Auszug

17. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz Für den Zeitraum vom 1. Januar 2020 bis 31. Dezember 2020

2 Der Landesbeauftragte

2.4 Besonderes elektronisches Behördenpostfach

In seinem XVI. Tätigkeitsbericht für das Jahr 2019 (Nr. 10.2) hat der Landesbeauftragte zum Sachstand der Einführung berichtet, dass er mit der Einrichtung des besonderen elektronischen Behördenpostfachs begonnen hatte.

Das besondere elektronische Behördenpostfach (beBPo) ist ein E-Mail-ähnlicher Dienst, insbesondere für Behörden, der eine OSCI-basierte Verschlüsselung verwendet und die Komplexität des verschlüsselten elektronischen Datenaustauschs vor den Nutzern weitgehend verbirgt. § 6 ERVV sieht das beBPo unter anderem als sicheren Übermittlungsweg für die elektronische Kommunikation mit den Gerichten vor. Analog dazu gibt es für Anwälte das besondere elektronische Anwaltspostfach (beA) und für Notare das besondere elektronische Notarpostfach (beN). Der Einsatz des beBPo beschränkt sich nicht nur auf die Kommunikation mit Gerichten; es kann auch durch Behörden für die Kommunikation untereinander verwendet werden. Bürger können u. U. als Nutzer der absenderbestätigten De-Mail an der sicheren Kommunikation teilnehmen.

Eine sichere elektronische Kommunikation ist nur mittels sicherer Verschlüsselung unter Verwendung erprobter und zuverlässiger Standards möglich. Deren Einrichtung und Nutzung ist allerdings technisch oft anspruchsvoll und für eine freiwillige Nutzung meist zu kostenintensiv. Um die Einführung sicherer elektronischer Kommunikation zu beschleunigen, ist die Nutzung durch gesetzliche Regelungen rechtlich verbindlich vorzuschreiben. Im Bereich der Justiz ist es zwischenzeitlich möglich, moderne Kommunikationstechnik anstelle von Telefax oder Brief zu nutzen. Datensammelnde Messenger und unsichere E-Mail-Lösungen wurden – aus datenschutzrechtlicher Sicht begrüßenswert – nicht zugelassen.

Die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV), aber auch die Verordnung über den elektronischen Rechtsverkehr bei den Gerichten und Staatsanwaltschaften des Landes Sachsen-Anhalt (ERVVO LSA) setzen auf sichere Verschlüsselung mittels OSCI, Prüfung und Bestätigung der Identität des Postfachinhabers sowie dessen Eintragung in ein sicheres elektronisches Verzeichnis. Das Verzeichnis digitaler Identitäten im elektronischen Rechtsverkehr – das Adressbuch – wird SAFE genannt. Für das beBPo kann der SAFE-konforme Verzeichnisdienst der Justiz genutzt werden. Um die rechtlichen Voraussetzungen dafür zu schaffen, mussten verschiedene Gesetze[4] um entsprechende Regelungen zum Umgang mit elektronischen Dokumenten erweitert werden.

Technische Grundlage des beBPo ist die Infrastruktur des Elektronischen Gerichts-und Verwaltungspostfachs (EGVP). Diese hat sich seit 2004 im Rahmen des Elektronischen Rechtsverkehrs bewährt. Ein beBPo und das EGVP sind grundsätzlich funktionsgleich. Die Justiz empfiehlt die Verwendung des beBPo, da es alle fachlichen Anforderungen abbildet und gleichzeitig durch die Identifikation und Herausgabe eigener Zertifikate auf die Anbringung von qualifizierten elektronischen Signaturen verzichtet werden kann. Das Postfach-Zertifikat dient der automatischen Verschlüsselung und das VHN-Zertifikat (vertrauenswürdiger Herkunftsnachweis) garantiert die Authentizität der Nachricht. Es ist keine zusätzliche elektronische Signatur notwendig.

Dies gilt allerdings dann nicht, wenn die Schriftform gesetzlich vorgeschrieben ist (§ 126 BGB). Hier ist zusätzlich eine qualifizierte elektronische Signatur zu verwenden (§ 126a BGB).

Alle Anwälte sowie Behörden und Körperschaften öffentlichen Rechts, an die Schriftstücke gegen Empfangsbekenntnis zugestellt werden können, sind gem. § 174 Abs. 3 ZPO verpflichtet, einen sicheren Übertragungsweg zu eröffnen.

§ 6 ERVV benennt nur „Behörden sowie juristische Personen des öffentlichen Rechts (Postfachinhaber)“ als EGVP/beBPo-Teilnehmer. Die ehemals mögliche Nutzung eines kostenfrei herunterladbaren EGVP-Clients durch Bürgerinnen und Bürger existiert nicht mehr, das zugehörige Downloadangebot fehlt zwischenzeitlich ebenso wie die Möglichkeit der Nutzung des Web-EGVP. Es wird auf „registrierte Drittprodukte“ und die absenderauthentifizierte De-Mail verwiesen. Zudem ist geplant, mit der Einführung eines „elektronischen Bürger- und Organisationen-Postfachs“ (eBO) zukünftig Bürgern und Unternehmen die Beteiligung am Elektronischen Rechtsverkehr über einen sicheren Übertragungsweg wieder zu ermöglichen.

Die Übermittlung von, mit einer qualifizierten elektronischen Signatur versehenen, elektronischen Dokumenten an das Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts über eine Anwendung, die auf OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht, dürfte der Standardfall sein. Es ist jedoch auch möglich, diese über einen „sicheren Übermittlungsweg“ zu versenden (§ 4 Abs. 1 Nr 1 ERVV). Ein solcher kann gem. § 130a Abs. 4 Nr. 1 ZPO auch der Postfach- und Versanddienst eines De-Mail-Kontos sein.

Der Landesbeauftragte verfügt über ein besonderes elektronisches Behördenpostfach, welches er sowohl in seiner Funktion als Landesbeauftragter für den Datenschutz, als auch für die ihm zur Wahrnehmung übertragenen Aufgaben des Landesbeauftragten für die Informationsfreiheit nutzt. Die Nutzung des für alle Teilnehmer bereitstehenden Adressbuchs ist nicht immer selbsterklärend, da jeder Adressat in seinen Möglichkeiten der Selbstbezeichnung frei ist. Eine Vereinheitlichung könnte die Nutzerfreundlichkeit erhöhen.

Der Landesbeauftragte plant darüber hinaus die Einrichtung eines De-Mail-Kontos zur Kommunikation mit Bürgerinnen und Bürgern nach Abschluss eines Rahmenvertrages mit einem Dienstleister durch das Ministerium der Finanzen. Ein solcher Vertrag war bis zum Ende des Berichtszeitraums nicht zustande gekommen.

6 Technik und Organisation

6.1 E-Government-Gesetz Sachsen-Anhalt

Wie bereits im XVI. Tätigkeitsbericht (Nr. 6.1) mitgeteilt, hat das Land mit dem 2019 in Kraft getretenen E-Government-Gesetz des Landes (EGovG LSA) den rechtlichen Rahmen für die weitere Entwicklung der elektronischen Verwaltung geschaffen und Regelungslücken des EGovG des Bundes geschlossen bzw. an die Besonderheiten des Landes angepasst. Verwaltungstätigkeiten, Fachverfahren und Querschnitts-dienste können auf dieser Grundlage elektronisch angeboten, bearbeitet bzw. abgewickelt werden.

Das vom Gesetz vorgegebene Kooperationsgremium zwischen kommunaler Verwaltung und Landesverwaltung wurde in Form des IT-Kooperationsrates eingerichtet. Der Landesbeauftragte ist beratendes Mitglied des IT-Kooperationsrates. Im Berichtszeitraum wurden durch den IT-Kooperationsrat vor allem die Umsetzung des Onlinezugangsgesetzes (OZG) im kommunalen Bereich sowie die künftige institutionelle Zusammenarbeit zwischen Land und Kommunen in diesem Zusammenhang thematisiert. Darüber hinaus wurden Fragen eines übergreifenden Informationssicherheitsmanagementsystems (ISMS) diskutiert und die Entwicklung der Glasfaseranbindung der Schulen des Landes erörtert.

Über die Notwendigkeit einer Fortschreibung der aktuellen E-Government-Strategie wurde noch keine abschließende Entscheidung getroffen, jedoch eine gebündelte und gut visualisierte Umsetzungsplanung aller, auch der bereits begonnenen, Projekte erbeten. Diese wird für das kommende Berichtsjahr erwartet.

6.2 Onlinezugangsgesetz und Portalverbund

In seinem XVI. Tätigkeitsbericht (Nr. 6.2) hatte der Landesbeauftragte berichtet, dass der Bundesgesetzgeber mit dem Onlinezugangsgesetz (OZG) die Rechtsgrundlagen dafür geschaffen hat, dass die Bürgerinnen und Bürger über einen Bund-Länder-Portalverbund bundesweit elektronische Verwaltungsleistungen bei der zuständigen Behörde beantragen können. Der Gesetzgeber hatte mit dem Erlass des OZG eine ganz bestimmte Fallkonstellation vor Augen:

Danach sollen die Bürgerinnen und Bürger ein Nutzerkonto beim Bund oder in einem Serviceportal eines Landes einrichten, mit dem sie sich über die in dem Nutzerkonto hinterlegten Identitätsdaten sicher authentifizieren können. Der Nutzer soll dann über den Portalverbund direkt zu der zuständigen Behörde geleitet werden, damit er bei ihr die von ihm begehrte Verwaltungsleistung beantragen kann. Er identifiziert sich und setzt mit seinem Antrag ein elektronisches Verwaltungsverfahren in Gang, das durch den Erlass eines elektronischen Verwaltungsaktes abgeschlossen wird. Das Nutzerkonto kann nämlich mit einem Postfach gekoppelt werden, sodass dem Nutzer auch elektronische Verwaltungsakte zugestellt werden können. Ein weiterer Clou besteht darin, dass nach dem „Once-Only-Prinzip“ in dem Nutzerkonto erforderliche Nachweise gespeichert werden können, die dann mit dem Einverständnis des Nutzers anderen Behörden in anderen Verwaltungsverfahren zur Verfügung gestellt werden können. Nachweise müssen also nicht ständig neu, sondern nur einmal („once-only“) erhoben werden.

Der IT-Planungsrat hat insgesamt 14 Themenfelder mit 575 Verwaltungsleistungen ermittelt, die nach dem OZG bis Ende 2022 digitalisiert sein sollen. Die Ministerpräsidentenkonferenz hat auf einer Tagung im Dezember 2019 vereinbart, dass ein Land ein Themenfeld übernimmt und für die dem Themenfeld zugeordneten Verwaltungsleistungen ein Online-Verfahren entwickelt. Dieses Verfahren soll dann von den anderen Ländern übernommen und implementiert werden können (Einer-für-alle-Prinzip). Sachsen-Anhalt betreut dabei das Themenfeld „Bildung“ (vgl. Nr. 6.2.1 „BAföG Digital“).

Das Ziel, bis Ende 2022 alle 575 Verwaltungsleistungen digitalisiert zu haben, erweist sich dabei als ehrgeizig. Bis Mitte 2021 waren erst 315 Verwaltungsleistungen verfügbar. Die Grundidee, dass der Antragsteller einen elektronischen Antrag stellt und daraufhin einen elektronischen Verwaltungsakt zugestellt bekommt, ist in der Praxis vielfach noch nicht umgesetzt. Bei BAföG Digital (vgl. Nr. 6.2.1) kommt der Bescheid z. B. derzeit noch per Post.

Unter datenschutzrechtlichen Gesichtspunkten ist zunächst darauf hinzuweisen, dass die Datenschutzaufsichtsbehörden des Bundes und der Länder keine Projektbeteiligten an den einzelnen Digitalisierungsvorhaben sind. Die Aufsichtsbehörden werden auch nicht als Genehmigungsbehörden tätig, die das Vorhaben für das jeweilige Land oder gar bundesweit per Verwaltungsakt datenschutzrechtlich genehmigen könnten. Es ist vielmehr Aufgabe des jeweiligen Landes bzw. des zuständigen Fachressorts, eigenverantwortlich die Vereinbarkeit des Vorhabens mit den einschlägigen daten-schutzrechtlichen Vorschriften zu prüfen. Die Datenschutzaufsichtsbehörden können dabei, wenn die Fachressorts die entsprechenden Vorarbeiten geleistet haben, beratend und unterstützend tätig werden.

Vor diesem Hintergrund hat die Konferenz der unabhängigen Datenschutzaufsichts-behörden des Bundes und der Länder (DSK) den Arbeitskreis (AK) Verwaltung beauftragt, eine Unterarbeitsgruppe (UAG) zur datenschutzrechtlichen Bewertung der OZG-Umsetzung von Portalen und auch Fachanwendungen einzurichten, die die möglichen Konstellationen von Betreibermodellen in Bezug auf deren datenschutzrechtliche Verantwortlichkeit und Umsetzung prüfen soll. Hierzu ist ein stetiger Austausch mit der Föderalen IT-Kooperation (FITKO) und dem Bundesministerium des Innern, für Bau und Heimat (BMI) vorgesehen.

Die vom AK Verwaltung eingesetzte „UAG Portallösungen“, an der auch Sachsen-Anhalt beteiligt ist, hat den Auftrag, zur Unterstützung und Beratung der öffentlichen Stellen des Bundes und der Länder ein Arbeitspapier zu entwickeln. Dieses war ursprünglich für das 1. Quartal 2021 vorgesehen. Trotz intensiver Beratungen und mehrfachen Sitzungen der UAG mit dem BMI lässt sich der von der DSK angedachte Zeitplan nicht mehr einhalten. Das beruht im Wesentlichen darauf, dass die Länder bei der Digitalisierung von Verwaltungsleistungen von dem Grundgedanken des OZG, dass die Bürgerinnen und Bürger über den Portalverbund zur zuständigen Behörde weitergeleitet werden und bei ihr direkt einen Antrag stellen, abgewichen sind:

Nach den neuen, zum Teil schon verwirklichten Planungen sollen den Bürgerinnen und Bürgern Antragsportale mit digitalen Antragsassistenten zur Verfügung gestellt werden, die den Antragsteller beim Ausfüllen des Antragsformulars unterstützen sollen (vgl. Nr. 6.2.1). Mit dem Antragsassistenten werden somit personenbezogene Daten erhoben, die im Antragsportal zwischengespeichert werden können, bevor sie an die zuständige Behörde weitergeleitet werden. Diese zusätzliche Datenerhebung durch das Antragsportal ist im OZG jedoch nicht vorgesehen.

Ein weiteres Problem besteht darin, dass das Antragsportal aufgrund einer Verwaltungsvereinbarung der teilnehmenden Länder stets nur von einem Land betrieben werden soll, das datenschutzrechtlich allein für den Betrieb des Portals verantwortlich erklärt wird. Das gilt auch dann, wenn der Antragsassistent Daten von Antragstellern an Behörden aus anderen Bundesländern übermittelt, also Antragsteller und Daten empfangende Behörde nicht dem Zuständigkeitsbereich des portalbetreibenden Landes unterfallen (Beispiel: Sachsen-Anhalt erhebt Daten eines Antragstellers aus Bayern und übermittelt diese an eine Behörde in Hamburg). Damit wurde auch das „Einer-für alle-Prinzip“ aufgegeben, denn es gibt hier keine Verwaltungsleistung mehr, die den anderen Bundesländern zur Nachnutzung zur Verfügung gestellt werden kann.

Die UAG hat in den Gesprächen mit dem BMI bereits klargestellt, dass sie diese Verwaltungsvereinbarungslösung für problematisch hält. Das ergibt sich schon daraus, dass nach deutschem Recht Grundrechtseingriffe, hier also die Verarbeitung personenbezogener Daten, nicht durch eine Verwaltungsvereinbarung geregelt werden können (vgl. auch Nr. 6.2.1 am Beispiel von BAföG Digital). Zudem würden durch die Verwaltungsvereinbarung die Zuständigkeit der datenverarbeitenden Behörde und damit auch die Zuständigkeit der Aufsichtsbehörde einseitig durch die Exekutive festgelegt. Auch solche Festlegungen kann nur der Gesetzgeber treffen.

Ein zusätzliches Problem ist der fehlende Informationsfluss. Die UAG Portallösungen kann die öffentlichen Stellen des Bundes und der Länder nur dann beraten und unterstützen, wenn sie weiß, welche Portalmodelle zum Einsatz kommen. Sie hat daher das BMI gebeten, Auskunft über die vorhandenen Portallösungen sowie die mit ihnen verbundenen Datenflüsse zu erteilen, um eine datenschutzrechtliche Bewertung der Portalmodelle vornehmen zu können. Diese Informationen wurden den Datenschutzaufsichtsbehörden jedoch nicht zur Verfügung gestellt. Damit fehlt eine Grundvoraussetzung für eine Beratungstätigkeit.

Der Bund hat die oben dargestellte Problematik mittlerweile gesehen und in §§ 9a bis c E-Government-Gesetz des Bundes auf Bundesebene das Antragsportal und die datenschutzrechtliche Verantwortlichkeit gesetzlich geregelt. Eine Lösung auf Landesebene könnte darin bestehen, entsprechende Regelungen in das E-Government-Gesetz des Landes aufzunehmen. Sinnvoll könnte es auch sein, in die Landesdatenschutzgesetze eine Befugnis zur Erhebung personenbezogener Daten und deren Übermittlung an die zuständige Behörde durch einen digitalen Antragsassistenten für die o. g. länderübergreifenden Fälle aufzunehmen. Vorbild für eine solche Regelung könnte z. B. § 24b Abs. 1 Satz 1 Bundes-elterngeld- und Elternzeitgesetz sein.

Der Landesbeauftragte wird über die Ergebnisse der UAG weiter berichten.

6.2.1 BAföG Digital

Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsleistungen über ein Bund-Länder-Portal auch digital anzubieten. Für die Bereitstellung der Verwaltungsleistungen haben Bund und Länder das „Einer-für-alle-Prinzip“ vereinbart. Nach dieser Vereinbarung ist Sachsen-Anhalt für das Themenfeld Bildung zuständig und betreut in diesem Zusammenhang das Projekt BAföG digital. Das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung hat dem Landesbeauftragten ein Datenschutzkonzept für den Online-Antragsassistenten BAföG digital vorgelegt. Der Landesbeauftragte hat das Ministerium hierzu beraten.

Gegenstand des Datenschutzkonzepts ist ein Antragsportal mit einem Online-Antragsassistenten, mit dem online Anträge auf Ausbildungsförderung gestellt werden können. Die Bearbeitung des Antrags erfolgt durch das einzelne für Ausbildungsförderung zuständige Amt mit dem jeweiligen Fachverfahren. Der Antragsassistent unterstützt beim Ausfüllen der Antragsformulare, die bereits für BAföG online genutzt wurden. Maßgeblich hierfür ist die BAföG-Formblatt-VwV des Bundesministeriums für Bildung und Forschung. Basis der Umsetzung dieses „Einer-für-alle-Verfahrens“ ist eine Verwaltungsvereinbarung von Bund und Ländern, in der das Land Sachsen-Anhalt als Rechteinhaber benannt wird. Das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung ist nach Art. 4 Nr. 7 zweiter Halbsatz DS-GVO als Verantwortlicher bestimmt. Mit der technischen Unterstützung und für den technischen Support ist der zentrale IT-Dienstleister Dataport AöR beauftragt.

Das Ministerium hält die Datenverarbeitung durch den Antragsassistenten gem. Art. 6 Abs. 1 lit. e DS-GVO i. V. m. § 4 Satz 1 Nr. 2 DSAG LSA für zulässig (erforderlich zur Erfüllung einer in der Zuständigkeit des Verantwortlichen liegenden Aufgabe, deren Wahrnehmung im öffentlichen Interesse liegt). Nach Art. 4 Nr. 7 zweiter Halbsatz DS-GVO könne der Verantwortliche durch Recht der Mitgliedstaaten vorgegeben werden. Dies seien Normen, die eine Rechtspflicht im mitgliedstaatlichen Recht begründen. Verwaltungsvorschriften und auch die vorgenannte Verwaltungsvereinbarung wären insoweit ausreichend.

Fraglich erschien die Rechtsauffassung, dass der bundesweite Betrieb des Online-Assistenten zur Erfüllung einer gerade in der Zuständigkeit eines sachsen-anhaltischen Ministeriums liegenden Aufgabe erfolge, deren Wahrnehmung im öffentlichen Interesse liege. Eine statthafte Aufgabe bzw. ein öffentliches Interesse, dass das Land Sachsen-Anhalt personenbezogene Daten von Menschen verarbeitet, die keinen Bezug zu Sachsen-Anhalt aufweisen, ist nur bedingt erkennbar. Eine Verwaltungsvereinbarung als Zuständigkeitsregelung könnte nicht ausreichen, sondern eine staatsvertragliche Zuweisung der Aufgabe geboten sein. Auch wenn das Recht der Mitgliedstaaten nach Art. 4 Nr. 7 zweiter Halbsatz DS-GVO nicht zwingend ein Parlamentsgesetz fordert, ist wohl zumindest eine parlamentsgesetzliche Ermächtigung und eine Veröffentlichung in einem außenwirksamen Regelwerk zu fordern.

