschreitende Verarbeitung liegt zum Beispiel dann vor, wenn der Verantwortliche personenbezogene Daten von Bürgerinnen und Bürgern mehrerer Mitgliedsstaaten verarbeitet oder verarbeiten lässt. Um die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden zu erleichtern, erfolgt der gegenseitige Austausch elektronisch über das Binnenmarkt-Informationssystem (IMI) der Europäischen Kommission. In diesem Rahmen hat die Landesbeauftragte in 1.433 Fällen geprüft, ob und welche Maßnahmen zu treffen sind:

In 801 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 entsprechend Verfahrensschritte ergriffen werden müssen. Die Federführung orientiert sich dabei an der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen in der EU. Eine Betroffenheit unserer Behörde ist demgegenüber dann gegeben, wenn die gemeldete Verarbeitungstätigkeit durch die jeweiligen Unternehmen erhebliche Auswirkungen auf Bürgerinnen und Bürger im Land Brandenburg haben könnte oder

die verantwortliche Stelle eine Niederlassung im Zuständigkeitsbereich der Landesbeauftragten hat.

Eine Federführung der Landesbeauftragten haben wir in vier Fällen grenzüberschreitender Datenverarbeitungen angenommen. Eine Betroffenheit unserer Behörde ergab sich in 32 Fällen. In den übrigen Fällen haben wir nach Durchsicht entschieden, uns nicht an dem weiteren Verfahren zu beteiligen, da die Verantwortlichen keine Niederlassung in Brandenburg hatten und keine Auswirkungen auf Brandenburgerinnen und Brandenburger festzustellen waren.

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

In 682 Fällen beteiligten wir uns an Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII Datenschutz-Grundverordnung, etwa im Rahmen gegenseitiger Amtshilfe oder bei der Vorbereitung einer Stellungnahme des Europäischen Datenschutzausschusses. Davon gehen 18 auf die Initiative der Landesbeauftragten zurück.

Im Berichtszeitraum wurden 89 Kooperationsverfahren nach Artikel 60 DS-GVO (One-Stop-Shop-Verfahren) durch einen Beschluss der jeweils zuständigen federführenden Aufsichtsbehörde abgeschlossen. 40 dieser Beschlüsse beruhen auf Prüfungen anderer deutscher Aufsichtsbehörden, zwei gehen auf die Landesbeauftragte zurück.

7 Förmliche Begleitung von Rechtssetzungsvorhaben

Aus den zahlreichen Beratungen ist die Begleitung legislativer Maßnahmen durch die Landesbeauftragte besonders hervorzuheben. Im Rahmen der insgesamt 688 Beratungen nahmen wir 29 Mal zu Gesetzen, Verordnungen, Satzungen oder Verwaltungsvorschriften Stellung. Die rechtliche Grundlage zur Beteiligung der Landesbeauftragten folgt aus § 18 Absatz 5 Satz 1 Brandenburgisches Daten-

schutzgesetz. 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 legislativen Maßnahmen.

Teil B: Bericht nach Art § 37 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdaten-schutzgesetz

1 Vorbemerkung zur Änderung der Rechtslage

Im vorangegangenen Tätigkeitsbericht berichteten wir über die im Land Brandenburg Mitte 2019 erfolgte Umsetzung der europäischen Richtlinie (EU) 2016/680 für Behörden, die zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder für die Strafvollstreckung personenbezogene Daten verarbeiten. Das neu geschaffene Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) richtet sich sowohl an Polizeibehörden als auch an die Justiz- und Maßregelvollzugsbehörden des Landes. Für die Polizei war damit dieses Gesetz neben spezialgesetzlichen Vorschriften (z. B. im Polizeigesetz oder in der Strafprozessordnung) für datenschutzrechtliche Fragen als maßgebliches Regelwerk heranzuziehen – unabhängig davon, ob sie zur Gefahrenabwehr oder zur Strafverfolgung tätig wurde. Diese einheitliche landesgesetzliche Ordnung wurde durch das zeitlich später in Kraft getretene Gesetz des Bundes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren[22] wieder aufgelöst.

Mit Artikel 1 dieses Gesetzes fügte der Bundesgesetzgeber die Regelung von § 500 neu in die Strafprozessordnung (StPO) ein. Diese Verweisungsnorm erklärt bei Datenverarbeitungen nach der Strafprozessordnung den dritten Teil des Bundesdatenschutzgesetzes (§§ 45 bis 84 BDSG) für entsprechend anwendbar. In diesem Teil finden sich sowohl Begriffsbestimmungen, Rechtsgrundlagen für die Verarbeitung personenbezogener Daten, Regelungen zu Betroffenenrechten, Auftragsverarbeitung, Berichtigung bzw. Löschung personenbezogener Daten als auch Vorschriften zum Datenschutz durch Technikgestaltung, Protokollierung und Datenübermittlungen an Drittstaaten oder internationale Organisationen.

Durch die Einfügung des § 500 StPO ergibt sich folgende Systematik: Handelt die Polizei zur Abwehr von Gefahren oder zur vorbeugenden Bekämpfung von Straftaten und erhebt personenbezogene Daten gemäß dem Brandenburgischen Polizeigesetz präventiv, gelten für die Datenverarbeitung neben den polizeigesetzlichen Normen die Regeln des Brandenburgischen Polizei-, Justizvollzugs- und

22 Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 20. November 2019 (BGBl. I 1724).

Maßregelvollzugsdatenschutzgesetzes. Soweit die Polizei aufgrund der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten (repressiv) tätig wird, sind dagegen die datenschutzrechtlichen Bestimmungen dieser Gesetze abschließend. Es sind ausschließlich spezialgesetzliche Normen des Gesetzes über Ordnungswidrigkeiten bzw. der Strafprozessordnung oder, soweit diese datenschutzrechtliche Belange nicht abschließend regeln, über die Verweisung in § 500 StPO die Bestimmungen in Teil 3 des Bundesdatenschutzgesetzes anwendbar. Die Datenschutzaufsicht verbleibt, wie § 500 Nummer 2 StPO klarstellt, bei der Landesbeauftragten. Das Anrufungsrecht betroffener Personen ist in den Fällen repressiven Handelns zwar in § 60 BDSG geregelt, hinsichtlich der datenschutzrechtlichen Aufsichtsbefugnisse der Landesbeauftragten über die Polizei gilt allerdings in beiden Fällen § 36 BbgPJMDSG.

2 Kennzeichenerfassungssystem KESY

Die automatisierte Kennzeichenerfassung und -speicherung – wie sie seit Jahren von der Polizei in Brandenburg mit dem Verfahren KESY betrieben wurde – hat ein Ende gefunden. 2019 hatten wir den Betrieb der Kameras im Aufzeichnungsmodus, der auf §§ 136f i. V. m. 100h Absatz 1 Satz 1 Nummer 2 Strafprozessordnung (StPO) gestützt wurde, beanstandet und eine Warnung ausgesprochen.[23] Wir konnten keine hinreichende Rechtsgrundlage erkennen, unterschiedslos Kennzeichendaten aller aufgezeichneten Kraftfahrzeuge und damit der ganz überwiegend unbeteiligten und zu Zielpersonen avancierenden Fahrzeugführenden zu verarbeiten. Aufgrund der Eingriffsqualität gegenüber diesen hielten wir die Maßnahme für unverhältnismäßig und sahen zudem Verstöße gegen das Gebot der Datensparsamkeit, das Erforderlichkeitsprinzip und die Notwendigkeit der unverzüglichen Löschung nicht erforderlicher Daten.

Selbst wenn man die Auffassung der Strafverfolgungsbehörden teilt, dass eine Rechtsgrundlage für die Nutzung von Kennzeichenlesesystemen bei der Strafverfolgung vorliegt, sahen wir diese als nicht mehr eingehalten an. Wir forderten, dass die Polizei für die laufenden Ermittlungsverfahren sowohl der brandenburgischen als auch anderer Staatsanwaltschaften (Fremdstaatsanwaltschaften) zukünftig jeden-

23 Tätigkeitsbericht Datenschutz 2019, B 3.4.

falls eine zeitnahe Durchsicht und Auswertung der gespeicherten sowie die Löschung nicht mehr benötigter Kennzeichendaten sicherstellt. In brandenburgischen Verfahren, in denen die gespeicherten Aufzeichnungen durch zugriffsberechtigte polizeiliche Ermittlerinnen und Ermittler aufgerufen und ausgewertet werden können, sollte eine Durchsicht tage- oder zumindest wochenweise erfolgen. In diesen Fällen ist eine kurzfristige Abstimmung mit den ermittlungsleitenden Staatsanwaltschaften, ob die Daten zur Strafverfolgung noch benötigt werden, gewährleistet. Dagegen gestaltet sich eine zeitnahe Auswertung und Löschung nicht relevanter Kennzeichendaten bei Verfahren aus anderen Ländern schwieriger, da die brandenburgische Polizei diese nicht selbst auswertet. Dennoch sollten diese Daten spätestens nach drei Monaten an die zuständige Staatsanwaltschaft übergeben und bei der brandenburgischen Polizei gelöscht werden. Die Polizei sahen wir dabei als verpflichtet an, eine Entscheidung der Staatsanwaltschaften herbeizuführen, d. h. aktiv um eine Verfügung zur weiteren Verwendung des Datenbestands zu ersuchen.

Am 26. Februar 2020 führten wir eine Nachkontrolle im Polizeipräsidium Brandenburg durch, bei der wir uns die laufenden Maßnahmen zur Bereinigung des Altdatenbestandes erläutern ließen. Zudem informierten wir uns über die geplanten Änderungen des Verfahrens KESY.

2.1 Umgang mit Altdaten

Die im Zusammenhang mit einem brandenburgischen Ermittlungsverfahren seit April 2017 bis Juni 2019 gespeicherten Kennzeichendaten (Altdaten) wurden zunächst vom KESY-Server auf ein gesondertes, externes, nicht für polizeiliche Abfragen zugängliches Speichermedium übertragen und auf dem Server gelöscht. Die Polizei hat sich dann an 35 Staatsanwaltschaften in 13 Bundesländern und den Generalbundesanwalt mit der Bitte gewandt, die Notwendigkeit weiterer Speicherung der Kennzeichendaten zu prüfen. Im Falle einer Negativentscheidung wurde eine Löschungsverfügung erbeten. Auffällig war, dass die überwiegende Anzahl der angefragten Staatsanwaltschaften keinen weiteren Bedarf an den Kennzeichendaten zurückmeldete. An die Staatsanwaltschaften, die keine

Löschung verfügt hatten, wurden bis Oktober 2020 alle Altdaten übergeben. Anfang Oktober erhielten wir vom zuständigen Polizeipräsidium die schriftliche Mitteilung, dass in Brandenburg alle vorhandenen Altdaten gelöscht wurden.

Darüber hinaus hat das Polizeipräsidium intern eine Reihe von Maßnahmen getroffen, um eine Akkumulation von Kennzeichendaten und deren Nutzung einzuschränken:

- Die Rechtevergabe für Zugriffe auf die gespeicherten Kennzeichendaten wurde auf diejenigen Personen beschränkt, die im Rahmen eines Observationsbeschlusses und einer Anordnung der Staatsanwaltschaft befugt sind, gespeicherte Kennzeichendaten einzusehen. Darüber hinaus erarbeitet das Polizeipräsidium eine Online-Schulung an der Hochschule der Polizei zum Einsatz von KESY, an der künftig berechtigte Nutzerinnen und Nutzer teilnehmen müssen. Die Rechtevergabe für das Verfahren muss begründet und von Vorgesetzten bestätigt werden. Die Nutzungsberechtigung für die Anwendung wird für einzelne Rechner freigeschaltet. Ein Zugriff von anderen Rechnern des Polizeinetzes ist nicht mehr möglich.

- Die Polizei aktiviert künftig den Aufzeichnungsmodus der Kameras, der alle Fahrzeuge erfasst, die die Anlage passieren, erst, wenn eine ausdrückliche schriftliche Verfügung der jeweiligen Staatsanwaltschaft zum Umfang der Nutzung insbesondere zum Aufzeichnungsmodus vorliegt.

- Unabhängig von der Laufzeit der Anordnung bei der Kennzeichenerfassung im Daueraufzeichnungsmodus verpflichtet eine interne Anweisung die polizeilichen Sachbearbeiterinnen und Sachbearbeiter, die gespeicherten Daten unverzüglich auszuwerten. Stellt sich heraus, dass die Daten für das Strafverfahren nicht mehr benötigt werden, ist eine Löschungsanordnung der Staatsanwaltschaft einzuholen. Auch wenn diese Regelung mehr Spielräume belässt als unsere Vorgaben in der ausgesprochenen Warnung, stellt sie eine wesentliche Verbesserung dar.

- Die rückwirkende Suchmöglichkeit in dem bestehenden Datenbestand wurde maßgeblich eingeschränkt. Während zuvor Daten und Bilder aller Kennzeichen von allen auch parallel vorliegenden Beschlüssen rückwirkend für 28 Tage eingesehen werden konnten, wurden Zugriffe nunmehr ausschließlich auf die Daten beschränkt, die während des Anordnungszeitraums einer jeweils zugrundeliegenden staatsanwaltlichen Anordnung erhoben werden. Das Polizeipräsidium beauftragte in dieser Hinsicht auch die Weiterentwicklung des Verfahrens, in dem systemseitige Zugriffsbeschränkungen ausgeweitet werden sollen.

Endlich: KESY-Altdaten gelöscht

Die aufwendige Sachverhaltsaufklärung zur Nutzung des Verfahrens KESY und die Überzeugungsarbeit, die bei den zuständigen Polizeibehörden nach Bekanntwerden des auslösenden Ermittlungsfalls im Hinblick auf die datenschutzrechtliche Bewertung in den letzten eineinhalb Jahren geleistet werden musste, haben sich gelohnt. Wesentlich ist, dass die Polizei Brandenburg ihre datenschutzrechtliche Verantwortung für die Kennzeichenerfassung anerkannt hat und erhebliche Anstrengungen unternimmt, das Verfahren rechtskonform und datensparsam umzugestalten. Der gespeicherte Altbestand an Kennzeichendaten bis einschließlich Juni 2019 wurde, soweit er nicht für anhängige Ermittlungs- und Strafverfahren vorgehalten werden muss, gelöscht.