Weiter wirft die Konzeption die Frage einer gemeinsamen Verantwortlichkeit auf, die nach Art. 26 DS-GVO vorliegt, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen. Nach dem Datenschutzkonzept entscheidet das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung des Landes Sachsen-Anhalt in Abstimmung mit den teilnehmenden Ländern im Lenkungskreis „BAföG digital“ über Inhalt, Zweck und Mittel der Verarbeitung von personenbezogenen Daten. Auch in der Verwaltungsvereinbarung werden Zwecke und Mittel der Datenverarbeitung gemeinsam bestimmt. Die strategische und operative Steuerung erfolgt über den gemeinsamen Lenkungskreis. Es liegt eine gewollte und bewusste Zusammenarbeit vor. Die Vertragsparteien nehmen Einfluss bzw. halten sich diesen durch die Verwaltungsvereinbarung offen. Diese Einflussnahme erfolgt auch im eigenen Interesse, da die Länder gehalten sind, Onlinezugänge zu gestalten. Zwar ist es im Fall des Antragsassistenten die Regel, dass fast alle der Beteiligten mit Ausnahme des verarbeitenden Landes Sachsen-Anhalt und des Landes aus dem der Antragsteller kommt sowie des Landes, in dem die zuständige Fachbehörde sitzt, kein Interesse und auch keine Befugnis haben, die Daten des jeweiligen Antragstellers zu verarbeiten. Insoweit könnte aber berücksichtigt werden, dass es für die gemeinsame Verantwortlichkeit mehrerer Betreiber für dieselbe Verarbeitung nicht zwingend erforderlich ist, dass jeder Zugang zu den personenbezogenen Daten hat. Insgesamt liegt eine gemeinsame Verarbeitung von Bund und Ländern nahe.

Auch die Frage nach den Rechtsgrundlagen für die Verarbeitung personenbezogener Daten ist problematisch. Insoweit könnte das Ministerium wohl für die landeseigenen Fälle auf § 4 DSAG LSA zurückgreifen. Sofern eine gemeinsame Verantwortlichkeit vorliegt, müssten aber alle Beteiligten auf eigene Rechtsgrundlagen zurückgreifen können. Andere Länder könnten, soweit sie durch den Wohnsitz des Antragstellers bzw. den Sitz des Amtes für Ausbildungsförderung betroffen sind, ggf. auf ihre allgemeinen datenschutzgesetzlichen Befugnisse zurückgreifen. Es verbliebe dann aber noch die Notwendigkeit, für das Ministerium im Falle seiner Nichtbeteiligung (kein Bürger und kein Amt aus Sachsen-Anhalt) eine Rechtsgrundlage zu finden. Dies könnte wohl nur durch eine Auftragsverarbeitung mit dem jeweiligen Land gemäß Art. 28 DS-GVO geschehen, sodass die Tätigkeit insoweit privilegiert wäre.

Der Landesbeauftragte hat das Ministerium umfassend beraten und eine Anpassung der Vereinbarungen und vertraglichen Ausgestaltungen angeregt. Das Ministerium ist aber zunächst seinem ursprünglichen Konzept gefolgt. Weiter wird die Problematik auch im Kreise der Datenschutzaufsichtsbehörden erörtert.

6.3 Verwaltungs- und Registermodernisierung – datenschutzkonform gestalten

In seinem XVI. Tätigkeitsbericht (Nr. 6.3) erörterte der Landesbeauftragte die Vorbereitungen des Normenkontrollrates, des IT-Planungsrates und des Bundesministeriums des Innern, für Bau und Heimat (BMI) zur Modernisierung der deutschen Registerlandschaft im Zuge der Untersetzung des Onlinezugangsgesetzes (OZG), welches die Digitalisierung der wesentlichen Verwaltungsleistungen bis 2022 zum Ziel hat.

Nachdem die Rahmenbedingungen festgelegt waren und die OZG-Umsetzung bereits in vollem Gange war, legte das BMI am 25. September 2020 den Entwurf zu einem Registermodernisierungsgesetz (RegMoG) vor, welches u. a. zum Ziel hatte, die Steueridentifikationsnummer als einheitliches registerübergreifendes Identifikationsmerk-mal zu verwenden (BT-Drs. 19/24226). Dieses Vorhaben stieß bei Verfassungsschützern, Bürgerrechtlern und den Datenschutzaufsichtsbehörden aufgrund von verfassungsrechtlichen Bedenken auf Kritik.

Hatte doch der Gesetzgeber mit der Einführung einer einheitlichen Steueridentifikationsnummer für alle Bürger auch festgelegt, diese nur zu Zwecken der Steuererhebung zu verwenden (vgl. § 139b Abs. 2 AO). Die bisher getrennte Führung unterschiedlicher Register durch unterschiedliche Behörden zu unterschiedlichen Zwecken ohne einen zentralen registerübergreifenden staatlichen Zugriff zu ermöglichen, resultiert aus dem Volkszählungsurteil des BVerfG vom 15. Dezember 1983 über das verfassungsmäßige Grundrecht auf informationelle Selbstbestimmung.

Aus diesem Grund legte die DSK in Ergänzung zu ihrer Entschließung vom 12. September 2019 „Digitalisierung der Verwaltung – datenschutzkonform und bürgerfreundlich gestalten!“, in der bereits die Anwendung sektorspezifischer Personenkennziffern – so wie etwa in der Republik Österreich umgesetzt – gefordert wurde, am 26. August 2020 die Entschließung „Registermodernisierung verfassungskonform umsetzen!“ **(Anlage 3)** vor.

Darin weist sie darauf hin, dass die Steueridentifikationsnummer bisher nur deswegen als verfassungskonform angesehen wird, weil sie einer engen Zweckbindung für steuerliche Zwecke unterliegt. Weiterhin attestiert die DSK ein hohes Missbrauchspotential in diesem sektorübergreifenden Ordnungsmerkmal, welches Bürgerdaten aus mehr als 50 Registern miteinander verknüpft und somit die technische und logische Grundlage dafür schafft, über weitere Ge-

setze verfassungsrechtliche Grundsätze aufzuweichen und eine zukünftige staatliche Profilbildung komplexer bürgerlicher Lebensverhältnisse zu ermöglichen. Auch kommt sie zu dem Schluss, dass die von autorisierten Behörden einsehbare Ende-zu-Ende-Verschlüsselung letztlich nicht vor einer missbräuchlichen Zusammenführung der Daten oder unbeabsichtigten Datenlecks schützen kann. Schließlich konstatiert sie, dass die Beschleunigung der Digitalisierung nicht als Argument benutzt werden darf, verfassungsrechtlich notwendige Nachbesserungen unter den Tisch fallen zu lassen.

6.8 Microsoft Office 365

Der Landesbeauftragte wurde von mehreren Behörden und Unternehmen gefragt, wie mit Office 365 (ProPlus) bzw. nunmehr „Microsoft 365 Apps for Enterprise“ (ab hier „MS 365“) umzugehen sei. Im Kern der Anfragen geht es um den Umgang mit Microsofts Online-Diensten und Bedenken bzgl. möglicher Datenabflüsse in Richtung Microsoft.

MS 365 ist eine als Software as a Service (SaaS) im Internet in der Microsoft Cloud angebotene Office-Suite. Es werden gehostete Webversionen der Microsoft-Office-Anwendungen mit Services in der Cloud kombiniert. MS 365 ist zwar auch lokal als On-Premises-Installation nutzbar, jedoch bieten zahlreiche Online-Dienste einen deutlichen Mehrwert und langfristig ist zu erwarten, dass der Schritt in die Cloud vollumfänglich vollzogen werden wird. Bereits seit vielen Jahren werden immer mehr Funktionen in die Cloud ausgelagert oder neue Funktionen nur dort angeboten. Enthalten sind regelmäßig die Office-Kernanwendungen Exchange Online, Lync Online und SharePoint Online, aber auch die Office Web Apps. Die zugehörigen Online-Dienste umfassen Online-Konten, E-Mail, Kalender, gemeinsam nutzbaren Speicherplatz im Internet, eine Kollaborationsplattform und selbst eine Videokonferenzplattform (Microsoft Teams).

Beim Einsatz von MS 365 handelt der Nutzer als Verantwortlicher (Art. 4 Nr. 7 DS-GVO) und Microsoft regelmäßig als Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO). Die DS-GVO benennt die zu prüfenden Kriterien, die ein Auftraggeber als Verantwortlicher zu berücksichtigen hat:
Einem Verantwortlichen obliegt es zunächst gem. Art. 32 Abs. 1 DS-GVO, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Kategorien personenbezogener Daten festzustellen und basierend darauf die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener natürlicher Personen zu beurteilen. Je nachdem, ob nur pseudonyme Metadaten in einer Ende-zu-Ende-verschlüsselten Videokonferenz oder detaillierte Bürger- oder Schülerdaten in einer Cloud verarbeitet werden, wird das Ergebnis stark variieren.

Da es sich bei der Nutzung von MS 365 regelmäßig um Auftragsverarbeitung handelt, sind die Voraussetzungen nach Art. 28 DS-GVO zu beachten. Der Verantwortliche hat danach bei der Auswahl eines Auftragsverarbeiters zu berücksichtigen, dass dieser hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen getroffen wurden und so durchgeführt werden, dass die Verarbeitung dauerhaft im Einklang mit den Anforderungen der DS-GVO erfolgt und damit der Schutz der Rechte der betroffenen Personen gewährleistet ist.

Ein Auftraggeber bleibt für die Verarbeitung der personenbezogenen Daten in seiner Hoheit voll verantwortlich und muss sich etwaige Fehler zurechnen lassen. Ein Auftragsverarbeiter ist vorab zu überprüfen und passend auszuwählen. Die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten gem. Art. 5 DS-GVO ist sicherzustellen.

Microsoft behauptet selbst, MS 365 sei DS-GVO-konform nutzbar. Dies muss aus einer Reihe von Gründen (mangelnder Transparenz, fehlenden Konfigurationsmöglichkeiten und auch rechtlichen Defiziten) bezweifelt oder gar verneint werden.

Zur Erfüllung der Verpflichtungen aus der DS-GVO stellt Microsoft dem Verantwortlichen Online Service Terms (OST) und Data Processing Addenda (DPA, Datenschutz-bestimmungen) als Vertragsbestandteile zur Verfügung. Die Datenschutzkonferenz (DSK) kommt im September 2020 nach Auswertung der OST und der DPA mit knapper Mehrheit zu dem Ergebnis, dass auf Basis der genannten Unterlagen kein daten-schutzgerechter Einsatz von MS 365 möglich ist. Die von Microsoft noch im Laufe des Untersuchungszeitraums angepassten Dokumente wiesen in den bereits vorab genannten Kritikpunkten keine wesentlichen Veränderungen auf.

Auch Datenschutzbeauftragte anderer EU-Länder und auch der Europäische Datenschutzbeauftragte sehen noch verschiedene offene Punkte, die mit der DS-GVO in Einklang zu bringen sind und noch Änderungen von Produkt und Vertragsbedingungen durch Microsoft erfordern. Abschließende Einschätzungen werden darüber hinaus dadurch erschwert, dass das Produkt unangekündigt geändert werden kann und auch die Vertragsbedingungen möglichen Änderungen unterliegen.

Eine verantwortliche Stelle, die Microsoft als Auftragsverarbeiter gem. Art. 28 DS-GVO mit der Bereitstellung von MS 365 beauftragen möchte, sollte sich einer Reihe von Problemen bewusst sein, die derzeit nicht vollumfänglich ausgeräumt werden können:

- Bei der Auftragsverarbeitung stellt Art. 28 DS-GVO genaue Anforderungen an die Inhalte des zugehörigen Vertrages. In den Dokumenten von MS 365 finden sich jedoch unpräzise Beschreibungen zu Arten und Zwecken der Datenverarbeitungen und den betroffenen personenbezogenen Daten.

- Die Dokumente enthalten nur unzureichende Informationen über Unterauftragnehmer, einschließlich deren Aktualisierung gem. Art. 28 Abs. 2 DS-GVO. Die Angaben Firmenname, Land und ein paar Worte zum angebotenen Dienst sind deutlich zu wenig![21] Auch sind weitergehende Informationen zum Datenumfang als beispielsweise „pseudonymisierte Kundendaten“ notwendig. Diese Informationen müssen auch ohne vorherige Anmeldung abrufbar sein.

- Es fehlen Beschreibungen der Umsetzungen risikoangemessener technischer und organisatorischer Maßnahmen gem. Art. 32 DS-GVO. Diese sind gegenwärtig durch Verantwortliche nicht überprüfbar!

- Eine Offenlegung personenbezogener Daten gegenüber amerikanischen Sicherheitsbehörden oder Geheimdiensten ist aufgrund des Clarifying Lawful Overseas Use of Data (CLOUD) Act und des Foreign Intelligence Surveillance Act (FISA) nicht ausgeschlossen.

  Datentransfers in Drittländer obliegen generell zusätzlichen Anforderungen. Der Europäische Gerichtshof urteilte am 16. Juni 2020 zur Zulässigkeit internationaler Datentransfers (C-311/18 – Schrems II) und der Unzulässigkeit des Privacy Shields. Die alternativ von der EU-Kommission angebotenen Standardvertragsklauseln sind ohne ergänzende Maßnahmen keine ausreichende Rechtfertigung für die Datenübermittlung in die USA und viele weitere Drittländer.

Der EDSA stellt in seinen Empfehlungen „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“[22] unter anderem fest, dass ein Transfer unverschlüsselter Daten – etwa im Rahmen einer Textverarbeitung in der Cloud – nicht rechtskonform möglich ist (Anhang 2, Anwendungsfall 6).

- Die eigene Verantwortlichkeit Microsofts im Rahmen der Verarbeitungen personenbezogener Daten für eigene Geschäftszwecke wird unzureichend transparent beschrieben und ist teilweise ohne ausreichende Rechtsgrundlage. Das betrifft z. B. die Weitergabe von Daten von Bürgern durch öffentliche Verwaltungen, aber auch Telemetriedaten-Abflüsse mit unbekanntem Umfang, Zielen und Zwecken.

- Darüber hinaus fehlen Angaben zu Löschregeln und -fristen von zu eigenen Zwecken durch Microsoft erhobenen personenbezogenen Daten.

Der Landesbeauftragte wurde durch eine Behörde gefragt, ob es datenschutzrechtlich möglich sei, eine deutlich kostengünstigere MS 365-Lizenzierung lediglich zum Zweck der Lizenzüberprüfung (und Vertragsverlängerung) einer bestehenden On-Premises-Installation zu nutzen. Eine Übertragung von Beschäftigtendaten in begrenztem, möglichst pseudonymen Umfang ins Azure Active Directory mit dem alleinigen Zweck der Authentifizierung und des Lizenzmanagements könnte als unproblematisch angesehen werden, auch weil die Daten in der EU verbleiben sollten. Zur Aktivierung und Aktualisierung des Product Keys würde dann bei der Anmeldung, einmal täglich, mit dem Office-Lizenzierungsdienst und dem Aktivierungs- und Validierungsdienst über eine Internetanbindung kommuniziert. Allerdings waren die dabei übertragenen Dateninhalte und Übertragungsziele unklar und sollten geprüft werden. Es wurde davon ausgegangen, dass nur kryptografische Token ausgetauscht werden, jedoch könnten auch Logs existieren und zusätzliche personenbezogene Daten übertragen und zu Profilen verdichtet werden. Auch sollte bedacht werden, dass die Nutzung von MS 365 als Möglichkeit der Lizenzkostenverringerung über On-Premises-Installationen allem Anschein nach nur temporär Bestand haben wird. Mit der Version 2019 wurde die Supportdauer verringert und an die der Version 2016 angeglichen – das Supportende der On-Premises-Version könnte demnach bereits feststehen.[23] Mittelfristiges Ergebnis der Migration ist mit hoher Wahrscheinlichkeit eine zunehmende Nutzung der Microsoft Cloud und damit eine dauerhafte, deutlich größere Abhängigkeit von Microsoft.

Die Lizenzierung zusätzlicher Dienste und Komponenten zu Testzwecken weist allerdings möglicherweise auf das langfristige Ziel der Behörde hin. Einige Lizenzen wurden um einen Office 365 Enterprise E1, sowie Mobility + Security E3 Plan erweitert. Diese bieten Zugriff auf Online-Dienste, wie etwa OneDrive, Exchange, Teams, SharePoint. Der von Bundesregierung, IT-Planungsrat und auch der EU immer wieder geforderten „Digitalen Souveränität“ – also der digitalen Unabhängigkeit von einzelnen, großen Anbietern – würde dies jedoch nicht entsprechen. Es wurde daher bereits vorab geraten, eine Evaluierung der eigenen Bedürfnisse, des Nutzens, der Risiken und der Möglichkeiten auch alternativer und Open-Source-Software vorzunehmen. Bei einer weitergehenden Nutzung insbesondere der Online-Komponenten von MS 365 wäre auch eine erneute Bewertung des Einsatzes notwendig.

In dem durch die Behörde angestrebten aktuellen Pilotprojekt mit:

- nur minimal betroffenen, personenbezogenen Daten,
- ohne Speicherung bei Drittanbietern,
- ohne Speicherung personenbezogener Daten Dritter,
- ohne Nutzung der Microsoft Online-Dienste für Fachaufgaben,
- ohne direkte Anbindung an Microsofts IKT-Infrastruktur und
- unter Nutzung von lokal installierter Software

sind die vorgenannten Kritikpunkte an MS 365 weniger schwerwiegend.

Bezüglich der im Raum stehenden Absicht des Abschlusses eines Landesvertrages zur Auftragsverarbeitung wurde vorsorglich auf die Einhaltung des Landesrechts (§ 15 Abs. 2 DSAG LSA – Unterwerfungspflicht des Auftragsverarbeiters) hingewiesen. Im Raum steht aber auch die Nutzung eines möglicherweise zukünftigen Bundes-Rahmenvertrages in einer Bundes-Cloud oder auch die Nutzung des Phoenix-Arbeitsplatzes von Dataport. Eine Entscheidung ist hier durch das Ministerium der Finanzen zu fällen.

Der Einsatz von MS 365 kann nur – wenn überhaupt möglich – in hinreichend abgesicherter Art und Weise erfolgen. Für Schulen und die öffentliche Verwaltung ist ein vollkommen datenschutzgerechter Einsatz derzeit wohl ausgeschlossen. Verantwortliche Stellen müssen sich eigenverantwortlich mit der Thematik auseinandersetzen, Risiken abwägen und zusätzliche Maßnahmen zu deren Minimierung ergreifen.

Jeder Verantwortliche muss selbst eine datenschutzrechtliche Bewertung vornehmen. Dabei muss nachgewiesen werden, dass das Produkt für den vorgesehenen Einsatzzweck und im geplanten Nutzungsumfang geeignet ist und die gesetzlichen Anforderungen vollständig erfüllt. Die rechtmäßige Verarbeitung muss nachgewiesen werden können (Art. 5 DS-GVO).

Der Landesbeauftragte rät aufgrund der beschriebenen Schwierigkeiten von der Nutzung von MS 365 derzeit nachdrücklich ab.

6.9 Mobiles Arbeiten – Home-Office

Bedingt durch die Corona-Pandemie sind Arbeitgeber und Dienstherren derzeit dazu angehalten bzw. bestrebt, Beschäftigte, deren Präsenz nicht unbedingt erforderlich ist, ins sog. Home-Office zu beordern. Beim Home-Office, oft auch Heimarbeit oder Wohnraumarbeit genannt, handelt es sich um die Verlagerung der Ausübung beruflicher bzw. dienstlicher Aufgaben in den privaten Wohnbereich. Diese Art der Arbeitsorganisation kann sich auf verschiedene technische und organisatorische Hilfsmittel stützen, die zum Teil schon in vorherigen Tätigkeitsberichten des Landesbeauftragten adressiert wurden. So hatte der Landesbeauftragte bereits in seinem IX. Tätigkeitsbericht (Nr. 14.14) und XIII./XIV. Tätigkeitsbericht (Nr. 12.12) die Telearbeit aus materiell-rechtlicher Sicht behandelt. Zudem hatte er sich in seinem XI. Tätigkeitsbericht (Nr. 4.9) zu den Themen Mobile Computing und Bring Your Own Device geäußert. Zuletzt hatte der Landesbeauftragte in seinem XVI. Tätigkeitsbericht (Nr. 6.9) zum Thema Geräte- und Datenträgerverschlüsselung beim mobilen Arbeiten aufgeklärt. Im aktuellen Tätigkeitsbericht wendet er sich dem Bereich Videokonferenzsysteme (Nr. 6.12) zu.

Die vorgenannten Themenbereiche fließen unterschiedlich stark in den Komplex Home-Office ein. So sollte Telearbeit, sofern Fernzugriffe auf unternehmens- bzw. behördeninterne Strukturen erfolgen, durch VPN-Kanäle abgesichert sein oder über sichere webbasierte Kollaborationsplattformen erfolgen. Der Einsatz privater Geräte bei der Verarbeitung betrieblicher bzw. dienstlicher Daten sollte generell vermieden oder nur unter strengen Vorgaben im Rahmen eines gut organisierten Mobile Device Managements durchgeführt werden. Mobile Datenträger und Geräte wie Laptops, Tablets und Smartphones sollten generell verschlüsselt sein. Der Zugang zu diesen Geräten sollte, wenn möglich, nur mit Zwei-Faktor-Authentifizierung oder zumindest mit sicheren Passwörtern ermöglicht werden. Bei der Nutzung von Chat- und Videokonferenzdiensten sollten geeignete Dienstleister ausgewählt und vertragliche Rahmenbedingungen berücksichtigt werden. Dies gilt auch für den Einsatz von Kollaborationsplattformen. Generell sollten personenbezogene Daten so wenig wie möglich die Unternehmens- bzw. Behördenstrukturen verlassen und wenn, dann nur verschlüsselt. Des Weiteren sollte zunächst immer erst der Eigenbetrieb vorgenannter Dienste in Betracht gezogen werden. Beim Einsatz von Dienstleistern ist von Anbietern aus unsicheren Drittländern Abstand zu nehmen und sind die Vorgaben des Art. 28 DS-GVO zu beachten. Außerdem sollten Verschlüsselungsmechanismen immer nach dem Stand der Technik implementiert sein und zusammen mit sicheren Passwörtern zur Anwendung kommen.

Schließlich ist die Unternehmens- bzw. Behördenleitung, die Home-Office anordnet, hinsichtlich der Verarbeitung personenbezogener Daten verantwortlich i. S. d. Art. 4 Nr. 7 DS-GVO und damit verpflichtet, die Grundsätze der Verarbeitung personenbezogener Daten gem. Art. 5 Abs. 1 DS-GVO einzuhalten, unabhängig davon, wo sich Mitarbeiter während der Arbeit aufhalten. Die vorgenannten technischen Maßnahmen müssen dabei auch durch organisatorische Maßnahmen untersetzt werden. So müssen für das Home-Office Regelungen getroffen und Beschäftigte verpflichtet werden, sich an entsprechende Vorgaben zu halten. Dabei sind die Effektivität und die Eignung sowohl der technischen als auch der organisatorischen Maßnahmen regelmäßig zu überprüfen. Eine übersichtliche Zusammenstellung der o. g. Kriterien hat das BSI in den Handreichungen „Tipps für sicheres mobiles Arbeiten“[24] und „Empfehlungen zum sicheren mobilen Arbeiten im Home-Office“[25] veröffentlicht.

Im Übrigen sind auch bei der Verbringung von papierbasierten Dokumenten in den privaten Wohnbereich Regelungen zu treffen, die eine unbeabsichtigte Offenlegung effektiv verhindern können. Je nach Risiko kommen z. B. folgende organisatorische Maßnahmen in Betracht: Transport erfolgt in einem geschlossenen Behältnis; Transport erfolgt auf direktem Wege in den privaten Wohnbereich, ohne Erledigung privater oder dienstlicher Pflichten; Behältnis wird während des Transportes jederzeit in unmittelbarer Nähe der transportierenden Person geführt und unter keinen Umständen dem Zugriff Dritter ausgesetzt; Transport erfolgt nicht via öffentlicher Verkehrsmittel, wo ein Zugriff Dritter mit erhöhter Wahrscheinlichkeit stattfinden kann; Aufbewahrung erfolgt an einem sicheren Ort bzw. in einem gesicherten Behältnis innerhalb des privaten Wohnbereichs; Belehrung über das erhöhte Risiko wird durchgeführt; Dokumentation der Ausgabe wird angelegt; Dokumentation der Rückführung wird angelegt; über Transport und Aufbewahrung wird zu Verschwiegenheit verpflichtet; Vorkommnisse bzgl. einer unbeabsichtigten Offenlegung oder Beschädigung werden unverzüglich gemeldet; regelmäßige Evaluierung der Wirksamkeit durchgeführter Maßnahmen; regelmäßige Mitarbeiterbefragung über die Realisierbarkeit angeordneter Maßnahmen.

Der CIO des Landes Sachsen-Anhalt erstellt derzeit eine Informationssicherheitsricht-linie zum Thema Telearbeit. Anlass dafür war der Beschluss des Landtages (LT-Drs. 7/2933) vom 24. Mai 2018 mit dem die Landesregierung aufgefordert wurde, ein Konzept zur Förderung und Umsetzung von Telearbeit für die unmittelbare Landesverwaltung zu erarbeiten. Dazu sollte eine umfassende Bestandsaufnahme zur Telearbeit vorgelegt werden, was mit dem Bericht „Telearbeit in der Landesverwaltung Sachsen-Anhalt“ inklusive eines Entwurfs einer Rahmenrichtlinie über flexibles Arbeiten in Telearbeit in der Landesverwaltung des Landes Sachsen-Anhalt (LT-Drs. 7/5474) erfolgte. Diese Unterlagen dienten als Grundlage für die weitere Behandlung in den zuständigen Ausschüssen für Inneres und Sport, für Finanzen, für Wirtschaft, Wissenschaft und Digitalisierung sowie für Arbeit, Soziales und Integration.

Nach kursorischer Durchsicht des Entwurfs der Informationssicherheitsrichtlinie zur Telearbeit konnte der Landesbeauftragte feststellen, dass auch für den Datenschutz wesentliche Anforderungen in dem Dokument adressiert werden. Allerdings sollte sich der CIO des Landes Sachsen-Anhalt nicht mehr allzu sehr mit dem Inkraftsetzen der Richtlinie Zeit lassen, denn schon vor Pandemiebeginn wurde Telearbeit in den obersten Landesbehörden intensiv in Anspruch genommen. So geht aus der Antwort der Landesregierung (LT-Drs. 7/6381) auf eine Kleine Anfrage zum Thema Telearbeit in der Landesverwaltung hervor, dass bereits in den Jahren 2018 und 2019 insgesamt 692 Anträge auf Telearbeit in den obersten Landesbehörden genehmigt wurden.

6.13 Informationssicherheit

Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) enthält Regelungen, unter anderem zu Aufgaben und Befugnissen, die spezifisch für das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind. Es wurde am 19. Juni 2020 geändert. Aufgaben des BSI sind u. a. Gefahrenabwehr, Sammlung und Auswertungen von Informationen zu Sicherheitsrisiken und -vorkehrungen, auch Eigenentwicklungen von Sicherheitsvorkehrungen, Entwicklung von Kriterien und Werkzeugen zur Bewertung von IT-Systemen (u. a. IT-Grundschutz), aber auch die Prüfung der Sicherheit von IT-Systemen und das Schlüssel- und Sicherheitsmanagement für die Bundes-Kryptografie. Auch kümmert sich das BSI um den Schutz kritischer Infrastrukturen (KRITIS) etwa durch Festlegung der Betreiber. Diese müssen angemessene technische und organisatorische Schutzmaßnahmen nach dem Stand der Technik treffen, um beispielsweise die Verfügbarkeit und Vertraulichkeit ihrer IT-Systeme sicherzustellen.

Das BSI kann Ländern Dienstleistungen anbieten und diese insbesondere bei der Absicherung ihrer IT unterstützen. Es warnt vor Sicherheitslücken oder aktuell kursierender Schadsoftware. Auch werden Mindeststandards für die Sicherheit der Bundes-IT erarbeitet.

Für die Landesbehörden gab es bereits 2018 und 2019 Bestrebungen, ein gemeinsames Informations-Sicherheits-Management-System (ISMS) aufzubauen. Dataport hostet dafür die Fachanwendung „HiScout“. Die HiScout GRC Software ist eine browserbasierte Multiuser-Standardsoftware für IT-Grundschutz, Informationssicherheits-Management, Business Continuity Management und Datenschutz-Management. Im Jahr 2020 erfolgten erste Schulungen der Nutzer. Behördenspezifische Anpassungen der Konfiguration, der sogenannte Behörden-Client, sollen bereitgestellt werden. Da die Informationssicherheit eine wichtige Voraussetzung für die Einhaltung des Datenschutzes ist, wird die Bereitstellung des Datenschutz-Moduls im Verbund vom Landesbeauftragten befürwortet.

Bereits im Dezember 2018 trat die lange erwartete Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalt (LISL LSA, Informationssicherheitsleitlinie) des Landes in Kraft, vgl. XV. Tätigkeitsbericht (Nr. 5.2). Die Arbeitsgruppe Informationssicherheit (AG InfoSic Land) stellt das ISM-Team, welches umgehend die Arbeit aufgenommen hat und – unter Einbeziehung des Landesbeauftragten – damit begonnen hat, die Regelungen mit Leben zu füllen. In UAGs der AG InfoSic im Ministerium der Finanzen werden nach und nach zugehörige Informationssicherheitsrichtlinien (ISRL) – beginnend mit der Passwort- und der Telearbeits-Richtlinie – erarbeitet.

Die ISRL werden für alle Stellen der unmittelbaren Landesverwaltung in Sachsen-Anhalt einschließlich der beauftragten externen Dienstleister gelten und einen Mindeststandard einfordern. Der mittelbaren Landesverwaltung und weiteren Stellen, u. a. dem Landesbeauftragten, wird die Berücksichtigung empfohlen. Positiv anzumerken ist, dass die Erarbeitung auf hohem Standard erfolgt und sich eng an den BSI-Vorgaben orientiert. Im Ergebnis sind einige Inhalte sogar strenger formuliert, als es der Landesbeauftragte gefordert hat. Alle Ressorts haben die Möglichkeit der Mitarbeit. Nicht einzuhaltende Punkte, Abweichungen und Ausnahmen sind dem Landes-CISO zu melden, insofern wird sich ein genaues Bild der IT-Sicherheitslage im Land im Rahmen des geregelten Umfangs nach und nach auch durch die Auswertung ggf. vorhandener Defizite zeichnen lassen. Die Dokumente sollen dann im Rahmen der planvollen Revision bei Bedarf angepasst werden.

Weitere in Arbeit befindliche ISRL sind die Behandlung von Sicherheitsvorfällen, das Dokumentenmanagement, Korrektur- und Vorbeugemaßnahmen, das Berichtswesen und die Prozessbeschreibung des Sicherheitsprozesses.

9 Verkehr

9.3 Anzeigen von Verstößen im ruhenden Verkehr, Datenweitergabe an den Ortsbürgermeister

Ein Beschwerdeführer vermutete eine rechtswidrige Datenweitergabe, als sich – unmittelbar, nachdem er verschiedene Verstöße im ruhenden Verkehr beim Ordnungsamt angezeigt hatte – der Ortsbürgermeister bei ihm meldete, um ihn zu überreden, die Anzeigen zurückzunehmen.

Obwohl die Stadt die Datenweitergabe bestritt und die Vermutung äußerte, der Ortsbürgermeister müsse aufgrund seiner Ortskenntnis die Person des Anzeigeerstatters erraten haben, bat sie um Mitteilung der Rechtsauffassung des Landesbeauftragten zu der Frage, ob § 85 Abs. 3 KVG LSA Ermächtigungsgrundlage für die Weitergabe personenbezogener Daten an den Ortsbürgermeister in allen Angelegenheiten, die die Ortschaft betreffen, ist.

Der Landesbeauftragte antwortete wie folgt: Die Rechte des Ortsbürgermeisters aus § 85 Abs. 3 KVG LSA waren bereits in der Gemeindeordnung a. F. festgeschrieben (§ 88 Abs. 3 Satz 3 u. 4 GO LSA), um die Funktion des Ortsbürgermeisters zu stärken.

Das Auskunftsrecht richtet sich ausdrücklich nur an den Ortsbürgermeister und beschränkt die Auskunft auf Angelegenheiten der Ortschaft. Das Auskunftsrecht wird durch das Akteneinsichtsrecht in Angelegenheiten, die die Ortschaft betreffen, ergänzt. Das Akteneinsichtsrecht kommt aber erst durch die Fassung eines Beschlusses durch den Ortschaftsrat zum Tragen.

Nach § 81 Abs. 4 KVG LSA gelten für die Ortschaftsräte die Vorschriften, die auch für die Gemeinderäte gelten und für das Verfahren im Ortschaftsrat die gleichen Vorschriften, die auch im Verfahren im Gemeinderat gelten, wenn im Abschnitt 4 – Ortschafts-verfassung – nichts Abweichendes geregelt ist. Davon gibt es einzelne Ausnahmen, wozu jedoch der § 45 Abs. 6 KVG LSA nicht gehört. Die Voraussetzungen, die im Verfahren der Akteneinsicht des Ortsbürgermeisters einzuhalten sind, sind somit identisch zum Verfahren, welches auch für die Einsetzung eines Akteneinsichtsausschusses im Stadtrat einzuhalten ist.

Gleichzeitig gibt § 81 Abs. 4 Satz 3 KVG LSA die Möglichkeit, Einzelheiten der Zusammenarbeit des Ortschaftsrates mit dem Stadtrat in der Geschäftsordnung zu regeln.

Der Beschluss für die Akteneinsicht des Ortsbürgermeisters muss, auch wenn das Verfahren nicht eindeutig im Gesetzestext vorgeschrieben ist, wie auch der Beschluss zur Bildung eines Akteneinsichtsausschusses nach § 45 Abs. 6 KVG LSA, auf einen hinreichend konkreten Anlass bezogen sein. Das heißt, er muss auf einen Einzelfall bzw. auf eine bestimmte Angelegenheit beschränkt sein (z. B. Verpachtung des Gemeindegrundstückes XY, nicht Untersuchung von Verpachtungen gemeindlicher Grundstücke allgemein, bzw. im konkreten Fall, nicht allgemein auf Parkverstöße im Bereich der Ortschaft). In den letztbenannten Fällen besteht die Gefahr, dass der Ortsbürgermeister durch solche Beschlüsse die Verwaltung dauerhaft kontrollieren würde, was nicht zu seinen Aufgaben gehört.

Aus der zugewiesenen Aufgabe durch den Beschluss ergibt sich der von der Verwaltung sicherzustellende Umfang des Datenschutzes. Es dürfen nur die personenbezogenen Daten dem Ortsbürgermeister bekannt werden, die für die jeweilige Aufgabenerfüllung der Akteneinsicht erforderlich sind. Gegebenenfalls ist zu schwärzen.

Der Ortsbürgermeister ist aufgrund § 32 KVG LSA zur Verschwiegenheit verpflichtet. Er darf somit im Ortschaftsrat zwar über das Ergebnis seiner Akteneinsicht berichten, jedoch nur in dem Umfang, den der Beschluss über die Akteneinsicht umfasst. Es sollte stets darauf geachtet werden, Informationen an den Ortschaftsrat in allgemeinen Formulierungen herauszugeben. Auf die Herausgabe von personenbezogenen oder personenbeziehbaren Daten soll soweit wie möglich verzichtet werden, da auch ein Verstoß z. B. gegen § 30 AO oder eine Verletzung von Amtsträgerpflichten u. a. eine Straftat oder Ordnungswidrigkeit sein könnte.

Ausgenommen vom Akteneinsichtsrecht dürften auch für den Ortsbürgermeister nach § 45 Abs. 7 KVG LSA Vorgänge sein, bei denen spezialgesetzliche Regelungen der Bekanntgabe entgegenstehen (z. B. im SGB) und Angelegenheiten, die nach § 6 Abs. 6 KVG LSA der Geheimhaltung unterliegen.

Aus hiesiger Sicht sprechen somit auch die nunmehr einzuhaltenden Regelungen der Datenschutz-Grundverordnung nicht grundsätzlich gegen die Akteneinsicht, zumal es sich beim Ortsbürgermeister um ein Organ der Ortschaft handelt, der wie der Stadtrat für die Stadt nicht als Dritter zu behandeln ist.

Der § 85 Abs. 3 KVG LSA ist somit als Ermächtigungsgrundlage für die Weitergabe der personenbezogenen Daten – immer im Rahmen des konkreten Ortschaftsratsbeschlusses – anwendbar.

15 Statistik, Kommunales

15.1 Zensus 2021 – Verschiebung auf 2022

Turnusgemäß war für den 16. Mai 2021 ein Zensus – also eine Volks-, Gebäude- und Wohnungszählung – vorgesehen (vgl. XVI. Tätigkeitsbericht, Nr. 13.1). Da aufgrund der Corona-Pandemie die planmäßige Vorbereitung und Durchführung des Zensus im Jahr 2021 nicht mehr sichergestellt werden konnte, hat der Deutsche Bundestag beschlossen, den Zensus um ein Jahr zu verschieben. Mit dem am 10. Dezember 2020 in Kraft getretenen Gesetz (BGBl. I S. 2675) steht als neuer Stichtag der 15. Mai 2022 fest.

Für den Fall, dass wegen der Corona-Pandemie „oder anderer zwingender Gründe“ eine weitere Verschiebung des Zensus erforderlich werden sollte, wurde die Bundesregierung ermächtigt, mit Zustimmung des Bundesrates Anpassungen durch Rechtsverordnung vorzunehmen.

Die Arbeiten zur Vorbereitung des Zensus waren in Folge der Corona-Pandemie zeitweise nur eingeschränkt möglich. Beschäftigte vieler Kommunen und auch der Statistischen Ämter des Bundes und der Länder wurden zum Teil in erheblichem Umfang für andere Aufgaben wie die Unterstützung der Gesundheitsämter bei der Kontaktnachverfolgung eingesetzt.

Der Großteil der Zensus-Daten wird zwar durch die Auswertung bestehender Quellen wie etwa der Melderegister gewonnen. Zur Erhebung von Informationen, die nicht in Registern verfügbar sind (beispielsweise zur Qualitätssicherung der Registerdaten), sind dennoch Vor-Ort-Befragungen erforderlich, deren Vorbereitung unter geltenden Pandemie-Bedingungen nicht möglich war. So konnten beispielsweise die vor Ort für die Befragung zuständigen Erhebungsstellen in Folge der Einschränkungen durch die Pandemie nicht wie geplant eingerichtet werden.

15.2 Behördliche Datenschutzbeauftragte der Kommunen

Seit Geltung der DS-GVO ist jeder Verantwortliche und Auftragsverarbeiter u. a. dann, wenn die Verarbeitung personenbezogener Daten von einer Behörde oder öffentlichen Stelle durchgeführt wird, verpflichtet, einen Datenschutzbeauftragten zu benennen und die Kontaktdaten der Aufsichtsbehörde – mithin dem Landesbeauftragten – mitzuteilen.

Vor diesem Hintergrund hat der Landesbeauftragte alle Kommunen im Land Sachsen-Anhalt schriftlich um Mitteilung der Kontaktdaten des jeweiligen Datenschutzbeauftragten gebeten. Diese Gelegenheit hat der Landesbeauftragte auch dazu genutzt, durch Mitteilung der direkten Kontaktdaten der Ansprechpartner für kommunale Fragen in seinem Haus zur Verbesserung der Kommunikation zwischen den Datenschutzbeauftragten der Kommunen und ihm beizutragen. Über diesen direkten Weg zu den Datenschutzbeauftragten der Kommunen beabsichtigt der Landesbeauftragte künftig wichtige Informationen den Datenschutzbeauftragten der Kommunen direkt zu übermitteln.

Im Ergebnis konnte positiv festgestellt werden, dass alle Kommunen im Land Sachsen-Anhalt ihrer Pflicht zur Benennung eines Datenschutzbeauftragten nachgekommen sind.

15.3 Kommunales Online-Portal „Sag’s uns einfach“

Viele Kommunen binden in ihr Webangebot die auf Landesebene zur kommunalen Nutzung bereitgestellte Plattform „Sag’s uns einfach“ ein.

Hierüber können Bürger kleinere Anliegen, sei es ein Schlagloch, eine defekte Straßenbeleuchtung oder eine illegale Abfallentsorgung, schnell und unkompliziert an ihre Gemeindeverwaltung herantragen.

Die Bürger geben Ihre Hinweise in entsprechende Formulare auf der Plattform ein. Diese sind zunächst nur für die Verwaltung der Kommune sichtbar. Erst nach entsprechender Prüfung und Anpassung durch die Verwaltung erfolgt ein datenschutzkonformer Hinweis auf der Homepage der Kommune, der allgemein sichtbar ist. Die Maßnahmen der Kommune aufgrund des Hinweises werden ebenfalls veröffentlicht. Für die Bürger ist so der Umsetzungsstand ihres Anliegens einfach nachvollziehbar.

Allerdings steckt der „datenschutzrechtliche Teufel“ auch hier gelegentlich im Detail. Bei der Übertragung der Hinweise auf die Homepage der Kommune wurden auch schon Adressdaten von Hinweisgebern mit veröffentlicht.

Die betroffenen Gemeinden haben den mit der Veröffentlichung verbundenen daten-schutzrechtlichen Verstoß bisher stets anerkannt. Im Regelfall sind solche Verstöße auf ein Augenblicksversagen der Mitarbeiter zurückzuführen und konnten für die Zukunft abgestellt werden. Allerdings lassen diese – tatsächlich recht seltenen – Fälle erkennen, dass nur aufmerksame und geschulte Mitarbeiter effektiv auf die Einhaltung der Datenschutzvorgaben hinwirken können. Eine regelmäßige Sensibilisierung zum Thema Datenschutz und auch eine angemessene Kontrolle der durchgeführten Verarbeitung sind daher angezeigt, auch um sicherzustellen, dass die Thematik im Arbeitsalltag präsent bleibt.