Nach wie vor bestehen unterschiedliche Auffassungen darüber, ob die Anordnung sonstiger besonderer für Observationszwecke bestimmter technischer Mittel gemäß § 100h Absatz 1 Satz 1 Nummer 1 StPO eine tragfähige Rechtsgrundlage für die strafprozessuale Dauererfassung von Kennzeichen darstellt. Auch hier zeichnet sich jedoch eine Veränderung ab, nachdem die Justizministerkonferenz 2019 das Bundesministerium der Justiz und für Verbraucherschutz gebeten hatte, eine gesetzliche Regelung zum Einsatz von automatisierten Kennzeichenlesesystemen im Strafverfahren zu erarbeiten. Am 15. Oktober 2020 veröffentlichte das Ministerium auf seiner Internetseite einen Referentenentwurf, der eine spezialgesetzliche Befugnis zum Fahndungseinsatz solcher Systeme im Strafverfahren enthält. Zweck des neu einzufügenden § 163g StPO-Entwurfs ist es laut Begründung, eine ausdrückliche rechtsichere Regelung nach

den Vorgaben des Bundesverfassungsgerichts zu schaffen. Danach muss für den Einsatz des automatisierten Kennzeichenlesesystems an bestimmten Stellen im öffentlichen Verkehrsraum ein auf Tatsachen gestützter Anfangsverdacht der Begehung einer Straftat von erheblicher Bedeutung bestehen. Weiter wird die Maßnahme auf den Zweck der Ermittlung des Aufenthaltsorts der oder des Beschuldigten begrenzt. Die für den automatisierten Abgleich vorgesehenen Halterdaten müssen vorab in dem schriftlichen Anordnungsverfahren genau bezeichnet werden. Der nachfolgend geregelte Abgleich der erfassten Kennzeichen, der unverzüglich auf die Erhebung zu folgen hat, bezieht sich auf Halterdaten von Fahrzeugen der Zielpersonen, also Beschuldigte oder Kontaktpersonen, die mit Beschuldigten in Verbindung gebracht werden können. Trefferdaten sollen manuell nachgeprüft, die übrigen erhobenen Daten sofort und spurenlos gelöscht werden.

Da im laufenden Gesetzgebungsverfahren noch Änderungen am Wortlaut zu erwarten sind, kann eine abschließende Bewertung dieses Regelungsvorschlags noch nicht vorgenommen werden. Eine Daueraufzeichnung, wie sie bisher durchgeführt wurde, scheint jedoch zukünftig ausgeschlossen zu sein. Am 22. Januar 2021 wurde dem Bundesrat die Neuregelung des § 163g StPO mit dem Gesetzentwurf zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften[24] zugeleitet.

2.2 Neuentwicklung des Verfahrens

Im Rahmen der Prüfung des Kennzeichenerfassungssystems KESY haben wir bereits im Jahr 2019 diverse Mängel bei den technisch-organisatorischen Maßnahmen festgestellt. So war die Datenverarbeitung – bis auf die stets umgesetzte Trennung nach präventiven und repressiven Zwecken – nicht nach den jeweiligen Ermittlungsverfahren und den jeweils betroffenen Personen getrennt und dadurch die unverzügliche Löschung von nicht mehr erforderlichen Daten erschwert bzw. unmöglich. Es fehlte außerdem an einer klaren Löschroutine. Zudem konnten alle nutzungsberechtigten Personen bis zu 28 Tage rückwirkend alle erhobenen Daten ohne automatische Beschränkung auf den jeweiligen Beschlusszeitraum einsehen.

24 Bundesrats-Drucksache 57/21 vom 22. Januar 2021.

Eine entsprechende Zugriffsbegrenzung konnte nur organisatorisch geregelt werden, da eine technische Umsetzung von differenzierten Zugriffsrechten mit der Software nicht möglich war. Nach Ablauf eines der Überwachung zugrunde liegenden Beschlusses mussten Nutzungsberechtigungen manuell entzogen werden, da es keine technische Möglichkeit gab, dies zu automatisieren. Zudem konnte nicht die Anzahl der gespeicherten Kennzeichen zu einem bestimmten Zeitpunkt – bezogen auf einen, mehrere oder alle Kamerastandorte – abgefragt werden; ein Gesamtüberblick über die verarbeiteten Kennzeichendaten war dadurch stark erschwert.

Diese Mängel haben wir gegenüber dem Polizeipräsidium Brandenburg kritisiert und klare Empfehlungen zur Verbesserung des Verfahrens gegeben. Im Rahmen der Nachkontrolle von KESY, die wir im Februar 2020 durchführten, haben wir erste Informationen zur geplanten Weiterentwicklung des Systems erhalten, die mit einer umfassenden Neukonzeption des technischen Verfahrens verbunden war. Nachdem ein hierzu geplanter Vor-Ort-Termin jedoch wegen der Pandemielage zunächst abgesagt werden musste, wurde uns das neue System schließlich im Mai 2020 von der Polizei Brandenburg vorgestellt.

Die Software befand sich ersichtlich noch in einem frühen Entwicklungsstadium, allerdings waren die geplanten Eigenschaften bereits erkennbar. Schon beim Anlegen eines neuen Vorgangs zur Kennzeichenerfassung im Fahndungs- oder Aufzeichnungsmodus müssen danach der Überwachungszeitraum, die einzubeziehenden Kamerastandorte und die jeweils zugriffsberechtigten Benutzerinnen und Benutzer festgelegt werden. Nach Ablauf des Zeitraums wird der Aufzeichnungsmodus automatisch deaktiviert und der Export der gesammelten Daten zur ermittlungsführenden Staatsanwaltschaft veranlasst, während die entsprechenden Fahrzeugdaten bei der Polizei gelöscht werden. Dadurch wird verhindert, dass es zu einer langfristigen Anhäufung personenbezogener Kennzeichendaten kommt.

Einzelne Kameras sollen für ein Ermittlungsverfahren zu- oder abgeschaltet werden können. Auch eine Zähl-funktion ist vorgesehen. Zudem wird es ein differenzierteres Rollen- und Rechtemanagement geben, um jene von uns kritisierten Mängel zu beheben. Zeitlich

sollen Zugriffe dadurch nur noch für die im Beschluss aufgeführten Laufzeiten möglich sein – allerdings war diese Funktion bei dem Vor-Ort-Termin noch nicht korrekt implementiert.

Zum Zeitpunkt der Präsentation der Software war auch noch ungeklärt, wie eine verfahrensübergreifende Nutzung von Daten realisiert wird. Viele der geplanten Funktionen waren noch nicht vollständig vorhanden. Ebenso fehlte eine Transportverschlüsselung mit Transport Layer Security (TLS), die wir als erforderlich ansehen, auch wenn keine Datenübermittlung über das offene Internet, sondern nur über Polizeinetze stattfindet.

Anfang Oktober 2020 gab es weitere Informationen zu KESY: Demnach sei die fertiggestellte Software inzwischen von der Entwicklerfirma übergeben worden und enthalte alle beauftragten Neuerungen. Dazu gehöre, dass die im Aufzeichnungsmodus erhobenen Daten nun mit Attributen versehen würden, sodass sie einem Ermittlungsverfahren bzw. Observationsbeschluss zugeordnet werden könnten. Die Nutzungsberechtigungen würden für ein konkretes Verfahren erteilt und ermöglichten ausschließlich den Zugriff auf die mit den entsprechenden Attributen versehenen Daten. Nach Ablauf des Beschlusszeitraums würde die Nutzungsberechtigung automatisch entzogen. Die Daten würden in dem von der Staatsanwaltschaft verfügten Umfang exportiert und an die zuständige Ermittlungsbehörde übergeben. Anschließend würden die zugehörigen Attribute gelöscht. Seien mit Daten eines Zeitraums keine Attribute mehr verknüpft, würden diese automatisch und unwiderruflich gelöscht. Die Verlängerung eines Beschlusses führe nicht zu einer längeren Speicherdauer der zuvor erhobenen Daten. Die Übernahme von Daten in andere Verfahren sei möglich. Die Produktivsetzung solle demnächst erfolgen.

Damit werden in dem neuen KESY-Verfahren wesentliche Forderungen hinsichtlich der Datentrennung und Datenlöschung sowie differenzierter Zugriffsrechte umgesetzt. Eine aktuelle Information darüber, ob die neue Software inzwischen produktiv gesetzt wurde, steht allerdings noch aus. Auch konnten wir bislang nicht überprüfen, ob das finale Produkt tatsächlich alle erforderlichen und geplan-

ten Funktionen enthält, da die Pandemielage Untersuchungen vor Ort weiterhin erschwert.

Bei erheblichen Veränderungen von automatisierten Verfahren wie vorliegend – insbesondere in einem datenschutzrechtlich sensiblen Bereich wie der polizeilichen Datenverarbeitung – sind darüber hinaus eine ganze Reihe an umfangreichen Dokumenten zu erstellen. Dazu gehören ein Sicherheitskonzept und eine Datenschutz-Folgenabschätzung. Letztere wurde uns zwar bereits in einer Entwurfsfassung übergeben, wir mussten der Polizei jedoch mitteilen, dass wir einen erheblichen Änderungsbedarf sehen. Eine überarbeitete Fassung haben wir bislang nicht erhalten. Das Sicherheitskonzept liegt uns ebenfalls noch nicht vor.

Im Ergebnis ist festzustellen, dass sich das System zur Kennzeichenerfassung in Brandenburg grundsätzlich positiv entwickelt und die Polizei erhebliche Anstrengungen unternimmt, um allen datenschutzrechtlichen Anforderungen gerecht zu werden. Wir werden ihr bei der Neuausrichtung von KESY weiterhin beratend und kontrollierend zur Seite stehen.

2.3 Auswirkungen auf das Handeln der Staatsanwaltschaften

In der Regel ordnen – nach Vorliegen eines richterlichen Beschlusses zur längerfristigen Observation – die Staatsanwaltschaften als ermittlungsleitende Stellen die Nutzung besonderer „für Observationszwecke bestimmter technischer Mittel“ gemäß § 100h Absatz 1 Satz 1 Nummer 2 Strafprozessordnung (StPO) an. Sie sind bis zur Anhängigkeit der Sache bei Gericht grundsätzlich auch für die Entscheidung über die Löschung von Daten zuständig. In der Vergangenheit wurde in den Anordnungen das einzusetzende Mittel überwiegend nicht festgelegt, nur gelegentlich das Verfahren KESY benannt, wobei Standorte und die Anzahl der in Brandenburg aufgestellten stationären Kameras offen blieben und die Anordnungsdauer von drei Monaten gewählt wurde. Auch die Verfahrensführung durch die Staatsanwaltschaften muss deshalb dahingehend angepasst werden, dass bis zu einer abschließenden Neubewertung der Rechtsgrundlage für automatisierte Kennzeichenlesesysteme eine fortgesetzte Ak-

kumulation von Daten Unbeteiligter verhindert und erhobene, nicht mehr erforderliche Daten unverzüglich gelöscht werden.

Aufgrund unserer auf die brandenburgischen Staatsanwaltschaften beschränkten Zuständigkeit haben wir das Gespräch mit der Generalstaatsanwaltschaft in Brandenburg gesucht. Gleichwohl sehen wir auch eine Verantwortung der zahlenmäßig überwiegenden Staatsanwaltschaften anderer Bundesländer, ihre Anordnungspraxis bei Amtshilfeersuchen an die geänderten Bedingungen bei den brandenburgischen Polizeibehörden anzupassen. Die Generalstaatsanwaltschaft zeigte sich unseren datenschutzrechtlichen Bedenken zwar durchaus aufgeschlossen, verteidigte jedoch die mehrmonatigen Speicherfristen. Sie wies darauf hin, dass sich im Bereich der organisierten Kriminalität bzw. Bandenkriminalität das Zusammenwirken einer Tätergruppe häufig erst mit fortlaufender Beobachtung verdichte. Vielfach seien zu Beginn der Ermittlungen nur eine Beschuldigte bzw. ein Beschuldigter und das Kennzeichen eines Tatfahrzeuges bekannt. Die Erkenntnis, dass eine Täterin oder ein Täter mehrfach beteiligt ist bzw. Fahrzeugwechsel vornimmt, dass weitere Personen mitwirken oder ein bestimmtes Muster in der Vorgehensweise besteht, ergebe sich erst in der Rückschau nach mehreren Wochen oder Monaten der Beobachtung. Für diese Fälle müssten Aufzeichnungen aus der Vergangenheit vorliegen, sodass die Fahrtroute eines erst später bekannt gewordenen Fahrzeugs rückwirkend überprüft werden kann.

Diese Argumentation ist aus Ermittlersicht nachvollziehbar, verkennt jedoch, dass das Bundesverfassungsgericht für die präventivpolizeiliche Nutzung von automatisierten Kennzeichenlesesystemen in jüngerer Zeit deutliche Beschränkungen zum Schutz der Rechte der Personen, die durch die Maßnahme betroffen sind, verhängt hat[25]. Jede automatisierte Kennzeichenkontrolle greift bereits bei der Erfassung eines Kennzeichens durch die Speicherung und den Datenabgleich in das Recht auf informationelle Selbstbestimmung aller davon betroffenen Personen ein. Überwiegend sind unter den massenhaft über Monate gespeicherten Fahrzeugkennzeichen weder Fahrzeuge von Beschuldigten noch von Kontaktpersonen von

25 Beschlüsse des Bundesverfassungsgerichts vom 18. Dezember 2018, 1 BvR 142/15, 1 BvR 2795/09, 1 BvR 3187/10.

Beschuldigten. Die Erfassung und Speicherung dieser Kennzeichen erfolgt, ohne dass ein auf tatsächliche Ermittlungserkenntnisse gestützter Anfangsverdacht besteht.