15.4 Kommunalverfassungsgesetz

Die Beeinträchtigungen durch die Corona-Pandemie im Jahr 2020 wirkten sich auch auf die Arbeit der kommunalen Vertretungen aus. So hat es sich für die Vertretungen und Gremien schnell als schwierig erwiesen, in Präsenz zu tagen und hierbei die notwendigen Beschlüsse zu fassen.

Dieser Problematik sollte der Entwurf eines „Zweiten Gesetzes zur Änderung des Kommunalverfassungsgesetzes“ dadurch Rechnung tragen, dass Regelungen zu „Verfahren in außergewöhnlichen Notsituationen“ geschaffen werden. Zum einen sollte die Durchführung von Sitzungen der Vertretung und ihrer Ausschüsse mittels Videokonferenztechnik ermöglicht werden, zum anderen sollten die Vertretung und ihre Ausschüsse über Verhandlungsgegenstände im Wege eines schriftlichen oder elektronischen Verfahrens abstimmen können.

Angesichts der technikoffenen Gestaltung der vorgesehenen Neuregelung hat der Landesbeauftragte zunächst allgemeine Hinweise und Empfehlungen erteilt.

Durch Gesetz vom 19. März 2021 wurde das Kommunalverfassungsgesetz um § 56a ergänzt, der das Verfahren für Vertretungen und ihre Ausschüsse u. a. in einer pandemischen Lage regelt.

Für die konkrete Umsetzung der neu geschaffenen Regelung im jeweiligen Einzelfall hat der Landesbeauftragte den Kommunen seine Unterstützung zugesagt.

15.5 Erteilung von Personenstandsurkunden

Aufgrund einer Beschwerde hatte sich der Landesbeauftragte mit einem Sachverhalt aus dem Personenstandsrecht zu befassen. Eine Privatperson hatte Abschriften von Abstammungsurkunden nicht für sich selbst, sondern für ein anderes Familienmitglied beantragt.

Durch die Aushändigung von Auszügen aus dem Personenstandsregister sind aufgrund von dort gespeicherten Hinweisen Sachverhalte bekannt geworden, die der Beschwerdeführer den weiteren Familienmitgliedern nicht bekannt geben wollte. Hingewiesen wird auf Einträge in Registern anderer Standesämter, z. B. Hinweise auf eine Scheidung oder Annahmen an Kindes statt (Adoption).

Der Landesbeauftragte hatte eine umfassende datenschutzrechtliche Stellungnahme abgegeben. Die Aushändigung der Ablichtung selbst war danach rechtmäßig im Sinne des § 62 Abs. 1 Satz 1 PStG. In Bezug auf den Hinweis hätte darüber hinaus jedoch § 1758 BGB Beachtung finden müssen. Gemäß § 1758 BGB dürfen Tatsachen, die geeignet sind, die Annahme eines Kindes und ihre Umstände aufzudecken, ohne Zustimmung des Annehmenden und des Kindes grundsätzlich nicht offenbart oder ausgeforscht werden. Der Landesbeauftragte hat daraufhin erklärt, dass der Hinweis auf Annahme an Kindes statt bei der Erstellung der Ablichtung hätte abgedeckt werden müssen.

Von Interesse ist der Sachverhalt auch deshalb, weil er nunmehr Gegenstand einer zivilrechtlichen Auseinandersetzung um immateriellen Schadensersatz ist. Es handelt sich um den ersten zivilrechtlich verfolgten Fall von immateriellen Schadensersatz mit Kommunalbezug in seinem Zuständigkeitsbereich, der dem Landesbeauftragten seit Geltung der DS-GVO bekannt geworden ist.

15.6 Hundebestandsaufnahme zur Erfassung steuerpflichtiger Hundehalter

In der Vergangenheit hatte der Landesbeauftragte bereits wiederholt auf die datenschutzrechtlichen Probleme bei der Schaffung von Regelungen zur und der Umsetzung einer Hundebestandsaufnahme hingewiesen.

Die satzungsrechtliche Ausgestaltung einer Hundebestandsaufnahme scheitert immer noch am Fehlen einer landesgesetzlichen Ermächtigungsgrundlage und §§ 88 ff. Abgabenordnung lassen keine generellen Ermittlungen nach unbekannten Steuerpflichtigen zu.

Aufgrund einer Beschwerde war der Landesbeauftragte mit einem Sachverhalt befasst, bei der sich eine Gemeinde zur Hundebestandsaufnahme einer Firma als Verwaltungshelfer bedienen wollte. Diese Firma sollte die Hundebestandsaufnahme als freiwillige Befragung ausgestalten.

Die Gemeinde wurde darauf hingewiesen, dass ein Verfahren zur Bestandsaufnahme, bei welchem durch die Feststellung des Vorhandenseins einer Besteuerungsgrundlage steuerrelevante Daten erhoben werden, bereits dem Steuerverwaltungsverfahren zuzurechnen ist. Steuerverwaltungsverfahren sind Teil der Eingriffsverwaltung und können bereits deswegen nicht wirk-

sam einwilligungsbasiert ausgestaltet werden. Das Über- und Unterordnungsverhältnis zwischen Staat und Bürgern steht hierbei bereits konzeptionell der datenschutzrechtlich geforderten Freiwilligkeit einer Einwilligung entgegen.

Der Landesbeauftragte hat die Gemeinde aufgefordert, die Befragung abzubrechen und die im Zusammenhang damit erhobenen Daten zu löschen. Dieser Aufforderung ist die Gemeinde nachgekommen.

17 Videoüberwachung

17.1 Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

Aufgrund der immer weiteren Verbreitung der Videoüberwachung hatte sich der Düsseldorfer Kreis, damals ein Gremium der Datenschutzkonferenz, schon im Jahre 2014 veranlasst gesehen, diese Entwicklung mit einer umfassenden Orientierungshilfe zu begleiten. Nicht erst seit dem Inkrafttreten der DS-GVO bestand an dieser Orientierungshilfe Änderungsbedarf. Für die Datenschutzkonferenz war Anlass zur Überarbeitung nicht zuletzt auch die Tatsache, dass das Risiko als von einer Videoüberwachung Betroffener in seinen Rechten verletzt zu werden, in den letzten Jahren erheblich gestiegen ist. Gründe dafür sind die immer leistungsfähigere und ausgefeiltere Technik, die geringen Anschaffungskosten und schließlich ihre enorme Verbreitung. Selbst in den Non-Food-Bereichen von Lebensmitteldiscountern werden zuweilen Überwachungskameras angeboten.

Die Datenschutzkonferenz hat deshalb die Orientierungshilfe umfassend überarbeitet und dabei die Leitlinien 3/2019 des EDSA zur Verarbeitung personenbezogener Daten durch Videogeräte[42] berücksichtigt. Neu hinzugekommen sind die Abschnitte zur Videoüberwachung in der Nachbarschaft und zur datenschutzrechtlichen Bewertung von Tür- und Klingelkameras, Drohnen und Wildkameras sowie von Dashcams.

Durch die Orientierungshilfe erhalten Verantwortliche und betroffene Personen ausführliche Informationen über die Voraussetzungen für eine datenschutzgerechte Videoüberwachung in den unterschiedlichsten Bereichen und über die Betroffenenrechte. Als Schlusskapitel enthält die Orientierungshilfe für Betreiber eine Checkliste mit den wichtigsten Prüfungspunkten im Vorfeld einer Videoüberwachung. Als Anhang finden sich Muster für Hinweisschilder, die es den Verantwortlichen erleichtern, den Transparenzpflichten gem. Art. 12 ff. DS-GVO nachzukommen.

Die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ ist auf der Homepage des Landesbeauftragten veröffentlicht.[43]

17.2 Videoüberwachung im Nachbarschaftsbereich

Ein erheblicher Teil der den Landesbeauftragten erreichenden Beschwerden betrifft Fälle, in denen Beschwerdeführer eine Videoüberwachung im nachbarschaftlichen Bereich rügen.

Mitunter wird dem Landesbeauftragten von den Betreibern einer Videoanlage entgegengehalten, die Videoüberwachung, die von Privatgrundstücken ausgehe, sei Privatsache. Die Vorgaben der DS-GVO sind jedoch nur dann nicht anwendbar, wenn die mit der Videoüberwachung einhergehende Verarbeitung personenbezogener Daten zur Ausübung ausschließlich

persönlicher oder familiärer Tätigkeiten erfolgt, Art. 2 Abs. 2 lit. c DS-GVO. Diese sogenannte „Haushaltsausnahme“ muss jedoch nach der Rechtsprechung des EuGH gerade im Bereich der Videoüberwachung eng ausgelegt werden. Sie greift z. B. nicht, wenn Aufnahmen des eigenen Grundstücks im Internet veröffentlicht werden und Dritte darauf erkennbar sind. Auch wenn die Videoüberwachung nur teilweise einen öffentlich zugänglichen Raum erfasst und dem Zweck des Schutzes des Eigentums, der Gesundheit und des Lebens der Besitzer des Hauses dient, ist die DS-GVO anwendbar.[44]

Rechtsgrundlage auch für die Videoüberwachung im nachbarschaftlichen Bereich ist Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Daraus folgt, dass die Videoüberwachung nur zulässig ist, soweit sie zur Wahrnehmung berechtigter Interessen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der Nachbarn, Passanten oder anderer betroffener Personen überwiegen. Der Landesbeauftragte wies in zahlreichen Fällen auf den Grundsatz der Datenminimierung hin, der verlangt, den Erfassungsbereich auf das für den jeweiligen Zweck erforderliche Maß zu beschränken. Insbesondere die Erfassung von Nachbargrundstücken ist daher regelmäßig unzulässig.

Vor diesem Hintergrund hat der Landesbeauftragte im Berichtszeitraum eine Handreichung zur „Videoüberwachung auf Privatgrundstücken und in der Nachbarschaft“ erarbeitet. Diese gibt einen Überblick über den bei der Beschwerdebearbeitung anzulegenden Prüfmaßstab. Sie macht aber auch deutlich, dass der Landesbeauftragte zwar die Videoüberwachung beschränken, nicht aber den Abbau einer Kamera verlangen kann. Auch kann er zur Kontrolle der Videoüberwachung keine Privaträume betreten. Daher verweist die Handreichung auch auf die zivilrechtlichen Möglichkeiten, gegen eine (vermeintliche) Videoüberwachung vorzugehen.

Die Handreichung ist auf der Internetseite des Landesbeauftragten veröffentlicht.[45]

17.3 Datenschutzgerechter Einsatz von Drohnen

„Drohne“ ist der umgangssprachliche Begriff für ein Luftfahrzeug, das ohne eine an Bord befindliche Besatzung automatisiert oder durch einen Menschen über eine Fernsteuerung betrieben und navigiert werden kann. In der europäischen Rechtsordnung wird ein unbemanntes Luftfahrzeug, einschließlich der Ausrüstung für seine Fernsteuerung, als unmanned aircraft system (UAS) bezeichnet. Seit der letzten Befassung des Landesbeauftragten mit dem Thema Drohnen im XII. Tätigkeitsbericht (Nr. 15.2.12) änderte sich die Rechtslage.

Die Fernpiloten der Fluggeräte, die über Kameras verfügen, haben nicht nur luftverkehrsrechtliche, sondern auch datenschutzrechtliche Vorschriften zu beachten. Letzteres gilt insbesondere deshalb, weil aus der Luft Bereiche überwacht werden könnten, in denen sich betroffene Personen sehr ungezwungen verhalten, weil sie sich vor einer Überwachung mit technischen Mitteln geschützt wähnen. Dazu gehören z. B. private Gärten, Terrassen, Freibäder, Strände etc. Durch die Beobachtung dieser Bereiche mit einer Kamera kommt es zur Verarbeitung personenbezogener Daten, wenn Personen erkennbar sind. Diese ist im Anwendungsbereich der DS-GVO nur dann zulässig, wenn die abgebildeten Personen eingewilligt haben oder eine gesetzliche Erlaubnisnorm erfüllt ist, Art. 6 Abs. 1 DS-GVO. Beide Voraussetzungen dürften beim Drohneneinsatz nur in den seltensten Fällen vorliegen.

Hinzu kommt für den datenschutzrechtlich verantwortlichen Drohnenbetreiber die Schwierigkeit, seinen gesetzlichen Informationspflichten nach Art. 12 und 13 DS-GVO nachzukommen. Er hat der betroffenen Person zum Zeitpunkt der Erhebung der Daten in leicht zugänglicher Form eine Reihe von Angaben mitzuteilen, z. B. seinen Namen und seine Kontaktdaten, die Zwecke der Verarbeitung und deren Rechtsgrundlage.

Das Betreiben von Kameradrohnen kann sogar strafrechtlich relevant sein. Nach § 201a Abs. 1 StGB kann mit Geld- oder Freiheitsstrafe bestraft werden, wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt. Nach der Gesetzesbegründung dieser Vorschrift kann auch ein Garten „Raum“ im Sinne dieser Vorschrift sein, nämlich etwa dann, wenn er durch eine hohe, undurchdringliche Hecke oder einen hohen Zaun bzw. eine Mauer gegen Einblick durch unberechtigte Personen geschützt wird (BT-Drs. 15/2466, S. 5). Die Verwirklichung dieses Tatbestands kann zur Einziehung der Kameradrohne führen.

Es ist deshalb dringend empfehlenswert, dass bei der Benutzung der Kameradrohne auf die Erfassung personenbezogener Daten betroffener Personen, die sich nicht damit einverstanden erklärt haben, und generell auf die Erfassung von Privatgrundstücken verzichtet wird.

Die Datenschutzkonferenz hat sich in einem Positionspapier[46] (Stand 16. Januar 2019) zur Nutzung von Kameradrohnen durch nichtöffentliche Stellen deutlich geäußert.

Seit dem 31. Dezember 2020 benötigen Piloten von Kameradrohnen ab einem Drohnengewicht von 250 Gramm einen Kompetenznachweis der Europäischen Agentur für Flugsicherheit. Diesen Kompetenznachweis, gemeinhin bezeichnet als kleiner Drohnenführerschein, stellt das Luftfahrt-Bundesamt nach dem erfolgreichen Abschluss eines Online-Trainings und einer Online-Theorieprüfung aus. Er bestätigt dem Inhaber, dass eine ausreichende Kompetenz für das Steuern einer Drohne im öffentlichen Bereich in den Themen Flugsicherheit/Luftraumbeschränkungen, Luftsicherheit, Luftrecht, menschliches Leistungsvermögen, Betriebsverfahren, allgemeine Kenntnisse zur Drohne und nicht zuletzt zu Privatsphäre und Datenschutz nachgewiesen wurde.

Der Landesbeauftragte erwartet von den Fernpiloten, dass sie die datenschutzrechtlichen Vorgaben beachten.

17.4 Gesichtserkennung mithilfe von Videotechnik

Durch immer leistungsfähigere Hard- und Software, womöglich in Kombination mit Künstlicher Intelligenz, rückt die automatisierte Erkennung von Personen auf Fotografien oder in Videodatenströmen datenschutzrechtlich in den Fokus. Doch nicht nur bei umfassend begleiteten Großprojekten zur Gesichtserkennung, wie z. B. an einem Berliner Bahnhof, spielt die Technik eine Rolle. In seinem XIII./XIV. Tätigkeitsbericht (Nr. 14.1.4) hatte sich der Landesbeauftragte mit Gesichtserkennungssoftware in Spielbanken befasst. Die den Kunden der Spielbank angebotene erleichterte und schnellere Einlasskontrolle durch eine Gesichtserkennung beruhte hier auf einer wirksamen datenschutzrechtlichen Einwilligung und war damit zulässig.

Dem Landesbeauftragten ist bekannt geworden, dass Arbeitgeber offenbar auf Fotografien der Gesichter seiner Beschäftigten basierende biometriegestützte Zugangskontrollen zum Unternehmensgebäude implementieren. Das Verfahren basierte ebenfalls auf einer Einwilligung nach Art. 7 DS-GVO. Die Einwilligung ist aber gerade im Arbeitsverhältnis nur dann wirksam, wenn sie freiwillig erfolgt. Bei der Beurteilung der Freiwilligkeit sind die im Beschäftigungsverhältnis bestehende Abhängigkeit sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Eine Einwilligung zur Verarbeitung biometrischer Daten im Rahmen der Zugangskontrolle im Arbeitsverhältnis kann daher regelmäßig nur dann wirksam sein, wenn der Zugang auch ohne die Verarbeitung biometrischer Daten möglich ist.

Es sind aber auch andere Konstellationen denkbar, bei denen mit Videoüberwachung öffentlich zugänglicher Bereiche erhobene Daten nach biometrischen Informationen ausgewertet werden. Das gelänge jedermann z. B. mithilfe von im Internet erhältlicher Bilderverwaltungssoftware. Eine Sammlung von Fotografien wird durch die Software in wenigen Augenblicken automatisch nach Gesichtern durchsucht. Die gefundenen Aufnahmen einer bestimmten Person könnten dann gruppiert angezeigt werden. So könnte nachträglich einfach festgestellt werden, wann diese Person sich im Aufnahmebereich einer Überwachungskamera aufhielt.

Das Szenario einer so genutzten Gesichtserkennung stellt jedenfalls einen intensiven Eingriff in die Persönlichkeitsrechte einer möglicherweise großen Zahl von Betroffenen dar, für das eine hinreichende Rechtsgrundlage zurzeit schlicht nicht existiert. Die Nutzung einer so genutzten Gesichtserkennungssoftware wäre im Anwendungsbereich der DS-GVO damit keinesfalls zulässig und folglich rechtswidrig. Deswegen – und aufgrund der Fehlerquote – empfiehlt der Landesbeauftragte dringend, auf eine Videoüberwachung im Verbund mit einer Gesichtserkennung im öffentlichen Raum gänzlich zu verzichten.

Auch die Datenschutzkonferenz hatte bei ihrer 93. Sitzung am 29. und 30. März 2017 in Göttingen in der Entschließung „Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken“ (s. XIII./XIV. Tätigkeitsbericht, Anlage 16) festgestellt, dass der Einsatz von Videokameras mit biometrischer Gesichtserkennung die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören kann, da es kaum möglich sei, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

18. – 20. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz Für den Zeitraum vom 1. Januar 2021 bis 31. Dezember 2023

2021

3 Technik und Organisation

3.5 Informationssicherheit (AG InfoSic Land)

Die AG InfoSic ist eine Arbeitsgruppe des IT-Planungsrats, die sich mit der Informationssicherheit in der öffentlichen Verwaltung befasst. Sie unterstützt den IT-Planungsrat in Fragen der IT-Sicherheit und fördert die Zusammenarbeit zwischen Bund, Ländern und Kommunen. Auf Landesebene gibt es die AG InfoSic (Land). Diese befasst sich ebenfalls mit dem Thema Informationssicherheit und ergänzt die Aktivitäten der AG InfoSic des IT-Planungsrats und trägt dazu bei, die Informationssicherheit in der öffentlichen Verwaltung in Sachsen-Anhalt

umfassend zu stärken. Sie fördert die Zusammenarbeit zwischen verschiedenen Akteuren, darunter Landesbehörden, Kommunen und IT-Dienstleistern und entwickelt und koordiniert konkrete Maßnahmen zur Verbesserung der Informationssicherheit.

Die Mitglieder der Arbeitsgruppe Informationssicherheit (AG InfoSic) Sachsen-Anhalt sind im Wesentlichen die Informationssicherheitsbeauftragten (ISB) der obersten Landesbehörden unter Leitung des Informationssicherheitsbeauftragten des Landes (CISO). Als Teil des Informations-Sicherheits-Management-Systems (ISMS) des Landes obliegt ihr eine wichtige Schlüsselrolle bei der Umsetzung einer einheitlichen und effizienten Informationssicherheitsstrategie im Land. Die AG InfoSic (Land) als ein Arbeitsgremium mit immer mehr Aufgaben und stetig steigendem Arbeitsaufwand hat sich im Berichtszeitraum eine Geschäftsordnung gegeben, um Sitzungen schnell und geregelt durchführen zu können. Diese regelt die wesentlichen Aspekte der Zusammenarbeit im Gremium. Alle Beschlüsse werden in der AG diskutiert, abgestimmt und abschließend beschlossen, wobei die Wirkung primär intern bleibt. Die Treffen fanden im Berichtsjahr ausschließlich virtuell statt.

Die Landesregierung von Sachsen-Anhalt hat zum 16. September 2021 das Ministerium für Infrastruktur und Digitales des Landes Sachsen-Anhalt (MID) gegründet. Ministerin wurde Dr. Lydia Hüskens. Das MID übernahm das Digitalressort vom Ministerium für Wirtschaft, Tourismus, Landwirtschaft und Forsten (MW) sowie die Zuständigkeit für die Informationssicherheit vom Ministerium der Finanzen (MF). Diese Zusammenführung markierte einen wichtigen Schritt zur Stärkung der Digitalisierung in Sachsen-Anhalt. Unter dem MID wurde eine stärkere Fokussierung auf digitale Themen und IT-Sicherheit möglich.