Wir halten deshalb die bisher herangezogene Ermächtigungsgrundlage für den Einsatz von KESY in Strafverfahren für nicht hinreichend bestimmt, um diesem Umstand gerecht zu werden. Auch können Vorgaben der Benachrichtigung erheblich mitbetroffener Personen und einer unverzüglichen Löschung der Daten nach dem in der Vergangenheit praktizierten Verfahren nicht umgesetzt werden. Die gegenwärtig noch nicht abgeschlossene Arbeit des Bundesgesetzgebers, eine tragfähige Rechtsgrundlage für die automatisierte Kennzeichenlesesysteme zu finden, entbindet die Staatsanwaltschaften nicht, für die laufenden Ermittlungsverfahren eine möglichst zielgerichtete Erfassung und frühzeitige Löschung nicht relevanter Kennzeichendaten vorzunehmen.

Die von der Generalstaatsanwältin in Brandenburg mittels Verfügung bereits im Jahr 2019 getroffenen Vorkehrungen, die bis zu einer Neuregelung der Rechtsgrundlage gelten, umfassen folgende Regelungen:

- Die Anordnung zur Nutzung des Verfahrens KESY im Aufzeichnungsmodus muss ausdrücklich erfolgen.

- Im jeweiligen Einzelfall ist von der Staatsanwaltschaft stets zu prüfen, ob eine räumliche und zeitliche Präzisierung der Aufzeichnung von Kennzeichen, d. h. eine Beschränkung der Beobachtung auf bestimmte Zielstrecken und zeitliche Befristung der Maßnahme infrage kommt. Dadurch sollen so weit wie möglich und vorhersehbar nicht tatrelevante Datenerhebungen ausgeschlossen werden. Dies beinhaltet auch, dass Staatsanwaltschaften anderer Bundesländer ohne Ortskenntnis in die Lage versetzt werden, sich über die Standorte der KESY-Anlagen zu informieren.

- Spätestens bei jedem Antrag auf Verlängerung der Maßnahme ist zu prüfen, ob eine weitere Aufzeichnung erforderlich ist und ob gespeicherte Daten gelöscht werden können.

- Die Löschung nicht tatrelevanter Daten ist grundsätzlich spätestens mit Abschluss der Ermittlungen anzuordnen.

Wir begrüßen diese Klarstellungen, weil insbesondere der Zeitpunkt der Löschung nicht benötigter Daten damit entsprechend den Vorgaben des § 101 Absatz 8 StPO vor den endgültigen Abschluss des Strafverfahrens verlagert wird. Wir halten jedoch daran fest, dass brandenburgische Staatsanwaltschaften verpflichtet werden sollten, in kürzeren Zeitabschnitten (etwa wochenweise) die gespeicherten Kennzeichendaten auf ihre Relevanz für das Strafverfahren zu überprüfen. Eine Entscheidung über die Löschung sollte zum frühestmöglichen Zeitpunkt, unabhängig von Anordnungsverlängerungen oder einer prozessualen Zäsur (Ermittlungsabschluss) erfolgen.

Schwieriger gestaltet sich eine Lösung für die Ermittlungsverfahren, in denen längerfristige Observationen unter Einsatz von KESY von Staatsanwaltschaften anderer Bundesländer angeordnet werden. Allein im Zeitraum von Juni 2019 bis März 2020 machten diese fast 60 % der Anordnungen aus, die von der Polizei Brandenburg umgesetzt wurden. Die tatsächliche polizeiliche Praxis, die entsprechend der Anordnungsdauer gespeicherten Daten ausschließlich zu „verwahren", lässt eine schnellere Löschroutine derzeit nicht zu. Wir fordern, dass diese Daten spätestens nach drei Monaten an die jeweiligen Staatsanwaltschaften zur weiteren Bearbeitung zu übergeben sind.

3 Datenschutz-Folgenabschätzung im Polizeibereich

Mit dem Wirksamwerden der neuen europäischen Datenschutzvorschriften im Rahmen der EU-Richtlinie 2016/680 (sogenannte JI-Richtlinie) im Jahr 2018 und deren Umsetzung durch das Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) wurde erstmals eine Verpflichtung zur Durchführung von Datenschutz-Folgenabschätzungen für die zuständigen Behörden eingeführt. Sie findet sich in § 21 BbgPJMDSG und ersetzt die zuvor im Brandenburgischen Datenschutzgesetz enthaltene Regelung zu einer Vorabkontrolle.

Eine Datenschutz-Folgenabschätzung ist vom Verantwortlichen für vorgesehene Datenverarbeitungsvorgänge immer dann durchzuführen, wenn die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, voraussichtlich ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge hat. Im Rahmen einer Datenschutz-Folgenabschätzung sollen die Auswirkungen für betroffene Personen identifiziert und hinsichtlich möglicher Schäden bewertet werden. Drohen durch die Verarbeitung schwerwiegende Schäden für den Datenschutz der Betroffenen, sind geeignete technische und organisatorische Maßnahmen zu ermitteln und umzusetzen, die die Auswirkungen abmildern.

Diese abstrakten Formulierungen müssen für konkrete Datenverarbeitungsvorgänge vom Verantwortlichen jeweils mit Leben gefüllt werden. Das bedeutet insbesondere, dass zunächst für beabsichtigte Datenverarbeitungen eine Untersuchung darüber durchzuführen und schriftlich zu dokumentieren ist, ob durch sie ein hohes Risiko für die Rechte und Freiheiten Betroffener entstehen kann (Schwellwertanalyse). Wir gehen gegenwärtig davon aus, dass der Schwellwert bei den meisten polizeilichen Datenverarbeitungsverfahren überschritten sein wird und damit die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung besteht, da allein der polizeiliche Kontext einer Datenverarbeitung bereits ein hohes Risiko bedeuten kann.

Nach der Schwellwertanalyse erfolgt die eigentliche Datenschutz-Folgenabschätzung. Deren Inhalte sind gesetzlich festgelegt. So müssen die Verarbeitungszwecke und die Verarbeitungsvorgänge einschließlich der jeweils verarbeiteten Datenkategorien beschrieben sowie die Erforderlichkeit und die Angemessenheit der Verarbeitung begründet werden. Weiterhin muss der Verantwortliche die Risiken für die Rechtsgüter der betroffenen Personen und deren schutzwürdige Interessen identifizieren und bewerten. Hierbei sind systematisch mögliche Schadensszenarien zu betrachten und deren Eintrittswahrscheinlichkeiten sowie Schadenshöhen zu bestimmen. Anschließend ist darzulegen, mit welchen technischen und organisatorischen Maßnahmen die ermittelten Risiken abgewendet oder ver-

ringert werden können. Die Ergebnisse der Datenschutz-Folgenabschätzung sind in einem Bericht nachvollziehbar zu dokumentieren.

Diese Anforderungen lassen bereits erahnen, wie umfangreich und komplex eine Datenschutz-Folgenabschätzung ist. Im Zentrum steht dabei die Bedrohungs- und Risikoanalyse, die nicht schematisch mittels Checklisten oder ähnlichen Hilfsmitteln abgearbeitet werden kann, sondern für jedes Verfahren individuell und angepasst durchgeführt werden muss. Im Unterschied zu einer Risikoanalyse, wie sie üblicherweise im Bereich der Informationssicherheit durchgeführt wird, ist hierbei konsequent die Perspektive der Betroffenen einzunehmen. Es geht also nicht darum, die durch die Datenverarbeitung entstehenden Risiken für die verantwortliche Institution zu ermitteln und abzumildern, sondern die von der polizeilichen Verarbeitung betroffenen Personen in ihren Rechten und Freiheiten zu schützen.