Die AG InfoSic (Land) wechselte im Zuge der Umstrukturierung ebenfalls vom MF zum MID.

Kurz nach der Regierungsbildung übernahm Staatssekretär Bernd Schlömer die Aufgabe des Beauftragten der Landesregierung für Informations- und Kommunikationstechnologie (CIO). Herr Schlömer sah in der Informationssicherheit eine große Herausforderung und nahm in seiner Funktion als CIO als Gast teil. Die ISB der Ressorts übergaben dem CIO ein Positionspapier, in welchem die Schwerpunkte für die nächsten Aufgaben dargestellt wurden.

Der IT-Kooperationsrat beschloss die Einrichtung einer Unterarbeitsgruppe der AG In-foSic unter der Leitung des MF mit dem Ziel der Einbindung der Kommunen in das ISMS des Landes. Die UAG soll die Zusammenarbeit von Land und Kommunen im Bereich der Informationssicherheit mit dem Schwerpunkt der Entwicklung einer Lösung zum schnellen Informationsaustausch von Warn- und Informationsmeldungen zu Sicherheitslücken sowie bei Sicherheitsvorfällen verbessern.

Im XVII. Tätigkeitsbericht (Kapitel 6.13) wurde über das Inkrafttreten der Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalt (LISL LSA, Informationssicherheitsleitlinie) des Landes und die damit einhergehende beginnende Erstellung belastbarer IT-Sicherheitsrichtlinien (ISRL) berichtet. Die ersten ISRL, die Passwort- und die Telearbeits-RL, befanden sich bereits auf der Zielgeraden und wurden nach Einarbeitung offener Rückmeldungen zügig vollendet. Die ISRL zum „Umgang mit Sicherheitsvorfällen“ wurde finalisiert, Umsetzungshinweise zu den Anforderungen ausgearbeitet. Weitere Arbeiten erfolgten – teils in UAGs – an ISRL und Prozessbeschreibungen betreffend das Dokumentenmanagement, Korrektur- und Vorbeugemaßnahmen, Organisation und Personal, Berichtswesen, Risikomanagement und dem landesweiten Sicherheitsprozess.

Intensiv wurde in der UAG „BITS“ am Behörden-IT-Sicherheitstraining gearbeitet. Ziel war die Anpassung vorhandener Inhalte an die Bedürfnisse der Landesverwaltung. BITS ist ein kostenloses webbasiertes Online-Training, das Beschäftigte in Behörden und öffentlichen Einrichtungen für die Gefahren der IT-Nutzung sensibilisiert. Es vermittelt grundlegende Kenntnisse und Verhaltensweisen, um die Informationssicherheit zu erhöhen und sensible Daten zu schützen.

Im Berichtszeitraum erfolgte ein Cyberangriff auf den Landkreis Anhalt-Bitterfeld. Eine Ransomware legte die IT-Infrastruktur des Landkreises durch Verschlüsselung von Dateien lahm. Der Landkreis rief den Katastrophenfall aus, um schnellere Hilfe von anderen Behörden zu erhalten. Das war das erste Mal, dass in Deutschland aufgrund eines Cyberangriffes der Katastrophenfall ausgerufen wurde. Der CISO unterstützte vor Ort. Es entstand ein erheblicher finanzieller Schaden, hauptsächlich durch die aufgrund von Datenverlusten eingetretene Handlungsunfähigkeit der Verwaltung. Der Vorfall verdeutlichte die Anfälligkeit öffentlicher Verwaltungen für Cyberangriffe und führte zu einem verstärkten Bewusstsein für die Bedeutung von Cybersicherheit in Deutschland. Alle verantwortlichen Stellen sollten aus dem Vorfall lernen, ihre IT-Sicherheitsmaßnahmen und Krisenmanagementpläne auf mögliche Verbesserungen prüfen und diese zügig umsetzen und dauerhaft verbessern.

Bereits im letzten Tätigkeitsbericht wurde darüber informiert, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) Ländern Dienstleistungen anbietet und diese insbesondere bei der Absicherung ihrer IT unterstützen kann. Der Abschluss einer Kooperationsvereinbarung „Zusammenarbeit mit dem BSI auf Bund-Länder Ebene“ wurde angestrebt. Bereits im Jahr 2018 erfolgten erste Gespräche mit dem BSI mit dem Ziel des Abschlusses einer Absichtserklärung. Dem folgte 2019 ein Vorschlag Dataports zu einer Absichtserklärung für eine länderübergreifende Zusammenarbeit mit dem BSI. 2020 erfolgte die Abstimmung einer Absichtserklärung für Sachsen-Anhalt mit dem Verbindungsbüro des BSI. Das Ministerium für Inneres und Sport (MI) erhielt durch die Länderarbeitsgruppe (LAG) Cybersicherheit der IMK den Entwurf einer Kooperationsvereinbarung im Bereich der Cybersicherheit: MI und MF sollten eine gemeinsame Kooperationsvereinbarung für Informations- und Cybersicherheit mit dem BSI für das Land schließen. Nach Diskussionen und rechtlichen Prüfungen wurde nun eine standardisierte Kooperationsvereinbarung im Bereich Cyber- und Informationssicherheit zwischen der LAG Cybersicherheit, der AG InfoSic (Bund) und dem BSI abgestimmt, welche per Umlauf in der AG versandt wurde. Nach landesspezifischen Anpassungen lag sie sodann dem MI zur Stellungnahme vor. Die Unterzeichnung der Kooperationsvereinbarung sollte dann im nächsten Jahr erfolgen.

3.6 Besonderes elektronisches Behördenpostfach

Der Elektronische Rechtsverkehr (ERV) dient dem Austausch elektronischer Dokumente zwischen Behörden, Bürgern und Gerichten. Ein sicherer Austausch allein reichte dazu nicht, notwendig war es auch, dass dieser rechtlich wirksam erfolgt. Bereits ab 2001 wurden u. a. mit dem Formvorschriftenanpassungsgesetz und dem Zustellungsreformgesetz die Vorrausetzungen dafür geschaffen, die Schriftform durch die elektronische Form ersetzen zu können. Durch das Justizkommunikationsgesetz (JKomG) wurden 2005 die rechtlichen Rahmenbedingungen geändert, um den elektronischen Zugang zu Gerichtsakten und den elektronischen Austausch von Dokumenten zu ermöglichen und so Prozessakten elektronisch führen zu können. 2013 folgte das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten, welches die Nutzung elektronischer Kommunikationsmittel im Rechtsverkehr mit den Gerichten verbessert. 2017 folgte dann die Elektronischer-Rechtsverkehr-Verordnung

(ERVV). Sie regelt die technischen Rahmenbedingungen für den elektronischen Rechtsverkehr sowie die Nutzung des besonderen elektronischen Behördenpostfachs. Es folgte im selben Jahr das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs. Der Name ist hier Programm. Damit waren 2018 die Weichen für die elektronische Übertragung von Dokumenten unter Wahrung der Schriftformerfordernis via Elektronischem Gerichts-und Verwaltungs-Postfach (EGVP) gemäß § 130a Abs. 4 ZPO per sicherem Übermittlungsweg gestellt. Für Behörden und juristische Personen des öffentlichen Rechts bot sich dafür die Einrichtung eines besonderen elektronischen Behördenpostfachs (beBPo) an. Der Landesbeauftragte war ein „Early Adopter". Die Nutzungshäufigkeit steigt seitdem stetig an.

In seinem XVII. Tätigkeitsbericht für das Jahr 2020 (Nr. 2.4) hatte der Landesbeauftragte noch die Absicht geäußert, zusätzlich zum elektronischen Behördenpostfach auch ein De-Mail-Konto zur Kommunikation mit Bürgerinnen und Bürgern einzurichten. Dazu sollte nur noch der Abschluss eines Rahmenvertrages mit einem Dienstleister durch das Ministerium der Finanzen abgewartet werden. Das hat sich mittlerweile von selbst erledigt: Offenbar gab es zu geringe Nutzerzahlen. Im Berichtszeitraum kündigte die Telekom als großer De-Mail-Anbieter an, dass der Dienst eingestellt werden sollte. Auch der Bundesrechnungshof sah das so und meinte, das Bundesinnenministerium (BMI) sei dabei gescheitert, De-Mail „als elektronisches Pendant zur Briefpost in der Bundesverwaltung zu etablieren". Der Landesbeauftragte sah daher von einer Einführung eines De-Mail-Zugangs ab.

De-Mail sollte einer „sicheren, vertraulichen und nachweisbaren" Kommunikation für jedermann im Internet dienen (§ 1 Abs. 1 De-Mail-Gesetz). Aber schnell war klar, dass die Kosten für die Nutzung zwar niedriger als bei der Papierpost, aber dennoch hoch genug waren, um eine umfassende Nutzung zu untergraben. Neben den Gebühren, sorgten dann auch der komplizierte Anmeldeprozess (Identifizierung), fehlende Verbreitung (der Empfänger musste ebenfalls einen Account haben), Konkurrenz (PGP und S/MIME), fehlende Integration in behördliche Kommunikation und Fachverfahren und zu wenig Förderung durch den Staat für fehlende Nutzerzahlen. Bundeseinrichtungen sollten bereits seit 2015 und Gerichte seit 2018 De-Mail nutzen, die Realität sah oft anders aus: Totalverweigerung und Ignoranz. Städte und Gemeinden waren nur optional dabei.

7 Schulwesen

7.2 Ausstattung von Schulen mit digitalen Geräten

Wie sich Veröffentlichungen entnehmen ließ, u. a. den Antworten der Landesregierung auf Kleine Anfragen (z. B. LT-Drs. 8/127, LT-Drs. 8/194), schritt die Umsetzung des DigitalPakts Schule mit großen Schritten voran. Digitale Endgeräte für Lehrkräfte und Schülerinnen und Schüler stehen in erheblichem Umfang zur Verfügung und sind vielfach bereits verteilt bzw. werden kurzfristig zur Verfügung gestellt. Dabei sollte bedacht werden, dass die Nutzung der Endgeräte mit gängiger außereuropäischer (außerhalb des Anwendungsbereichs der DS-GVO) Software, insbesondere Microsoft Office 365, datenschutzrechtliche Fragen aufwirft. Eine gewisse Sensibilität hierfür ist in den Schulen bereits vorhanden. Den Landesbeauftragten erreichten im Berichtszeitraum einige Anfragen. Leider ist es schon aus Kapazitätsgründen nicht möglich, individuelle Beratungen und Hilfen zur Installation anzubieten. Der Landesbeauftragte hat daher die Schulen zunächst auf die gesetzlich bestimmte eigene Verantwortung hingewiesen.

Sie tragen für die Verarbeitung der Daten der Schülerinnen und Schüler die Verantwortung, sie müssen die datenschutzrechtlichen Vorgaben einhalten. Bei Schülerinnen und Schülern handelt es sich vielfach um Minderjährige, die eines besonderen Schutzes bedürfen. Die DS-GVO betont diesen Schutzbedarf u. a. in den Erwägungsgründen 38, 58, 65, 71 und 75 DS-GVO sowie Art. 8, Art. 12 Abs. 1, Art. 57 Abs. 1 lit. b DS-GVO. Weiter hat der Landesbeauftragte auf die wesentlichen problematischen Fragestellungen hingewiesen, die die Schulen zu klären haben, um in der konkreten Umsetzung vor Ort eine rechtskonforme Verarbeitung der Schülerdaten zu erreichen.

Grundsätzlich ist die Schule befugt, Daten der Schülerinnen und Schüler und Eltern auf Basis des Schulgesetzes insoweit zu verarbeiten, wie dies für die Erfüllung des Bildungs- und Erziehungsauftrags erforderlich ist. Dabei ist es möglich, sich automatisierter Verarbeitung, auch in Auftragsverarbeitung bei einem Dienstleister, zu bedienen. Die Anforderungen der DS-GVO müssen dabei eingehalten werden. Insbesondere sind die Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO (Transparenz, Vertraulichkeit, Datenminimierung, Erforderlichkeit und Zweckbindung) sowie die Anforderungen an technische und organisatorische Vorgaben (Art. 5 Abs. 1 lit. f, Art. 25 Abs. 1, Art. 32 DS-GVO) zu beachten. Dies muss die Schule in eigener Verantwortung prüfen und die Einbindung von geeigneten IT-Dienstleistern datenschutzkonform gewährleisten. Bei einer Umsetzung ist auch zu beachten, dass Softwareprodukte im Auslieferungszustand oft nicht umfassend den Geboten der datenschutzfreundlichen Voreinstellungen (Art. 25 Abs. 2 DS-GVO) entsprechen, sodass insoweit eine Nachjustierung erforderlich werden kann.

Bei einer Verlagerung von personenbezogenen Daten zu einem Dienstleister bedarf es einer Rechtsgrundlage. Ist eine Übermittlung angedacht, wäre grundsätzlich die Regelung des § 84a SchulG LSA einschlägig. Die Übermittlung von personenbezogenen Daten an nichtöffentliche Stellen ist aber sehr stark eingeschränkt (§ 84a Abs. 8 Satz 2 SchulG LSA) und dürfte zudem an der fehlenden Erforderlichkeit scheitern. Übermittlungen von Schülerdaten an nichtöffentliche IT-Dienstleister kommen daher grundsätzlich nicht in Betracht. Es verbleibt deshalb in der Regel nur die Möglichkeit eine derartige Inanspruchnahme eines Dienstleisters im Wege der Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO vertraglich auszugestalten.

Vor dem Hintergrund der regelmäßigen Unzulässigkeit der Datenübermittlung an einen privaten Dritten ist auch stets zu prüfen, ob über die inhaltliche Nutzung der Softwareprodukte hinaus auf andere Weise Daten übermittelt werden, sei es durch Nutzung anfallender Daten durch den Dienstanbieter für eigene Zwecke oder durch die Notwendigkeit einer persönlichen Anmeldung der Nutzer. Zu betrachten ist weiter, welche der verschiedenen cloudbasierten Online Dienste des Anbieters Verwendung finden sollen, bei denen personenbezogene Datenflüsse entstehen können. Auch bei Standardanwendungen wie Schreib- und E-Mailprogrammen (bei Microsoft Word und Outlook) kommt die Sammlung personenbeziehbarer Daten des Anwenders in Betracht, die über Inhalte hinausgeht (z. B. bezüglich der Verwendung der Rücktaste oder der Worte vor und nach dem in der Rechtschreibüberprüfung geprüften Wort). Durch eine Vielzahl von erfassten Ereignissen können Profile entstehen. Unter anderem können Daten über das genutzte Endgerät, die Adresse des Internetzugangs und Standortdaten personalisiert werden. Dabei ist zu berücksichtigen, dass von einem Personenbezug einer Information bereits ausgegangen werden muss, wenn eine Identifizierbarkeit gegeben ist (siehe dazu Erwägungsgrund 26 DS-GVO). Einfache Pseudonymisierungen als Sicherungsmaßnahmen wären daher gegebenenfalls nicht ausreichend, soweit die Information durch eine Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können.

Schulen obliegt es, neben der Einhaltung der bereichsspezifischen Vorschriften zur konkreten Datenverarbeitung (§ 84a ff. SchulG LSA) die europarechtlichen Grundsätze (Art. 5 DS-GVO) und Vorgaben, insbesondere in technischer und organisatorischer Hinsicht (Art. 5 Abs. 1 lit. f, Art. 25, Art. 32 DS-GVO) einzuhalten und die Einhaltung auch nachzuweisen (Art. 5 Abs. 2 DS-GVO). Sie müssen daher gem. Art. 32 Abs. 1 DS-GVO Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Kategorien personenbezogener Daten feststellen und basierend darauf die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener natürlicher Personen beurteilen. Sodann sind geeignete technische und organisatorisch Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Für die Auftragsverarbeitung sind zudem die Voraussetzungen nach Art. 28 DS-GVO zu beachten. Der Verantwortliche hat danach bei der Auswahl eines Auftragsverarbeiters darauf zu achten, dass letzterer hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen getroffen wurden und so durchgeführt werden, dass die Verarbeitung dauerhaft im Einklang mit den Anforderungen der DS-GVO erfolgt und damit der Schutz der Rechte der betroffenen Schülerinnen und Schüler gewährleistet ist.

Es erscheint mehr als fraglich, ob es Schulen gelingen kann, eine datenschutzrechts-konforme und damit zulässige Verarbeitung von Schülerdaten bei Nutzung außereuropäischer Software nachzuweisen. Wiederholt haben Beratungen und Prüfungen von Datenschutzaufsichtsbeschwerden erhebliche Bedenken in Bezug auf einen datenschutzkonformen Betrieb von IT-Diensten hervorgebracht. Abschließende Einschätzungen werden zudem dadurch erschwert, dass Produkte unangekündigt geändert werden können und auch die Vertragsbedingungen möglichen Änderungen unterliegen. Infolge mangelnder Transparenz, fehlender Konfigurationsmöglichkeiten und auch offener rechtlicher Fragen bleiben vielfach erheblich Zweifel.

Bisher standen für die Organisation und Gewährleistung eines digitalisierten Betriebs von Schulorganisation und Unterricht gerade in der besonderen Situation der Corona-Pandemie nur wenige Angebote zur Verfügung. Ob trotz vielfältiger Fragen und Bedenken auch weiter davon ausgegangen werden kann, dass Produktnutzungen als alternativlos und damit noch vertretbar anzusehen sind, erscheint fraglich.

9 Sozialwesen

9.1 Sozialdaten auf Briefumschlägen

Ein Beschwerdeführer teilte dem Landesbeauftragten mit, vom Jugendamt eines Landkreises Briefe erhalten zu haben, auf deren Umschlägen handschriftlich neben dem Aktenzeichen und dem vollständigen Namen seines Kindes auch die Bezeichnung des Inhaltes („Neuberechnung UH“ und „Auskunft+Verzug“) vermerkt war. Damit sind von außen Sozialdaten sichtbar, die Dritte zur Kenntnis nehmen können.

In einer ersten Stellungnahme teilte der Landkreis mit, dass die Angaben auf den Umschlägen zumindest in Teilen zwingend erforderlich seien. Um zu beweisen, was tatsächlich zugestellt wurde, sei beispielsweise nur das Aktenzeichen auf dem zuzustellenden Schriftstück nicht ausreichend. Hierfür sei eine Konkretisierung erforderlich, sodass die Umschläge darüber hinaus mit der Kurzbezeichnung der Inhalte beschriftet werden müssten. Die Angabe des Kindesnamens sei verzichtbar, da ein Bezug über das Aktenzeichen möglich sei.

Aber auch dieses modifizierte Verfahren begegnete aus hiesiger Sicht weiterhin erheblichen datenschutzrechtlichen Bedenken. Durch die Angabe der Kurzbezeichnung des Inhaltes erfolgte weiterhin eine Übermittlung personenbezogener Daten an Dritte. Eine Rechtsgrundlage hierfür war nicht gegeben. Darüber hinaus war zweifelhaft, inwieweit durch diese Maßnahme konkret nachweisbar sein soll, welcher Inhalt sich im Umschlag befindet. Die Beschriftung des Umschlages mit der Kurzbezeichnung des Inhaltes beweist nicht, dass sich dieser auch im Umschlag befindet. Aus hiesiger Sicht kommt einem entsprechenden Vermerk des Verwaltungsmitarbeiters auf dem Entwurf, der das Schriftstück in den Umschlag steckt, das gleiche Beweispotential zu und bewirkt keine Datenübermittlung an Dritte.

Aufgrund dieses Vorschlags hat der Landkreis sein Verfahren umgestellt. Nunmehr wird auf dem Briefumschlag lediglich das Aktenzeichen vermerkt. Auf der Postzustellungsurkunde wird ein intern festgelegter Code notiert, der intern einen eindeutigen Bezug zum versandten Schreiben herleiten kann.

Eine Übermittlung personenbezogener Daten an Dritte durch Vermerke auf den Briefumschlägen erfolgt auf diese Weise nicht mehr.

Von außen auf Briefumschlägen notierte personenbezogene Sozialdaten führen zu einer unzulässigen Datenübermittlung an Dritte und müssen daher unterbleiben.