Bei hohem Risiko Vorsorge treffen.

Zu beachten ist auch, dass eine Datenschutz-Folgenabschätzung nicht durch die von der Behörde benannten Datenschutzbeauftragten vorzunehmen ist. Diese sind zwar gemäß § 21 Absatz 3 BbgPJMDSG zu beteiligen, die Durchführung obliegt aber dem Verantwortlichen selbst.

Bei der Polizei Brandenburg bestand ein erheblicher Beratungsbedarf dahingehend, wie bei konkreten Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen ist. Wir haben daher einige Materialien erarbeitet, in denen wir deren Struktur und methodische Durchführung beschreiben. Darüber hinaus haben wir die Datenschutzbeauftragte der Polizei Brandenburg bei der Erstellung von Formularen unterstützt sowie Vorgehensweise und Zielrichtung von Datenschutz-Folgenabschätzungen erläutert. Anhand eines ausgewählten Verfahrens haben wir in einem gemeinsamen Arbeitstreffen zusammen mit einem Vertreter des Verfahrensverantwortlichen und der Datenschutzbeauftragten die Vorgehensweise der Datenschutz-Folgenabschätzung erklärt und eine beispielhafte Risikoanalyse durchgeführt.

Durch die uns bisher vorgelegten Entwürfe für Datenschutz-Folgenabschätzungen bei polizeilichen Datenverarbeitungen wurde jedoch auch deutlich, dass nach wie vor ein erheblicher Beratungs- und Verbesserungsbedarf in diesem Bereich besteht. Die vollständige Erfüllung der gesetzlichen Anforderungen zur Durchführung einer Datenschutz-Folgenabschätzung ist eine anspruchsvolle, komplexe Aufgabe und bedarf noch erheblicher Anstrengungen. Wir würden es in diesem Zusammenhang begrüßen, wenn die Datenschutzbeauftragte der Polizei Brandenburg als Multiplikatorin wirken könnte, um anhand der von uns zur Verfügung gestellten bzw. gemeinsam erarbeiteten Materialien und methodischen Handreichungen eine nachhaltige Qualitätsverbesserung bei den anstehenden Datenschutz-Folgenabschätzungen zu erreichen. Selbstverständlich stehen wir dabei gern weiterhin beratend und unterstützend zur Verfügung.

4 Zahlen und Fakten

Der Berichtszeitraum war im Vergleich zum Vorjahr durch deutlich weniger neue Beschwerden betroffener Personen gegen Datenverarbeitungsvorgänge bei der Polizei Brandenburg geprägt. Insgesamt erreichten uns 18 Beschwerden, davon waren 13 gegen Polizeibehörden gerichtet und fünf Eingaben bezogen sich schwerpunktmäßig oder ausschließlich auf staatsanwaltliches Handeln. Die Eingaben im Polizeibereich betrafen unterschiedlichste Sachverhalte, wie etwa nicht oder nicht ausreichend erteilte Auskünfte zu gespeicherten personenbezogen Daten, zweckfremde Verwendung von rechtmäßig erhobenen Daten, zu lange Speicherfristen und Berechtigung oder Umfang polizeilicher Auskunftsersuchen an andere Behörden.

Zugleich wurden wie im Vorjahr zeitintensive Beratungen mit den Polizeibehörden durchgeführt. Hier sind drei wesentliche Schwerpunkte zu nennen: die Begleitung des weiterentwickelten Kennzeichenerfassungssystem KESY, das einheitliche Fallbearbeitungssystem der Polizei und Hinweise zur Erstellung von Datenschutzfolgenabschätzungen. Vor-Ort-Besuche und -Gespräche konnten bedingt durch die gebotene Kontaktvermeidung während der Corona-Pandemie nur sehr eingeschränkt durchgeführt werden.

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

Teil C: Die Dienststelle

1 Öffentlichkeitsarbeit

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder führte am 28. Januar 2020 wieder eine zentrale Veranstaltung anlässlich des Europäischen Datenschutztages in Berlin durch. Der Konferenzvorsitzende des Vorjahres – Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz – lud hochqualifizierte Referentinnen und Referenten aus Recht, Politik und Wissenschaft zum Thema „Künstliche Intelligenz – zwischen Förderung und Bändigung“ ein. Ebenso wie die übrigen Konferenzmitglieder beteiligte sich auch die Landesbeauftragte an der Ausrichtung der Veranstaltung.

Die im Berichtszeitraum allgegenwärtige Pandemie führte bereits im Frühjahr zu einem erhöhten Informationsbedarf vonseiten der Verantwortlichen sowie der Bürgerinnen und Bürger. Die Landesbeauftragte stellte in ihrem Internetangebot Handreichungen zur Verfügung, die sie im Laufe des Jahres ergänzt oder aktualisiert hat. Frühzeitig boten wir Hinweise für Schulen und Lehrkräfte zur datenschutzgerechten Gestaltung des selbstständigen Lernens während der Corona-Pandemie an. Im Zuge der Verpflichtung insbesondere der Gastronomie zur Erhebung von Kontaktdaten der Gäste haben wir häufig gestellte Fragen zu datenschutzrelevanten Gesichtspunkten für Gäste, Gastronominnen und Gastronomen sowie andere Verpflichtete beantwortet. Außerdem entwickelte die Landesbeauftragte ein später mehrfach aktualisiertes Musterformular zur Erhebung der Kontaktdaten von Gästen. Unsere ersten Hinweise zu technischen und organisatorischen Maßnahmen für die Umsetzung des Datenschutzes bei der Heimarbeit haben wir um die im Laufe der Pandemie gewonnenen Erfahrungen ergänzt und aktualisiert. Darüber hinaus nutzten wir im Rahmen unserer Öffentlichkeitsarbeit in punkto Datenschutz und Pandemie auch Empfehlungen der Datenschutzkonferenz sowie des Europäischen Datenschutzausschusses. Sämtliche Informationen waren als Schwerpunkt gebündelt auf unserer Website abrufbar.

Die zwischenzeitlich vergriffene Druckbroschüre der Datenschutz-Grundverordnung haben wir im Berichtszeitraum unverändert nach-

drucken lassen und das Bundesdatenschutzgesetz nach einer Gesetzesänderung als Broschüre neu aufgelegt.

Gemeinsam mit den übrigen unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat die Landesbeauftragte erneut mehrere Orientierungshilfen für die Praxis des Datenschutzes veröffentlicht. Im Berichtszeitraum waren darunter das Standard-Datenschutzmodell, die Orientierungshilfe mit Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail und die Orientierungshilfen zur Videoüberwachung durch nicht öffentliche Stellen sowie zu Videokonferenzsystemen.

Auch hat die Landesbeauftragte wieder die vom Europäischen Datenschutzausschuss herausgegebenen Leitlinien in ihrem Internetangebot veröffentlicht. Dabei handelt es sich um die Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, die Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch, die Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 sowie die Leitlinien 05/2020 für die Einwilligung nach der Verordnung 2016/679. Bezüglich des Urteils des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II“) vom 16. Juli 2020 haben wir zudem die deutschsprachige Übersetzung der Antworten auf häufig gestellte Fragen vom Europäischen Datenschutzausschuss übernommen.