9.2 Datenschutz in Kindertagesstätten

Sowohl das Personal von Kitas als auch Eltern haben in der Vergangenheit zahlreiche Fragen an den Landesbeauftragten gestellt oder um konkrete Informationen zur Verarbeitung personenbezogener Daten von in Kitas betreuten Kindern gebeten. Vor diesem Hintergrund hat der Landesbeauftragte die Antworten zu den häufigsten Fragen in den „Hinweisen zum Datenschutz in der Kindertagesstätte“ auf seiner Homepage zusammengestellt und auf seiner Homepage veröffentlicht.[24]

10 Beschäftigtendatenschutz

10.1 Homeoffice

Zunehmend verlagert sich die Verarbeitung von personenbezogenen Daten aus den Büros und Dienststellen in den häuslichen Bereich (siehe hierzu u. a. den Bericht zur Telearbeit in der Landesverwaltung Sachsen-Anhalt, LT-Drs. 7/5474). Infolge der Corona-Pandemie und der verbindlichen Vorgaben für Arbeitgeber, Heimarbeit anzubieten (§ 28b Abs. 4 IfSG), hat die Anzahl der Beschäftigten im Homeoffice nochmals erheblich zugenommen. Dazu wird der häusliche Arbeitsplatz mittels Informations- und Kommunikationstechnologie (IKT) mit dem Büro/der Dienststelle verbunden. Gelegentlich erfolgt auch ortsunabhängiges mobiles Arbeiten unter Einsatz von IKT. Da die Heimarbeit in vielen Fällen mit der Verarbeitung personenbezogener Daten verbunden ist, müssen auch im Hinblick auf den Datenschutz besondere Anforderungen bedacht werden. Durch die Auslagerung der Verarbeitung in den häuslichen oder mobilen Bereich stehen dabei nicht mehr die Sicherheitsvorkehrungen zur Verfügung, wie im betrieblichen/dienstlichen Bereich, sodass eine höhere Gefährdung der Sicherheit der Datenverarbeitung gegeben ist. Der Arbeitgeber/die Dienststelle bleibt aber der für die Einhaltung

der datenschutzrechtlichen Anforderungen Verantwortliche(r) nach Art. 4 Nr. 7 DS-GVO, sodass ergänzende technische und organisatorische Maßnahmen (Art. 32 DS-GVO) getroffen werden müssen. Auch besondere Situationen, wie in der Corona-Pandemie, suspendieren nicht von den gesetzlichen Vorgaben, deren Einhaltung gerade in der Krise Stabilität gewährleistet.

Arbeitgeber bzw. Dienststellen müssen sich daher vielen Fragen stellen und viele geänderte bzw. neue Maßnahmen ergreifen, um letztlich auch im Hinblick auf Haftungsrisiken datenschutzkonform zu handeln. Das fängt mit der Prüfung an, ob der Beschäftigte seine Aufgaben ggf. auch ohne oder mit weniger personenbezogenen Daten in Heimarbeit erledigen kann (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit. c DS-GVO). Wenn die Verwendung personenbezogener Daten notwendig ist, sollte der behördliche Datenschutzbeauftragte beteiligt werden. Dieser könnte auch bei der sinnvollen Ausgestaltung der Heimarbeit in Betriebs- oder Dienstvereinbarungen mitgestalten. Weiter erscheint unumgänglich, für die Beschäftigten einen Handlungsleitfaden herauszugeben und sie besonders zu sensibilisieren, sowie ein Sicherheitskonzept zu erstellen (allgemeine und spezifische Maßnahmen zur Datensicherheit; Festlegungen, wie z. B. zu Hard- und Softwarekomponenten; Verschlüsselung (Ende-zu- Ende-Verschlüsselung, VPN), aktuelle Protokolle, Sicherheitskopien). Besondere Bedeutung genießen die Aspekte der Sicherheit der Kommunikation und des Transfers der zu verarbeitenden Daten (Netzanbindung oder lokale Speichermedien; kein Liegenlassen von Unterlagen oder PCs im Pkw auf dem Supermarktparkplatz). Den Gefahren des Zugriffs unbefugter Dritter auf die Daten ist zu begegnen. Für den häuslichen Bereich sind auch Sicherungsvorgaben geboten (z. B. Zugangstüren, Schrank, verschließbare Aktentasche, keine „Vernichtung“ im heimischen Papierkorb). Eindeutig zu bevorzugen ist der Einsatz professionell administrierter Technik, die in hohen Maße Datensicherheit, z. B. in Bezug auf Firewall, Virenschutz, Malwareschutz, sichere Verbindungen und Verschlüsselungen gewährleistet. Private Geräte sind oft mit Anwendungen versehen, die sich bei der Installation umfassende Zugriffsrechte haben gewähren lassen. Mit deren Nutzung im privaten Umfeld erhöht sich auch die Gefahr in Bezug auf Schadsoftware. Sind gute Sicherheitsvorkehrungen getroffen, ist zu bedenken, dass sie an Wert verlieren, wenn ihre Einhaltung nicht in angemessenem Umfang geprüft wird. Allerdings darf dabei aus Sicht des Beschäftigtendatenschutzes kein unverhältnismäßiger Überwachungsdruck entstehen. In Bezug auf die genutzten Geräte sind verschiedene Sicherheitsaspekte zu bedenken und zu regeln. Dies gilt u. a. für die sichere und hinreichend passwortgeschützte Anbindung an das dienstliche/betriebliche System. Auch das „Drumherum“ sollte bedacht und gestaltet werden (Verbindung mit privaten Geräten, Ausdruck am heimischen Drucker, private Nutzung dienstlicher Geräte etc.). Soweit mobiles Arbeiten gestattet ist, sind auch insoweit die Besonderheiten auszugestalten (z. B. die Nutzung bzw. das Ausschalten von Verbindungstechnologien (Bluetooth, NFC, öffentliche W-LAN-Hotspots) des genutzten Gerätes. Letztlich muss man sich als Verantwortlicher auch die Frage stellen, ob die Auftragsverarbeiter, die man ggf. eingesetzt hat, Mitarbeiter in Heimarbeit beschäftigen und dabei den gebotenen Sicherheitsanforderungen gerecht werden.

Zur Unterstützung der Arbeitgeber und Dienststellen in Bezug auf die hier nur auszugsweise angesprochenen Fragestellungen, die notwendig mit der Ausgestaltung der Heimarbeit verbunden sind, hat der Landesbeauftragte im Berichtszeitraum umfängliche „Hinweise zum Homeoffice in Behörden und Betrieben“ nebst einer Checkliste zur vereinfachten Umsetzung im Infopaket Homeoffice auf seiner Homepage veröffentlicht.[25]

10.2 Digitalisierung von Versorgungsakten

Eine Anfrage an den Landesbeauftragten galt der Digitalisierung von Versorgungsakten von Beamten durch externe Dienstleister. Grundsätzlich sind Auftragsverarbeitungen durch externe Dienstleister auf der Basis von Art. 28 DS-GVO möglich. Die anfragende Stelle nahm aber Bezug auf eine Entscheidung des Oberverwaltungsgerichts Schleswig-Holstein (vom 27. Juli 2016, Az.: 2 MB 11/16, juris), wonach die Auslagerung des Einscannens von Personalakten an einen externen Dienstleister nicht zulässig sei.

Auch wenn die genannte Entscheidung keine bindende Wirkung in Sachsen-Anhalt begründet, hat der Landesbeauftragte im Hinblick auf die vergleichbare Rechtslage die geäußerten Bedenken bestätigt. Die Herausgabe von Personalaktendaten an Dritte ist durch die Regelungen des Beamtenrechts zum Umgang mit Personalakten beschränkt. Insoweit wurde auf § 50 S. 3, 4 BeamtStG (Vertraulichkeit, begrenzte Verwendungszwecke der Personalverwaltung und Personalwirtschaft) sowie auf die engen Vorgaben des Landesbeamtengesetzes verwiesen (in Sachsen-Anhalt §§ 84 ff LBG LSA). Diese spezielle Ausprägung des Schutzes des Persönlichkeitsrechts der Betroffenen (Personalaktengeheimnis) macht eine Verarbeitung auf der Basis einer allgemeinen datenschutzrechtlichen Basis (Art. 28 DS-GVO, Auftragsverarbeitung) unmöglich. Zudem gebietet dies auch der Grundsatz des Vorrangs bereichsspezifischer Regelungen vor allgemeinem Datenschutzrecht. Auch in § 2 Abs. 5 DSAG LSA findet sich die Regelung des Vorrangs bereichsspezifischer Regelungen sowie zum Vorrang von Berufs- oder besonderen Amtsgeheimnissen (wie z. B. Personalaktengeheimnis). Die Datenschutz-Grundverordnung steht dieser beamtenrechtlichen Gestaltung nicht entgegen (siehe Art. 88 Abs. 1 DS-GVO).

11 Kommunales und Meldewesen

11.1 Veröffentlichung in Rats- und Bürgerinformationssystemen

In einer Vielzahl der Kommunen Sachsen-Anhalts werden mittlerweile automatisierte Rats- oder Bürgerinformationssysteme eingesetzt, die es der Verwaltung ermöglichen, den kommunalen Sitzungsdienst effizient zu steuern und es gleichzeitig den ehrenamtlichen Mandatsträgern und den Bürgern ermöglichen, sich zeitnah über die in den kommunalen Gremien zur Beratung oder Beschlussfassung anstehenden Themen zu informieren. So werden vielfach schon nicht nur die Tagesordnung der kommunalen Gremien, sondern auch bereits die zur Beratung und Beschlussfassung anstehenden Vorlagen sowie die Niederschriften der Sitzungen in das einer breiten Öffentlichkeit zugängliche kommunale Internetangebot eingestellt.

Im zurückliegenden Zeitraum erreichten den Landesbeauftragten immer wieder Beschwerden darüber, dass die Kommunen Unterlagen im Rats- und Bürgerinformationssystem veröffentlicht hatten, die personenbezogenen Daten enthielten.

11.1.1 Veröffentlichung von Sitzungsvorlagen

Die Befugnis zur Weitergabe personenbezogener Daten in Sitzungsvorlagen an die Vertretung ergibt sich in den meisten Fällen aus Art. 6 Abs. 1 lit. e und Abs. 3 DS-GVO i. V. m. § 53 Abs. 4 Kommunalverfassungsgesetz des Landes Sachsen-Anhalt (KVG LSA). Danach sind die für die Verhandlung erforderlichen Unterlagen grundsätzlich beizufügen. Von der Übersendung ist abzusehen, wenn das öffentliche Wohl oder berechtigte Interessen Einzelner dem

entgegenstehen. Folglich dürfen der Vertretung personenbezogene Daten – beispielsweise als Anlage zu Beschlussvorlagen – zur Verfügung gestellt werden, soweit dies für die Beschlussvorbereitung oder die Information der Vertretung sowie gegebenenfalls zur späteren Ausführung der Beschlüsse erforderlich ist, es sei denn, das öffentliche Wohl oder berechtigte Interessen Einzelner stehen dem entgegen.

Die Veröffentlichung solcher Sitzungsunterlagen kann sich aus § 28 Abs. 1 KVG LSA ergeben. Danach unterrichtet der Hauptverwaltungsbeamte die betroffenen Einwohnerinnen und Einwohner über die allgemein bedeutsamen Angelegenheiten der Kommune in geeigneter Form. Die Zulässigkeit der gleichzeitigen Veröffentlichung personenbezogener Daten bemisst sich dabei nach dem vorgenannten Grundsatz der Erforderlichkeit zur Information der Einwohnerinnen und Einwohner sowie dem entgegenstehenden öffentlichen Wohl und den berechtigten Interessen Einzelner. Sie ist danach zulässig, sofern ausschließlich die zum Verständnis unbedingt erforderlichen personenbezogenen Daten enthalten sind. Im Einzelfall sind dabei immer die schutzwürdigen Interessen der Betroffenen sorgfältig zu prüfen. Grundsätzlich stellen die Namen betroffener Personen keine Information dar, die für das Verständnis des Sachverhalts erforderlich sind.

Insgesamt wird die Erforderlichkeit, personenbezogene Daten in einem Rats- und Bürgerinformationssystem für die Öffentlichkeit bereitzustellen, nur in wenigen Ausnahmefällen anzuerkennen sein. Bevor Sitzungsunterlagen der Allgemeinheit zur Verfügung gestellt werden, sind personenbezogene Daten deshalb in der Regel zu schwärzen.

11.1.2 Veröffentlichung von Beschlüssen

Aus § 28 Abs. 1 KVG LSA i. V. m. § 52 Abs. 1 und 2 KVG LSA lässt sich ableiten, dass Beschlüsse der Gemeindevertretung zu veröffentlichen sind, soweit nicht im Einzelfall aus Gründen des öffentlichen Wohls oder berechtigter Interessen Einzelner 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 anonymisieren ist, ist aber auch dann erforderlich, wenn Beschlüsse in öffentlicher Sitzung getroffen wurden, ausnahmsweise aber personenbezogene Daten enthalten.

11.1.3 Veröffentlichung von Niederschriften

Entsprechend § 58 Abs. 3 KVG LSA ist die Einsichtnahme in die Niederschriften über die öffentlichen Sitzungen zu gestatten. Das Nähere regelt die Geschäftsordnung. Sofern entsprechende Regelungen in der Geschäftsordnung zur Veröffentlichung von Niederschriften im Rats- und Bürgerinformationssystem getroffen wurden, ergibt sich daraus die Grundlage für eine Veröffentlichung der Niederschriften.

Nach § 58 Abs. 1 KVG LSA muss die Niederschrift einer Sitzung der Gemeindevertretung einen gewissen Mindestinhalt aufweisen – beispielsweise die Namen der Teilnehmenden. Dazu gehören jedoch ausschließlich solche Personen mit einem aktiven Teilnahmerecht im kommunalverfassungsrechtlichen Sinn.

Die Veröffentlichung von Niederschriften mit dem beschriebenen (auch personenbezogenen) Mindestinhalt ist im Hinblick auf die Erforderlichkeit für die Aufgabenerfüllung der Kommune (Beteiligung der Einwohnerinnen und Einwohner nach § 28 Abs. 1 KVG LSA) immer

zulässig. Dazu gehört auch die Zuordnung der Teilnehmenden zu deren Beiträgen und Wortmeldungen. Nur so können die Interessierten das Handeln der Vertretung sowie der Verwaltung verstehen und ihre Wahlentscheidung entsprechend ausrichten.

Weitere personenbezogene Daten können nur aufgenommen werden, wenn dies zur Beteiligung der Einwohnerinnen und Einwohner im Einzelfall erforderlich ist. In den meisten Fällen ist es das nicht. Beispielsweise spielt es keine Rolle, welche Bürger über die genannten, offiziellen Teilnehmenden hinaus an einer Ratssitzung teilgenommen haben. Entsprechende Anwesenheitslisten dürfen in der Regel nicht Inhalt der Niederschrift werden. Auch ist die namentliche Bezeichnung von 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 vielen Fällen hatten es die Gemeinden versäumt, zwischen den Voraussetzungen für die Weiterleitung von personenbezogenen Sitzungsunterlagen an die Vertretung und an die Öffentlichkeit über das Rats- und Bürgerinformationssystem zu unterscheiden. Sie stellten dieselben Dokumente zuerst den Vertretungen und anschließend unverändert der Öffentlichkeit zur Verfügung, ohne zu berücksichtigen, dass für beide Schritte unterschiedliche Voraussetzungen gelten. In den überwiegenden Fällen konnte eine datenschutzgerechte Anonymisierung durch Schwärzung der Unterlagen erfolgen. In Einzelfällen wurden die entsprechenden Unterlagen vollständig aus dem Rats- und Bürgerinformationssystem entfernt, da die jeweiligen Kommunen selbst gar keinen Grund für eine personenbezogene Veröffentlichung sahen.

11.2 Zuständigkeit der behördlichen Datenschutzbeauftragten der Kommunen für die Kommunalvertretungen

Der Landesbeauftragte für den Datenschutz wird regelmäßig mit Anfragen konfrontiert, die die datenschutzrechtliche Verantwortlichkeit eines Gemeinde-, Stadtrates oder Kreistages einschließlich seiner ehrenamtlichen Mitglieder betreffen.

Datenschutzrechtlich Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO ist die Kommune als Gebietskörperschaft des öffentlichen Rechts.

Die datenschutzrechtliche Verantwortlichkeit umfasst daher auch die Tätigkeit des Hauptorgans Gemeinde-, Stadtrat bzw. Kreistag, mithin auch die Verarbeitung personenbezogener Daten durch die Ratsmitglieder.

Die Kontrollpflicht und -befugnis des behördlichen Datenschutzbeauftragten umfasst auch die Tätigkeit der Ratsarbeit. Dies stellte sowohl für die Ratsmitglieder als auch für den Datenschutzbeauftragten selbst manchmal eine überraschende Erkenntnis dar.

11.3 Wahlwerbung

Den Landesbeauftragten für den Datenschutz erreichten im Rahmen der anstehenden Landtagswahl Beschwerden von Bürgern zum Erhalt von persönlich adressierter Wahlwerbung. Die Beschwerdeführer vermuteten einen Datenschutzverstoß durch die jeweilige Partei.

Tatsächlich können Parteien solche Adressdaten rechtskonform von den Meldebehörden abfragen. Dabei gelten allerdings enge datenschutzrechtliche Rahmenbedingungen – und dieser Weitergabe kann bürgerseits widersprochen werden.

Die rechtliche Erlaubnis für personalisierte Wahlwerbung ergibt sich aus dem Bundesmeldegesetz (BMG). Danach können die Meldebehörden Parteien im Zusammenhang mit Wahlen Auskünfte aus dem Melderegister erteilen (sogenannte Gruppenauskünfte). Zulässig ist dabei nur die Übermittlung von

- Vor- und Nachname,
- ggf. Doktortitel
- und die derzeitige Wohnanschrift,

nicht aber z. B. das Geburtsdatum. Bei den jeweiligen auf Antrag der Partei erteilten Meldeauskünften gelten zudem folgende gesetzliche Vorgaben, zu denen sich die Parteien schriftlich gegenüber den Behörden verpflichten:

- Die Auskünfte erfolgen nur für den Zeitraum von sechs Monaten vor einer Wahl. Nach der Wahl sind Namen und Adressdaten innerhalb eines Monats von den Verantwortlichen wieder zu löschen.
- Die übermittelten Daten dürfen ausschließlich nur für die Wahlwerbung verwendet werden. Unzulässig wäre die Nutzung der Adressdaten zur Aufnahme in eine „allgemeine Adressdatenbank“ oder zur Mitgliedergewinnung für die Partei.
- Zudem dürfen Auskünfte nur über einzelne Altersgruppen erteilt werden, die Partei muss also bei ihrer Abfrage einen konkreten Altersbereich nennen. So ließen sich zum Beispiel die Adressen aller Erstwählenden oder jungen Erwachsenen ermitteln. Parteien können ihre Wahlwerbung dadurch gezielt an die entsprechende Altersgruppe anpassen.

Halten sich die Empfänger von Meldedaten für Wahlkampfzwecke an diese gesetzlichen Vorgaben, ist deren Verarbeitung aus datenschutzrechtlicher Sicht zulässig. Das Persönlichkeitsrecht der Bürger tritt in diesen Fällen hinter das Recht politischer Parteien oder Organisationen an demokratischer Teilhabe im Rahmen von Wahlen zurück.

Bürger, die keine Wahlwerbung erhalten möchten, haben die Möglichkeit, der Veröffentlichung bzw. der Weitergabe an Dritte zu widersprechen. Für den Widerspruch ist keine besondere Form vorgesehen, er kann in Schriftform, persönlich oder per E-Mail bei der zuständigen Meldebehörde erhoben werden. Wer ihn erhebt, muss weder eine Begründung angeben noch

eine Frist beachten. Der Widerspruch ist gebührenfrei und wirkt grundsätzlich auf Dauer, entfaltet für die Vergangenheit jedoch keine Wirkung. Eine Rücknahme des Widerspruchs ist möglich.

Häufig stellen die Gemeinden auf ihren Service-Portalen digitale Widerspruchsformulare zur Verfügung. Auf das Widerspruchsrecht ist zudem einmal jährlich durch ortsübliche Bekanntmachung – also z. B. in einem Mitteilungsblatt – hinzuweisen. Aufgrund des Widerspruchs trägt die Meldebehörde im Melderegister eine Übermittlungssperre für Gruppenauskünfte mit dem Zweck „Wahlwerbung“ ein.

Weiterführende Informationen und Rechtsquellen:

- § 50 Abs. 1 Satz 1 BMG Meldebehörden dürfen Parteien Auskunft aus dem Melderegister geben, jedoch nur, wenn die Wahlberechtigung an eine Altersgrenze geknüpft ist (z. B. 18 Jahre) und nur über einzelne Altersgruppen

- § 44 Abs. 1 Satz 1 BMG listet die Daten auf, die abgefragt werden dürfen

- § 50 Abs. 1 Satz 3 BMG bestimmt eine Löschfrist von einem Monat nach der Wahl

- § 50 Abs. 5 BMG regelt den Widerspruch der Weitergabe

Parteien dürfen im Vorfeld anstehender Wahlen nach Altersgruppen kategorisierte Datensätze von den Meldebehörden abfragen, um diesen Wählergruppen anschließend personalisierte Wahlwerbung zuzusenden. Eine Verwendung der Daten über Wahlwerbung hinaus ist unzulässig. Bürger können jederzeit einer solchen Weitergabe ihrer Daten widersprechen. Die Meldebehörde trägt dann eine entsprechende Übermittlungssperre ein. Die Sperre gilt für die Zukunft und ist unbefristet.