Das Internetangebot der Landesbeauftragten war zuletzt im Jahr 2012 neu gestaltet worden. Der Zentrale IT-Dienstleister des Landes Brandenburg, der mit dem Webhosting beauftragt ist, hat in der Zwischenzeit ein neues Redaktionssystem eingeführt. Er reagierte damit auf die veränderten Anforderungen an einen zeitgemäßen Webauftritt. Unter anderem ermöglicht das neue System eine Nutzung auf mobilen Endgeräten sowie einen barrierearmen Zugang zu der Website. Die obligatorische Umstellung auf das neue Redaktionssystem hat die Landesbeauftragte genutzt, um ihr Internetangebot vollständig zu erneuern. Von nicht mehr aktuellen Informationen haben wir uns getrennt und das neue, zeitgemäße Layout eingesetzt,

um die Seite übersichtlicher zu strukturieren. Außerdem haben wir das Beschwerdeformular unter Berücksichtigung der Erfahrung seiner Nutzung in den beiden letzten Jahren umfassend überarbeitet. Zusätzlich bieten wir Verantwortlichen jetzt auch ein Formular zur Meldung von Datenschutzverletzungen an. Nach einer intensiven Vorarbeit konnte das neue Internetangebot zum Jahresende freigeschaltet werden. Es ist weiterhin unter www.LDA.Brandenburg.de erreichbar.

2 Pressearbeit

Die Pressearbeit im ersten Quartal des Jahres 2020 konzentrierte sich auf den Streit um die Zulässigkeit der automatischen Kennzeichenerfassung auf brandenburgischen Autobahnen durch die Polizei. Hierzu veröffentlichte die Landesbeauftragte zwei Presseinformationen. Gleich zu Jahresbeginn informierte sie die Medien über ihre Beanstandung gegenüber dem Polizeipräsidium Brandenburg. Sie erläuterte, weshalb sie die Kennzeichenerfassung sowie die fortgesetzte Speicherung der ohne Anlass erhobenen Daten für einen unrechtmäßigen Eingriff in das Recht auf informationelle Selbstbestimmung hielt. Im Februar gab sie eine Presseinformation heraus, um darauf aufmerksam zu machen, dass die Polizei das Verfahren erstens nahezu unverändert weiterbetrieb und zweitens die unrechtmäßigen Datensätze bisher nicht gelöscht hatte.

Ende März veröffentlichte die Landesbeauftragte ihren Tätigkeitsbericht Datenschutz 2019. Brandenburg hatte zu dieser Zeit bereits strikte Kontaktbeschränkungen wegen der Corona-Pandemie beschlossen; auf eine Pressekonferenz wurde deshalb verzichtet. Stattdessen stellten wir die Schwerpunkte des Berichts in einer längeren Aussendung dar. Im Mai nahm die Landesbeauftragte den zweiten Jahrestag der Einführung der Datenschutz-Grundverordnung zum Anlass, um Forderungen nach einer Zurückdrängung des Datenschutzes, die unter dem Eindruck der Pandemie vielfach erhoben worden waren, entgegenzutreten. Sie stellte klar, dass der inzwischen nicht mehr ganz so neue Rechtsrahmen auch für den Alltag in Verwaltungen und Unternehmen gute Gestaltungsmöglichkeiten bietet. Die Umsetzung der Verpflichtung von Cafés und Restaurants zur Erfassung von Gästedaten durch die SARS-CoV2-Umgangs-

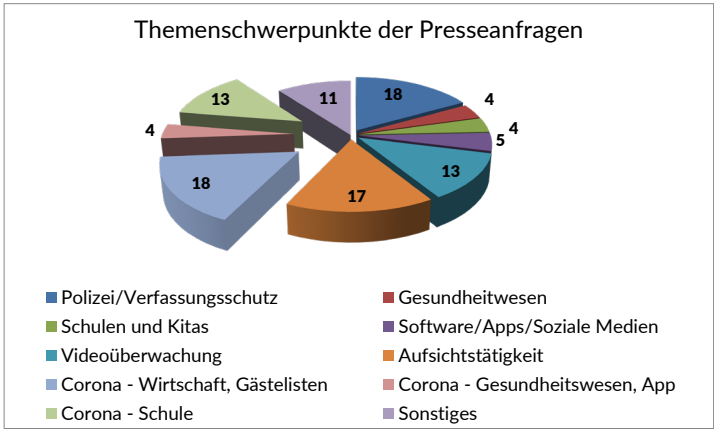
verordnung war Gegenstand einer landesweiten Überprüfung der Landesbeauftragten. Im August informierten wir über das – wenig zufriedenstellende – Ergebnis. Wir wiesen in der Presseinformation insbesondere auf unsere Beratungen der Gastwirtinnen und Gastwirte sowie auf unsere Musterformulare und FAQs zur Erhebung von Kontaktdaten hin.

Im August nahm die Landesbeauftragte an einer gemeinsamen Bundespressekonferenz zur bevorstehenden Einführung der elektronischen Patientenakte mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie mit einer weiteren Kollegin und einem Kollegen aus den Ländern teil. Sie machte in einer begleitenden Presseinformation darauf aufmerksam, dass das hierfür im Eilverfahren auf den Weg gebrachte Patientendaten-Schutz-Gesetz den Datenschutz insbesondere in der ersten Umsetzungsphase nur unzureichend berücksichtigt. Damit werden die Rechte der Versicherten ohne Not und unter Verstoß gegen europäisches Datenschutzrecht beschnitten. Wir forderten die Landesregierung auf, im Bundesrat auf Verbesserungen des Gesetzes zu dringen.

Im Oktober fanden in Potsdam – pandemiebedingt reduzierte, dafür aber zeitlich und räumlich ausgedehnte – Feierlichkeiten zum 30. Jahrestag der Deutschen Einheit statt. Die Staatskanzlei des Landes Brandenburg ließ vom 5. September bis zum 4. Oktober 2020 mehrere Standorte dieser EinheitsEXPO 2020 in der Landeshauptstadt mit Kameras überwachen. Nach einer eingehenden Prüfung stellte die Landesdatenschutzbeauftragte fest, dass die damit verbundene Datenverarbeitung größtenteils unzulässig war. Sie informierte die Medien im November über eine förmliche Verwarnung, die sie im Ergebnis gegenüber der Staatskanzlei ausgesprochen hat.

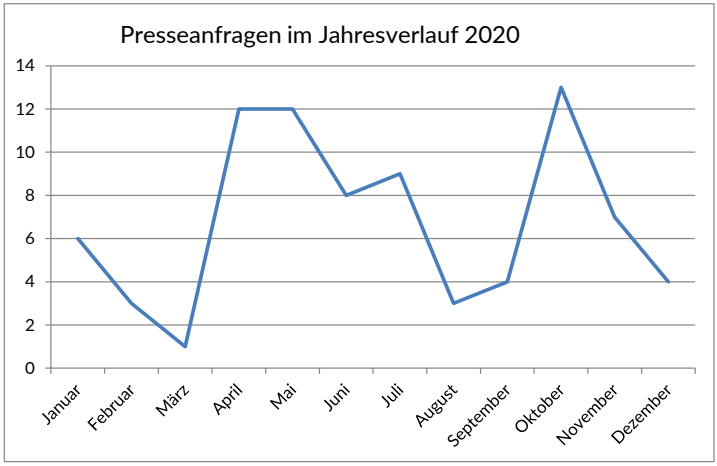
Nachdem die Landesbeauftragte im Vorjahr 84 datenschutzbezogene Presseanfragen zu beantworten hatte, stieg deren Anzahl im Berichtszeitraum auf 107. Wir hatten bereits im letzten Tätigkeitsbericht festgestellt, dass sich das Interesse der Medien am Datenschutz nach Einführung der Datenschutz-Grundverordnung auf hohem Niveau eingependelt hatte. Nunmehr ist es sogar noch angewachsen. Ein Drittel der Anfragen bezog sich auf pandemiebedingte Themen. Hier standen das schulische Distanzlernen, die Wohnraumarbeit so-

wie der Umgang von Unternehmen bzw. Gastwirtinnen und Gastwirten, aber auch der Gesundheitsverwaltung mit personenbezogenen Daten im Vordergrund. Die bereits erwähnte automatische Kennzeichenfahndung der Polizei Brandenburg war Anlass für etwa ein Sechstel der Anfragen – diese erreichten uns vor allem in den ersten Wochen des Jahres. In der gleichen Größenordnung beantworteten wir Fragen zu unserer Aufsichtstätigkeit. Das bezog sich im Wesentlichen auf verhängte Bußgelder, Datenschutzverletzungen, die uns nach Artikel 33 Datenschutz-Grundverordnung zu melden sind, oder auf Sanktionsbefugnisse der Landesbeauftragten. Ein gutes Zehntel der Medienanfragen betraf Videoüberwachungen aller Art.



Betrachtet man die Presseanfragen im Jahresverlauf, überrascht deren geringe Zahl im März nicht. Die Pandemie und der erste Lockdown hatten das Land auch medial fest im Griff. Rasch stellten sich jedoch Fragen zum Umgang mit dem Datenschutz auf der Arbeit, in der Schule oder zu Hause. Plötzlich war die Datenschutzaufsichtsbehörde wieder gefragt. Nach einer Pause im Spätsommer kam dann ein gewohnt bunter Strauß an Themen zur Sprache – vom Dauerbrenner Videoüberwachung über Fragen zu Bußgeldverfahren bis hin zum Datenschutz bei Auskunfteien. Erst im Dezember – parallel zu den verschärften Eindämmungsmaßnahmen gegen die Ausbreitung des SARS-CoV-2 – verengte sich das Spektrum wieder auf coronarelevante Themen.

Wir haben in diesem Jahr ausgewertet, um welche Daten verarbeitenden Stellen es bei den Medienanfragen geht. In über der Hälfte der Fälle standen öffentliche Stellen, also Verwaltungen – einschließlich Schulen – im Fokus des Interesses. Ein Drittel der Anfragen bezog sich auf Verantwortliche aus der Wirtschaft.



Während, wie bereits im Vorjahr, knapp die Hälfte der Journalistinnen und Journalisten aus dem Printbereich stammte, also für Tages- und Wochenzeitungen bzw. für Nachrichtenmagazine recherchierte, war das Interesse des Fernsehens von einem Zehntel im Jahr 2019 auf ein Viertel im Berichtszeitraum gestiegen. Knapp zwei Drittel der Anfragen entstammte regionalen Medien aus Brandenburg oder, in weit geringerem Umfang, aus Berlin. Überregional berichtete ein knappes Drittel; fünf Prozent der anfragenden Pressekontakte reichte über die Bundesgrenzen hinaus.

3 Personal und Organisation der Dienststelle

Im Berichtszeitraum gelang es, alle freien Stellen im Bereich Technik und Organisation mit engagierten neuen Mitarbeitern zu besetzen. Daneben waren auch der Wechsel einiger Mitarbeiterinnen des Bereichs Recht zu anderen Dienststellen im Land Brandenburg bzw. zu anderen Arbeitgeberinnen und Arbeitgebern sowie ein Eintritt in

den Ruhestand auszugleichen. Insgesamt konnte ich im Jahr 2020 sieben Stellenbesetzungsverfahren erfolgreich durchführen.

Für das Haushaltsjahr 2021 hat der Landtag Brandenburg meiner Behörde zwei neue Stellen für den juristischen Bereich bewilligt – eine davon steht für Aufgaben des Datenschutzes, die andere für das Themengebiet Akteneinsicht zur Verfügung. Hierfür bin ich sehr dankbar. Allerdings handelt es sich dabei nur um einen Tropfen auf den heißen Stein; die Arbeitsüberlastung meiner Mitarbeiterinnen und Mitarbeiter kann damit nur zu einem kleinen Teil aufgefangen werden. So steht der Personalzuwachs weiterhin außer Verhältnis zu dem viel stärker gestiegenen Beratungsbedarf insbesondere öffentlicher Stellen. Digitalisierungsprojekte haben hier rasant an Fahrt aufgenommen – die Verantwortlichen erwarten zu Recht die Unterstützung durch meine Fachleute. Neben den vielen zusätzlichen, pandemiebedingten Vorhaben begleitet meine Dienststelle auch langfristige E-Government-Projekte. Der brandenburgische Vorsitz im Arbeitskreis Verwaltung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder bindet darüber hinaus personelle Kapazitäten. Diese Tätigkeit zieht zudem die Mitarbeit in weiteren Arbeitsgremien beispielsweise zur Umsetzung des Onlinezugangsgesetzes sowie zur Registermodernisierung nach sich.

Der langfristige und intensive Personaleinsatz im Rahmen der Begleitung von Gesetzesvorhaben und Digitalisierungsprojekten führt insbesondere zu fehlenden Kapazitäten für die Bearbeitung von Beschwerden und Anfragen der Bürgerinnen und Bürger. Sie müssen immer länger auf eine Antwort bzw. auf die Bearbeitung ihrer Fälle warten. Da hier regelmäßig konkrete Datenschutzverstöße – also Grundrechtseingriffe – im Raum stehen, empfinden alle Beteiligten solche Verzögerungen als inakzeptabel.

Die stark begrenzten räumlichen Kapazitäten sowie die fehlende Barrierefreiheit der jetzigen Unterbringung meiner Dienststelle führten dazu, dass der Brandenburgische Landesbetrieb für Liegenschaften und Bauen mir im Berichtszeitraum verschiedene Möglichkeiten für einen Umzug in die Landeshauptstadt Potsdam oder deren unmittelbare Nähe vorschlug. Nach detaillierter Prüfung und Kontakt mit den jeweiligen Vermietern stellte sich heraus, dass dieses Vorha-

ben aus Kostengründen gegenwärtig nicht realisierbar ist. Insofern hoffe ich, auf der von meiner Behörde bereits seit ihrer Gründung genutzten Liegenschaft in Kleinmachnow zusätzliche und barrierefrei zugängliche Büroräume anmieten zu können.

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