11.4 Auskünfte aus dem Liegenschaftskataster

Wiederholt erreichten den Landesbeauftragten für den Datenschutz Beschwerden von Grundstückseigentümern, die bezüglich ihrer Grundstücke Kaufanfragen erhalten hatten, aber gar nicht an einem Verkauf interessiert waren. Die Kaufinteressenten gaben in der Regel an, die Eigentümerdaten durch ein Auskunftsersuchen aus dem Liegenschaftskataster erhalten zu haben.

Auf Anfrage teilte das zuständige Landesamt für Vermessung und Geoinformation Sachsen-Anhalt (LVermGeo) mit, dass Auskünfte aus dem Liegenschaftskataster generell gem. § 13 Abs. 1 Satz 2 Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt erfolgten. Demnach erhalten – wenn öffentliche Belange dem nicht entgegenstehen – neben den Eigentümern auch solche Personen Auskunft, die ein berechtigtes Interesse daran darlegen.

Weiter teilte das LVermGeo mit, dass das Vorliegen eines berechtigten Interesses in Bezug auf die personenbezogenen Daten des Liegenschaftskatasters im Lichte neuerer katasterrechtlicher Rechtsprechung zu bewerten sei. Danach könne ein berechtigtes Interesse auch dann vorliegen, wenn Eigentümerangaben zur Anbahnung von Verhandlungen bzw. vorgelagert zur Klärung der Verkaufsbereitschaft des jeweiligen Eigentümers benötigt würden. Andernfalls

würde ein berechtigtes Interesse voraussetzen, dass bereits Verhandlungen stattgefunden haben bzw. die Verkaufsabsicht des Eigentümers bekannt sei. Dann sei der Eigentümer jedoch bereits bekannt, sodass sich ein Auskunftsersuchen erübrige.

In einigen Fällen wurde bezüglich der Grundstücke der Beschwerdeführer im Geschäftsbuch des LVermGeo kein Eintrag auf mündliche oder schriftliche Auskunft verzeichnet, sodass nicht nachvollziehbar war, wie der Interessent sein berechtigtes Interesse nachgewiesen hatte. Allerdings wurden dort bisher nur kostenpflichtige Anträge registriert. Mündliche Auskünfte unter einer Dauer von 15 Minuten, die kostenfrei sind, wurden nicht im Geschäftsbuch vermerkt.

Aufgrund der Beschwerden hat das LVermGeo seine bisherige Vorgehensweise bei mündlichen Auskünften unter einer Dauer von 15 Minuten dahingehend geändert, dass auch diese entsprechend dokumentiert werden. Dadurch können Grundstückseigentümer zukünftig in ähnlichen Situationen in Erfahrung bringen, wer aufgrund welches berechtigten Interesses Auskunft aus dem Liegenschaftskataster erhalten hat.

12 Wirtschaft

12.7 Erfüllung des Auskunftsanspruchs nach Art. 15 DS-GVO

In seinem Urteil vom 15. Juni 2021 (VI ZR 576/19) hat sich der Bundesgerichtshof unter anderem zum Umfang des Auskunftsanspruchs nach Art. 15 DS-GVO geäußert. Ein ebenfalls thematisierter Punkt war die Frage, ob ein Auskunftsanspruch nach Art. 15 DS-GVO auch bei unrichtiger oder unvollständiger Auskunft erfüllt sein kann.

Nach dem Urteil ist der – grundsätzlich weit zu verstehende – Auskunftsanspruch dann erfüllt, wenn der Auskunftsverpflichtete unmissverständlich zum Ausdruck bringt, er habe die Auskunft in dem konkret geschuldeten Umfang vollständig erteilt. Dazu ist es notwendig, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdeckt. Der bloße Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist führt nicht dazu, dass noch weitergehende Auskunft erteilt werden muss. Selbst eine inhaltliche teilweise falsche Auskunft führt nicht automatisch dazu, dass der Anspruch nicht erfüllt wurde.

Das Urteil erscheint auf den ersten Blick vielleicht etwas merkwürdig. Es bedeutet aber weder, dass eine grobe Erteilung von Auskünften genügt, noch, dass die bloße Vermutung einer falschen Auskunft oder geringe Fehler dazu verpflichten, die Beantwortung nachzubessern. Der Auskunftspflichtige muss genau prüfen, in welchem Umfang die Auskunft berechtigterweise begehrt wird und sich mit jeder Kategorie der Auskunftsgegenstände ernsthaft auseinandersetzen. Wird eine Auskunft erteilt, macht der pauschale Hinweis, weitere personenbezogene Daten des Auskunftsberechtigten würden nicht verarbeitet, eine Auskunft nicht automatisch vollständig.

Eine Ergänzung kann der Auskunftsberechtigte vor allem dann verlangen, wenn sich der Auskunftspflichtige zu bestimmten Punkten gar nicht äußert.

Auskunftsbegehren nach Art. 15 DS-GVO sollten durch den Berechtigten klar formuliert und durch den Verpflichteten sorgfältig beantwortet werden.

12.8 Dokumentation der Löschung personenbezogener Daten

Der Landesbeauftragte wurde gefragt, wie durch einen Verantwortlichen nachgewiesen werden kann, dass eine Löschungsverpflichtung aus Art. 17 DS-GVO erfüllt worden ist. Zu klären war, ob für Nachweiszwecke dasjenige Schreiben gespeichert werden darf, mit dem einer betroffenen Person die Löschung ihrer personenbezogenen Daten bestätigt wird oder ob dadurch unnötigerweise weiterhin Daten der betroffenen Person gespeichert werden.

Der Begriff der Löschung ist in der DS-GVO nicht definiert. Wenn eine betroffene Person die Löschung beantragt, wird jedoch grundsätzlich davon auszugehen sein, dass alle zu ihrer Person vorhandenen Daten unkenntlich gemacht werden sollen. Dies beinhaltet regelmäßig auch die Daten, die im Zuge der Bearbeitung eines Antrags auf Löschung verarbeitet werden. Dem Antrag ist zu entsprechen, wenn die Voraussetzungen des Art. 17 Abs. 1 DS-GVO erfüllt sind.

Im Regelfall kann ein Verantwortlicher den Nachweis der ordnungsgemäßen Löschung personenbezogener Daten durch ein geeignetes Löschkonzept erbringen. In Einzelfällen kann zur Durchsetzung von Betroffenenrechten eine weitere Dokumentation unter vorübergehender Speicherung personenbezogener Daten erforderlich sein, wie z. B. bei der Erteilung von (Negativ-)Auskünften nach Art. 15 DS-GVO. Datenbestände, die der Rechenschaftspflicht oder weiteren Aufbewahrungspflichten unterfallen, sollten dann aber im Produktivsystem nicht mehr verfügbar sein. Sie sind also strukturell vom aktiven Datenbestand getrennt zu halten.

Bei den Anforderungen an die Nachweispflichten muss zwischen der anlassbezogenen Ausübung eines Betroffenenrechts, z. B. in Form eines Löschungsverlangens, und der routinemäßigen Löschung gemäß Löschkonzept unterschieden werden.

Im Regelfall kann ein Verantwortlicher den Nachweis der ordnungsgemäßen Löschung personenbezogener Daten durch ein geeignetes Löschkonzept erbringen.

2022

17 Technik und Organisation

17.1 Was ist ein Löschkonzept?

Ein Löschkonzept ist eine formale schriftliche Zusammenstellung, die in der Praxis zu implementierende Löschvorgänge theoretisch untermauert. Die DIN-Norm 66398 beschreibt formal den Prozess zur Erstellung eines Löschkonzeptes.[31]

Zunächst müssen dazu alle Verarbeitungsvorgänge, bei denen personenbezogene Daten verarbeitet werden, die einer Löschfrist gem. Art. 17 DS-GVO unterliegen, kategorisch erfasst werden. Dann müssen die einzelnen Datenfelder darunter gelistet werden. Zu jedem Datum muss erfasst werden, welche gesetzliche Aufbewahrungsfrist besteht. Von Vorteil ist dabei die Angabe entsprechender Rechtsgrundlagen. Falls keine gesetzlichen Aufbewahrungsfristen bestehen, muss erfasst werden, zu welchem Zweck die Daten erhoben wurden und wann dieser Zweck erloschen ist, die Daten also nicht mehr erforderlich sind.

Schließlich sollte für jede Datenkategorie beschrieben werden, ob dafür eine automatische, zyklische oder manuell ausgelöste Löschung vorgesehen ist, ob diese ausschließlich digital stattfindet oder auch Akten und Datenträger existieren, die vernichtet werden müssen. Die Angabe einer zuständigen Abteilung bzw. Person erhöht die Nachverfolgbarkeit.

Neben dem Kurzpapier 11 „Recht auf Löschung“[32], welches von der Datenschutzkonferenz veröffentlicht wurde, bieten zahlreiche öffentlich zugängliche Internetseiten eine praktische Anleitung zur Erstellung von Löschkonzepten.[33]

17.2 Besonderes elektronisches Behördenpostfach

Seit dem 1. Januar 2022 ist die Nutzung des elektronischen Rechtsverkehrs (eRV) für Behörden und juristische Personen des öffentlichen Rechts verpflichtend.[34] Über sogenannte „sichere Übermittlungswege“ ist es möglich, in rechtssicherer Art und Weise elektronische Dokumente zu verschicken. Für Behörden wird die Nutzung des besonderen elektronischen Behördenpostfachs empfohlen, welches einfach und kostenfrei genutzt werden kann.

Für den Landesbeauftragten war es schon immer ein besonderes Anliegen, Bürgerinnen und Bürgern, aber auch Unternehmen und anderen Behörden eine sichere und vertrauliche Kommunikationsmöglichkeit anzubieten. Dazu konnte etwa Verschlüsselung mittels X.509-Zertifikaten oder PGP genutzt werden. Die erforderlichen Schlüssel sind auf der Website des Landesbeauftragten verfügbar. Auch über anonym und verschlüsselt nutzbare Webformulare ist es möglich, die Behörde zu erreichen. Das besondere elektronische Behördenpostfach ist ein weiterer Weg und eröffnet einen sicheren elektronischen Übertragungsweg für elektronische Dokumente. Bisher blieben Bürgerinnen und Bürger von diesem Übermittlungsweg ausgenommen (nur kurze Zeit war die Nutzung kostenfrei möglich, wurde dann aber leider unterbunden).

Im Berichtszeitraum wurde die EGVP-Infrastruktur[35], das Elektronische Gerichts- und Verwaltungspostfach, um ein weiteres besonderes elektronisches Postfach – diesmal für Bürgerinnen und Bürger sowie Organisationen – bereichert. Das elektronische Bürger- und Organisationenpostfach (eBO) ist ein weiterer sicherer Übermittlungsweg, der den schriftformersetzenden Versand und die Zustellung elektronischer Dokumente ermöglicht (§ 130a Abs. 4 Nr. 4 ZPO). Er dient auch der sicheren Übermittlung für nicht formbedürftige Nachrichten im elektronischen Rechtsverkehr. Postfachinhaber werden überprüft und wie bei den anderen Postfächern auch im SAFE-Verzeichnisdienst veröffentlicht. Die Überprüfung erfolgt anhand eines elektronischen Identitätsnachweises, mit Hilfe eines qualifizierten elektronischen Siegels oder in einem manuellen Identifizierungsverfahren mittels in öffentlich beglaubigter Form abgegebener Erklärung (Notar).

Für die Nutzung des eBO wird eine kostenpflichtige Software benötigt. Die ehemals kostenfreie Bereitstellung einer Software ist entfallen. Nutzer werden im Adressbuch des eRV veröffentlicht, aber die Daten können nur von der Justiz, Behörden, Rechtsanwältinnen und Rechtsanwälten, Notarinnen und Notaren sowie Steuerberaterinnen und Steuerberatern eingesehen werden. Auch Inhaber anderer besonderer elektronischer Postfächer (beA, beBPo, beN) können eine Kommunikation aufnehmen. Andere eBO-Postfachinhaberinnen und -inhaber haben darauf keinen Zugriff. Damit wird der Nutzen des Postfachs auf den Justiz-Kontext beschränkt.

17.4 Informationssicherheit (AG InfoSic Land)

Die Leitlinie zur Informationssicherheit (LISL LSA) in der unmittelbaren Landesverwaltung Sachsen-Anhalt bestimmt bei der Nutzung von Informationstechnik (IT), dass ein erforderliches und angemessenes Sicherheitsniveau herzustellen und aufrecht zu erhalten ist sowie verbleibende Restrisiken zu minimieren sind. Sie verlangt den obligatorischen Betrieb eines Informationssicherheitsmanagementsystems (ISMS) gemäß IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) als kontinuierlichen Prozess. Das IT-Grundschutzkompendium gibt die hier zu erfüllenden technischen und organisatorischen Maßnahmen zur Auswahl vor. Der dabei einzuhaltende Mindeststandard wird in den IT-Sicherheitsrichtlinien (ISRL) des Landes festgehalten. Es wurde weiter an den ISRL gearbeitet.

In der UAG „Awareness“ wurde anhand des BSI-Bausteins ORP.3 „Sensibilisierung und Schulung zur Informationssicherheit“ ein Schulungs-, Sensibilisierungs- und Trainingskonzept erstellt. Dieses bildet den Rahmen für die Planung, Durchführung und Strukturierung von Schulungs- und Sensibilisierungsmaßnahmen im Land. Ziel ist die Bereitstellung einer Awareness-Plattform für die unmittelbare Landesverwaltung, die es erlaubt, kontinuierliche Informationssicherheits-Awareness-Kampagnen durchzuführen und auszuwerten. Gedacht ist dabei etwa an Phishing-Simulationen und interaktive bzw. multimediale Nutzersensibilisierungen.

In der UAG „BITS“ wurde in vielen Treffen weiter an den Inhalten für das an die Bedürfnisse des Landes angepasste Behörden-IT-Sicherheitstraining gearbeitet. Es wurde eine an das Land angepasste Version erstellt und von den Stakeholdern auch praktisch erprobt. Neben der Anpassung bestehenden Schulungsmaterials wurden auch neue Lektionen erstellt, etwa zu den Themen Videokonferenzen und Home-Office. Innerhalb der Landesverwaltung musste nun eine technische Plattform für die Nutzung durch die Beschäftigten eingerichtet werden. Die technischen Anforderungen wurden an das MID als Arbeitsauftrag weitergegeben.

Im XVII. Tätigkeitsbericht wurde über das Inkrafttreten der Leitlinie zur Informationssicherheit der unmittelbaren Landesverwaltung Sachsen-Anhalt (LISL LSA, Informationssicherheitsleitlinie) des Landes und die damit einhergehende beginnende Erstellung belastbarer IT-Sicherheitsrichtlinien (ISRL) berichtet. Die ersten ISRL, die Passwort- und die Telearbeits-RL, befanden sich bereits auf der Zielgeraden und wurden nach Einarbeitung offener Rückmeldungen zügig vollendet. Die ISRL zum „Umgang mit Sicherheitsvorfällen“ wurde finalisiert und Umsetzungshinweise zu den Anforderungen ausgearbeitet. Weitere Arbeiten erfolgten – teils in UAGs – an ISRL und Prozessbeschreibungen betreffend Korrektur- und Vorbeugemaßnahmen, Organisation und Personal, Berichtswesen, Risikomanagement und dem Landesweiten Sicherheitsprozess.

Nachdem im letzten Jahr die ISRL „Dokumentenmanagement“, „Passwortrichtlinie“ und „Telearbeit“ inhaltlich abgeschlossen und von den ISB der obersten Landesbehörden und dem CISO freigegeben wurden, erfolgte nun auch zum Ende des Jahres die Freigabe durch die Hausleitungen der obersten Landesbehörden und dem CIO. Die Dokumente wurden im Extranet im CISO-Bereich eingestellt.

Gem. Abschnitt 4 LISL LSA tragen die Leitungen der obersten Landesbehörden die Verantwortung für die Informationssicherheit in ihren Zuständigkeitsbereichen. Die durch Dataport bereitgestellten Sicherheitskonzepte waren, abgesehen vom zertifizierten Rechenzentrumsbetrieb, unzureichend und zu einer fundierten Information der Hausleitungen bezüglich des aktuellen Stands der IT-Sicherheit ungeeignet. Die AG InfoSic (Land) regte eine Überprüfung

essentieller Querschnittsdienste bzw. zentral beauftragter Verfahren in Form einer IS-Kurzrevision an. Ziel ist die Gewinnung von Kennzahlen, anhand derer den Hausleitungen in angemessener Form ein Lagebild vermittelt werden kann, damit diese Risiken richtig einschätzen und gegebenenfalls übernehmen können.

Die UAG „Kommunen“ traf sich virtuell per Videokonferenz. Kommunen sollen im Bereich der Informationssicherheit enger an das ISMS Land angebunden werden. Das betrifft insbesondere den Informationsaustausch von Warn- und Informationsmeldungen zu Sicherheitslücken sowie bei Sicherheitsvorfällen. Dazu war eine Meldung von Ansprechpartnern in den Kommunen und deren Einrichtung auf dem Kundenportal des CERT Nord notwendig, damit die dort erstellten Lageberichte und Warnhinweise einen Empfänger finden. Aufgaben des CERT Nord sind der Informationsdienst, ein Warndienst, allgemeine Beratung und die Behandlung von Sicherheitsvorfällen. Dafür steht es in engem Kontakt mit anderen CERTs und dem BSI. Das MID unterstützte das CERT Nord bei der Aufnahme in die E-Mail-Verteiler und die Verpflichtungen der Ansprechpartner nach dem Traffic Light Protocol (TLP). Eine TLP-Verpflichtung ist eine Vereinbarung, die den sicheren Austausch von sensiblen Informationen regelt. Sie verwendet Farbcodes, um den Grad der Vertraulichkeit und die Bedingungen für die Weitergabe eines Dokumentes zu kennzeichnen.

Im Jahr 2021 war die Unterzeichnung einer Kooperationsvereinbarung zwischen dem Land Sachsen-Anhalt und dem BSI geplant. Diese konnte bisher noch nicht erfolgen, da zuvor die Konkretisierung der Handlungsfelder erforderlich ist. Es musste ein zeitlicher Handlungsrahmen festgelegt und ein Arbeitsprogramm für beide Partner entwickelt werden. Die konkreten Kooperationsfelder wurden unter den AG InfoSic-Mitgliedern abgestimmt, um Arbeitsschwerpunkte zu ermitteln. Ziel war es, die wichtigsten Punkte für die nächsten 2 Jahre zu planen und ein konkretes Vorhaben zu entwickeln.

Das MID hatte mit Unterstützung durch das MI die Federführung bei der Erstellung eines Informationssicherheitsgesetzes für das Land Sachsen-Anhalt. Das IT-Sicherheitsgesetz soll die Sicherheit in einem vernetzten Raum wie dem Internet oder dem Landesnetz gewährleisten. Der erste Entwurf sollte bis Ende April 2022 erstellt werden. Im Rahmen der Erstellung wurde der Landesbeauftragte im Juli um eine Prüfung des Abschnitts „Maßnahmen zur Sicherstellung der Informationssicherheit“ ersucht. Gegen den vorgelegten Auszug aus dem Gesetzentwurf bestanden im Grunde keine Bedenken. Es wurden einzelne Defizite erkannt und es konnten sachdienliche Hinweise gegeben werden.

Der gesamte Entwurf des IT-Sicherheitsgesetzes lag leider nicht vor. Das war insofern unglücklich, da ausgehend von den Inhalten der IT-Sicherheitsgesetze anderer Bundesländer angenommen werden konnte, dass weitere Passagen, ggf. auch das Gesetz als Ganzes, datenschutzrelevant sein könnten und bewertet werden sollten.

Das Gesetz wurde mangels Ressourcen und wohl auch entsprechender juristischer Unterstützung bei der Bearbeitung im Berichtszeitraum nicht mehr vollendet. Es wurde jedoch kontinuierlich über Fortschritte in der AG InfoSic (Land) berichtet.

Im Dezember 2021 wurde eine kritische Sicherheitslücke in log4j gefunden. Log4j ist ein Framework für das Logging von Anwendungsmeldungen in Java. Die Lücke war gefährlich, da sie in einer weit verbreiteten Java-Bibliothek vorhanden war und es Angreifern ermöglichte, Schadcode auf betroffenen Systemen auszuführen. Die Schließung der Sicherheitslücke erfolgte rasch, die Umsetzung durch die Softwarehersteller, die log4j integriert hatten, zog

sich teilweise über Monate hin. Auch die AG InfoSic (Land) beschäftigte sich mit der Prüfung von Soft- und Hardware und der Ermittlung der eingesetzten Versionen von log4j.

Das führte direkt zum Thema Software Bill of Materials (SBOM). Die SBOM ist eine Liste all jener Komponenten einer Software, die bei der Erstellung der Software als Teil dieser eingebaut wurden. Wünschenswert wäre es, wenn alle eingesetzte Software im Land bekannt und dazu jeweils eine aktuelle SBOM verfügbar wäre. So würde jede Schwachstelle in einer Komponente, die nicht behoben wird, für Kunden und Nutzer sichtbar. Insbesondere bei neuen Produkten sollte eine Information zu allen eingesetzten Komponenten systematisch eingefordert werden. Eine Erstellung einer SBOM durch Dataport wurde bisher aus Kapazitätsgründen abgelehnt. Eine entsprechende Zusammenstellung wird jedoch, insbesondere als Grundlage für Risikoanalysen, für notwendig erachtet. Der Landesbeauftragte befürwortet, dass bei allen Beschaffungen von Software wie Fachanwendungen bereits in den Verträgen entsprechende Bereitstellungen in einem standardisierten Format vorgesehen werden. Mehr noch, es wird angeregt, Hersteller zu bestenfalls kontinuierlichen (CI/CD-basiert), in jedem Fall jedoch bei Sicherheitsvorfällen bzw. auf Nachfrage, zeitnahen Bereitstellungen von aktualisierter Software zu verpflichten.

Im Nachgang zum Sicherheitsvorfall im Landkreis Anhalt-Bitterfeld, wurde dort ein Expertenbeirat ins Leben gerufen. Vorrangig sollen Möglichkeiten zur Schaffung von Fähigkeiten für ein Incident Response bei einem akutem Sicherheitsvorfall identifiziert und bewertet werden. Die Ergebnisse sollen anderen Bedarfsträgern zur Verfügung gestellt werden.

Aufgrund der hohen Bedrohungslage in den Kommunen bot das BSI den Ländern eine „Roadshow Kommunen“ in Form eines Webinars an. Das BSI wollte die Organisation übernehmen, die Länder sollten sich aktiv etwa mit eigenen Vorträgen beteiligen. Sachsen-Anhalt plante, das Angebot anzunehmen und etwa erste Schritte auf dem Weg zum IT-Grundschutz in Form eines „Blaupausen-Fahrplans“ (ISB benennen, Rollen- und Rechte festlegen, ...) einzubringen. In einer gemeinsamen Veranstaltung des BSI und dem Ministerium für Infrastruktur und Digitales des Landes Sachsen-Anhalt wurde noch im August 2022 mit Blick auf die aktuelle Bedrohungslage für die Informationssicherheit sensibilisiert und die unterschiedlichen Unterstützungsangebote vorgestellt.

18 Telekommunikation und Medien

18.2 Kurzgutachten zum Betrieb von Facebook-Fanpages

Der Europäische Gerichtshof hatte bereits in seinem Urteil vom 5. Juni 2018 (Aktenzeichen C-210/16) festgestellt, dass Betreiber einer Facebook-Fanpage und das Unternehmen Facebook (jetzt: Meta Platforms Inc.) gemeinsame Verantwortliche gemäß Art. 26 DS-GVO sind.

Die sich daraus ergebenden Pflichten wie z. B. die Einhaltung der Grundsätze aus Art. 5 Abs.1 DS-GVO, die Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO und die Informationspflichten aus Art. 13 DS-GVO können von den Fanpage-Betreibern jedoch kaum erfüllt werden, da es hinsichtlich der Datenverarbeitung bei Facebook an der erforderlichen Transparenz fehlt.

Zu diesem Ergebnis kommt auch eine Arbeitsgruppe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), die ein Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages erstellt hat. Demnach ist

die Datenverarbeitung, die beim Besuch einer Facebook-Fan-page vorgenommen wird, weder mit der DS-GVO noch mit dem Telekommunikation-Telemedien-Datenschutz-Gesetz vereinbar, weshalb ein datenschutzkonformer Betrieb zurzeit nicht möglich ist.

In ihrem Beschluss vom 23. März 2022 hat die DSK das Kurzgutachten zur Kenntnis genommen und der Bewertung zugestimmt.[36] Weiterhin wurde festgelegt, die obersten Landes- bzw. Bundesbehörden über den Inhalt des Kurzgutachtens zu informieren und darauf hinzuwirken, dass von Landes- bzw. Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können. Ziel dieses Vorgehens ist aber kein generelles Verbot von Facebook-Fanpages, sondern der rechtskonforme Betrieb, der jedoch nur mit Änderungen bei der Datenverarbeitung durch Facebook und dessen Mutterkonzern Meta gewährleistet werden könnte.

18.3 Häufige Mängel beim Einsatz von Cookies und Tracking-Mechanismen

Auf vielen Internetseiten werden regelmäßig Cookies gesetzt und ausführbarer Skript-code von Drittanbietern eingebunden. Beide Technologien können sowohl dazu eingesetzt werden, eine Internetseite datenschutzkonform mit zusätzlichen Funktionalitäten aufzuwerten als auch die Aktivitäten der Seitenbesucher zu verfolgen und seitenübergreifende Profile zu erstellen (Tracking).

Wenn das Anlegen und Auslesen von Cookies für die reine Bereitstellung einer Inter-netseite nicht unbedingt erforderlich ist, ist gem. § 25 TTDSG (ab 2024 TDDDG) für diese Art der Datenerhebung eine Einwilligung einzuholen. Bei der Datenerhebung durch ausführbaren Skriptcode (z. B. zur Reichweitenanalyse) bzw. Einbindung anderer Inhalte (z. B. Schriftarten, Captcha usw.) wäre Art. 6 Abs. 1 lit. a, b oder f DS-GVO gemäß der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien vom Dezember 2021[37] anzuwenden und das Urteil des LG München vom 20. Januar 2022 (Az. O 17493/20) zu beachten.

Möglicherweise kann die Anwendung von Skriptcode, der nicht explizit der Profilbildung dient, auch als berechtigtes Interesse des Webseitenbetreibers eingeordnet und im Rahmen der Abwägung ohne Einwilligung zulässig befunden werden. Dies wäre z. B. denkbar bei der Einbindung eines Captcha-Mechanismus zur Erhöhung der Sicherheit einer Webseite ohne Datenübermittlung in unsichere Drittstaaten oder bei der Einbindung eines anonymisierten Statistikwerkzeuges auf der eigenen Webseite. Umgekehrt würde bei der Einbindung von Trackingmechanismen Art. 6 Abs. 1 lit. a DS-GVO anzuwenden sein und eine Einwilligung wäre Voraussetzung und Rechtsgrundlage der Datenverarbeitung (siehe Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. Mai 2020 „Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich“[38]).

Zu beachten ist ebenfalls, dass sich die vorgenannte Rechtmäßigkeitsbetrachtung lediglich auf die Verarbeitung der Daten innerhalb des Europäischen Wirtschaftsraums bezieht. Es muss daher auch geprüft werden, ob es bei einer Datenverarbeitung zu einer Übermittlung personenbezogener Daten in Drittländer kommt. Eine Übermittlung von personenbezogenen Daten in Drittländer ohne durch die EU-Kommission anerkanntes Datenschutzniveau (z. B. EU-U.S. Data Privacy Framework[39]) darf nur vorbehaltlich geeigneter Garantien, wie z. B. Standarddatenschutzklauseln, oder bei Vorliegen eines Ausnahmetatbestandes für bestimmte Fälle gemäß Art. 49 DS-GVO erfolgen (siehe Urteil des EuGH vom 16. Juli 2020 Az. C-311/18).

Um bei einem Besuch einer Internetseite eine wirksame Einwilligung einzuholen muss der Besucher vorab zum einen umfassend informiert werden und zum anderen aktiv seine Einwilligung, z. B. durch Klicken auf einen Button „Ich bin einverstanden“, bekunden. Eine rechtmäßige Einwilligung kann auf einer Internetseite durch einen Consent Manager umgesetzt werden. Reine Cookie-Banner, die nur allgemein über das Anlegen von Cookies informieren und mit nur einem Knopf „Bestätigen“ oder „OK“ ausgeblendet werden können, erfüllen nicht die Anforderungen an eine Einwilligung gem. Art. 7 DS-GVO.

Häufig werden auf Internetseiten Consent Manager eingeblendet und obwohl noch gar keine Einwilligung durch den Besucher erteilt wurde, werden bereits Skripte von Drittanbietern wie Google nachgeladen und Cookies durch diese gesetzt. Beides ist unrechtmäßig. Internetseitenbetreiber haben darauf zu achten, das Einbinden einwilligungspflichtiger Cookies und Skripte erst dann aktiv auszuführen, nachdem die Besucher im Consent Manager eingewilligt haben. Ohne Einwilligung sind beim ersten Laden der Internetseite nur solche Cookies erlaubt, die zwingend zum grundlegenden Betrieb der Internetseiten erforderlich sind, so z. B. Sitzungs-Cookies oder Warenkorb- Cookies. Skriptcode Dritter, etwa für Menüfunktionalitäten, sollte lokal gehostet angeboten werden.

Schließlich gilt es ebenfalls zu beachten, dass es durch das Einbinden externer Inhalte ermöglicht wird, dass die Anbieter der Inhalte während des Abrufes durch den Browser der Seitenbesucher deren IP-Adresse, Geolokation, Ursprungswebseite und Zeitstempel erheben und verarbeiten können. Also bereits durch das reine Einbinden von Inhalten Dritter Daten des Besuchers an diese Dritten übermittelt werden. Auch dies bedarf einer Einwilligung, die gemeinsam mit der für Cookies erhoben werden kann.

Wenn Internetseiten mittels Cookies und ausführbarem Skriptcode die Aktivitäten der Seitenbesucher verfolgen sollen oder personenbezogene Daten der Besucher an Dritte übermittelt werden, muss eine Einwilligung der Besucher per Consent Manager eingeholt werden, noch bevor die Cookies und Skripte geladen werden.

25 Verwaltung allgemein

25.1 Zensus 2022

Wie bereits im XVII. Tätigkeitsbericht (Nr. 15.1) berichtet, war turnusgemäß für den 16. Mai 2021 ein Zensus – also eine Volks-, Gebäude- und Wohnungszählung – vorgesehen, die aufgrund der Corona-Pandemie jedoch um ein Jahr auf den 15. Mai 2022 verschoben werden musste. Der Zensus 2022 wurde registergestützt durchgeführt und umfasste vier Erhebungsteile (Bevölkerungszählung, Gebäude- und Wohnungszählung, Haushaltebefragung auf Stichprobenbasis, Erhebungen an Anschriften mit Sonderbereichen).

Damit europaweit einheitliche Grunddaten über die Bevölkerung und die Wohnsituation verfügbar sind, sind die Mitgliedstaaten nach der Verordnung (EG) Nr. 763/2008 über Volks- und Wohnungszählungen verpflichtet, alle zehn Jahre einen Zensus durchzuführen. Die nationalen gesetzlichen Regelungen für den Zensus 2022 finden sich im Bundesstatistikgesetz (BStatG) und im Zensusgesetz 2022 (ZensG 2022). Die Auskunftspflicht ergibt sich aus § 15 BStatG i. V. m. § 23 ZensG 2022. Kommen Befragte ihrer Auskunftspflicht nicht nach und verweigern die Teilnahme am Zensus 2022, stellt dies eine Ordnungswidrigkeit dar, die mit einer Geldbuße geahndet werden kann (siehe § 23 Abs. 1 BStatG).

Die beim Zensus 2022 erhobenen Daten unterliegen dem Statistikgeheimnis bzw. der statistischen Geheimhaltung gem. § 16 Abs. 1 BStatG. Alle an der Organisation und Durchführung des Zensus 2022 beteiligten Personen werden auf das Statistikgeheimnis verpflichtet. Verstöße dagegen sind strafbar und werden entsprechend verfolgt.

Außerdem gibt es ein sogenanntes Rückspielverbot. Das bedeutet, dass bearbeitete Einzeldatensätze, die noch einen Personenbezug aufweisen, von den Statistischen **Ämtern nicht an die Stellen „zurückgespielt" werden dürfen, von denen die Ursprungs**daten stammen. Auch eine Weitergabe von Daten mit Personenbezug an sonstige Stellen und Behörden erfolgt nicht. Der Zweckbindungsgrundsatz nach Art. 5 Abs. 1

lit. b DS-GVO verhindert zudem, dass die für den Zensus erhobenen Daten nachträglich für andere Zwecke verwendet werden können. Dies wäre rechtlich unzulässig.

Bei den im Zensus 2022 erhobenen Einzelangaben handelt es sich zunächst um personenbezogene Daten. Deshalb ist es besonders wichtig, die Vertraulichkeit und Integrität dieser Daten zu gewährleisten. Allerdings werden die „Hilfsmerkmale", wie z. B. Name und Anschrift der Auskunftspflichtigen, von den für die Ergebnisse des Zensus relevanten Daten („Erhebungsmerkmale") frühestmöglich getrennt. Die Weiterverarbeitung und die Auswertung der Zensus-Ergebnisse erfolgen dann auf Basis der anonymisierten Daten.

Gemäß § 7 Abs. 1 Zensusausführungsgesetz Sachsen-Anhalt 2022 (ZensAG 2022 LSA) haben die örtlichen Erhebungsstellen die für die Durchführung des Zensus 2022 benötigten Erhebungsbeauftragten anzuwerben, auszuwählen, zu bestellen, auf die Wahrung des Statistikgeheimnisses und des Datengeheimnisses schriftlich zu verpflichten und sie über ihre Rechte und Pflichten zu belehren. Die Bestellung eines oder einer Erhebungsbeauftragten darf nicht erfolgen, wenn Tatsachen die Annahme rechtfertigen, dass der oder die Erhebungsbeauftragte nicht die erforderliche Zuverlässigkeit besitzt.

Zur Überprüfung der Zuverlässigkeit kann die örtliche Erhebungsstelle eine unbeschränkte Auskunft nach § 41 Abs. 1 Nr. 9 des Bundeszentralregistergesetzes einholen. Die örtliche Erhebungsstelle kann darüber hinaus eine Stellungnahme der für den Wohnort der Bewerberin oder des Bewerbers zuständigen Behörde der Landespolizei, einer zentralen Polizeidienststelle oder des Landeskriminalamts einholen, soweit dies zur Überprüfung der Zuverlässigkeit erforderlich ist.

Gemäß § 20 Abs. 1 ZensG 2022 dürfen Erhebungsbeauftragte außerdem nicht in der unmittelbaren Nähe ihrer Wohnung eingesetzt werden, um zu vermeiden, dass sie ihnen bekannte Personen befragen.

25.2 Zensus 2022 – Beschwerden

Den Landesbeauftragten erreichten während der Haushaltsbefragung und der Wohnungs- und Gebäudezählung mehrere Beschwerden darüber, dass im Rahmen des Zensus 2022 einige Rechte aus der DS-GVO eingeschränkt wurden und zwar das Auskunftsrecht nach Artikel 15, das Recht auf Berichtigung nach Artikel 16, das Recht auf Einschränkung der Verarbeitung nach Artikel 18 und das Widerspruchsrecht nach Artikel 21 DS-GVO.

Die Petenten wollten wissen, warum ihre Rechte im Rahmen des Zensus 2022 derart eingeschränkt wurden. Außerdem kritisierten sie, dass in Deutschland nur 8 Bundesländer die Betroffenenrechte ausgeschlossen haben und diese in 4 Bundesländern eingeschränkt wurden.

Durch die unterschiedlichen Regelungen sahen sie sich als Bewohner des Landes Sachsen-Anhalt deutlich benachteiligt und diskriminiert.

Der Ausschluss der Betroffenenrechte ergibt sich aus § 9 Satz 1 Zensusausführungs-gesetz Sachsen-Anhalt 2022 (ZensAG 2022 LSA) i. V. m. Art. 89 Abs. 2 DS-GVO.

Art. 89 Abs. 2 DS-GVO besagt unter anderem, dass bei der Verarbeitung personenbezogener Daten zu statistischen Zwecken im Recht der Mitgliedsstaaten Ausnahmen von den Rechten gemäß der Art. 15, 16, 18 und 21 vorgesehen werden können, wenn diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.

Da die genannten Rechte die Durchführung des Zensus 2022 beeinträchtigen würden, wurde in § 9 Satz 1 ZensAG 2022 LSA festgelegt, dass zum Schutz der fristgemäßen und vollständigen Durchführung des Zensus 2022 die Rechte gem. Art. 15, 16, 18 und 21 DS-GVO nicht bestehen.

Basierend auf dem Zensusgesetz 2022 haben die Bundesländer eigene Zensusausführungsgesetze erlassen, wie das in Sachsen-Anhalt mit dem ZensAG 2022 LSA der Fall ist. Da es sich hierbei um Landesrecht handelt, entscheiden die einzelnen Landesparlamente unabhängig über die Gesetzesinhalte, sodass die Regelungen in den Bundesländern unterschiedlich sein können.

25.3 Beratungsanfragen Onlinezugangsgesetz (OZG)

Das Ministerium für Wirtschaft, Wissenschaft und Digitalisierung hatte sich Mitte 2020 mit einem Datenschutzkonzept für einen Online-Antragsassistenten BAföG Digital nebst Entwurf einer Verwaltungsvereinbarung für alle Bundesländer an den Landesbeauftragten mit der Bitte um Prüfung und Abnahme gewandt.

Da dies eine der ersten OZG-Anwendungen war, die für die sogenannte Nachnutzung durch andere Bundesländer vorgesehen war, hatte der Landesbeauftragte die Gründung einer Arbeitsgruppe unter Beteiligung der anderen Aufsichtsbehörden angeregt, im Rahmen derer die datenschutzrechtlichen Problemstellungen gemeinsam besprochen und abgestimmt werden konnten. Insbesondere im Hinblick auf die Zuweisung der datenschutzrechtlichen Verantwortlichkeit gab es erheblichen Klärungsbedarf, der im Ergebnis auf Druck der Aufsichtsbehörden auf Bundesebene zur Einführung einer gesetzlichen Regelung im OZG führen wird.

Der Landesbeauftragte hatte im letzten Jahr eine Vielzahl von Beratungsanfragen aus den obersten Landesbehörden und Kommunen zu verzeichnen, die die Umsetzung weiterer OZG-Projekte in der Nachnutzung betraf. Hierbei stellten sich immer wieder dieselben Fragen hinsichtlich der datenschutzrechtlichen Verantwortlichkeit, der Nutzungsmöglichkeit von Verwaltungsvereinbarungen oder der Notwendigkeit von Auftragsverarbeitungsverträgen einschließlich deren Ausgestaltung.

Der Landesbeauftragte konnte unter Nutzung der Erfahrungen aus der geschaffenen Arbeitsgruppe wesentliche Hilfestellungen leisten. Eine abschließende Rechtssicherheit wird allerdings erst nach der anvisierten Änderung des OZG zu erwarten sein.

2023

32 Technik und Organisation

32.2 Informationssicherheit (AG InfoSic Land)

Die Arbeit in den UAG der AG InfoSic (Land) wurde erfolgreich fortgesetzt, viele Projekte, meist Informationssicherheitsrichtlinien, auch weitgehend abgeschlossen. Sie warten jetzt auf ihre Finalisierung und abschließende Freigabe. Offen blieb lange Zeit, wie die verbindliche Veröffentlichung von ressortübergreifenden Informationssicherheitsrichtlinien derart erfolgen kann, dass die Inhalte nicht öffentlich einsehbar werden und der Schutzbedarf „intern“ gewahrt bleibt. Auch die Art und Weise der Veröffentlichung wurde wiederholt diskutiert. Muss diese über einen gemeinsamen Runderlass erfolgen oder kann sie der CIO wie geplant auf der Grundlage von §13 EGovG veröffentlichen? Ein zum Ministerialblatt alternatives Verfahren soll daher im Informationssicherheitsgesetz festgeschrieben werden. Bereits vom CIO gezeichnete Richtlinien sollen über die Hausleitungen und die ISB in den jeweiligen Ressorts bekannt gegeben werden.

Die UAG „BITS“ wurde in die UAG „Awareness“ migriert. Die im letzten Jahr eingerichtete BITS-Entwicklungsplattform befindet sich jetzt in der dSecureCloud und ist aus dem Landesnetz erreichbar. Es war geplant, eine landeseigene, übergreifende Schulungsplattform (ILIAS) mit Betrieb bei Dataport für alle Ressorts zur Verfügung zu stellen. Diese sollte neben den bereits vorhandenen Inhalten aus der Landesverwaltung Niedersachsen auch BITS und das Modul „Phishing“ beinhalten. In einer Machbarkeitsstudie sollte ein funktionaler Prototyp der ILIAS-Plattform im MID bereitgestellt werden, um sie genauer evaluieren und beurteilen zu können. Auch mögliche Nutzer anderer Plattformen und Dienstleister sollten so motiviert werden, ILIAS auch zu verwenden. Derweil lehnte Dataport die Bereitstellung der ILIAS-Plattform ab und schlug als Alternative Moodle vor. Auf Nachfrage mehrerer Trägerländer bei Dataport nach dem Betrieb von ILIAS, erfolgte dann doch die Aufnahme in das Produktportfolio.

In der UAG „Cloudnutzung und KI“ entstand im November 2023 das „Merkblatt KI“, welches kurz und prägnant wichtige Hinweise zur Nutzung von KI in der öffentlichen Verwaltung gibt.

Anfang des Jahres 2023 wurde ein erster Entwurf des Informationssicherheitsgesetzes Sachsen-Anhalt durch BSI und MI geprüft, später auch in der Runde der Informationssicherheitsbeauftragten der Ressorts vorgestellt. Es wurde um sehr kurzfristige Stellungnahmen gebeten, die in der zur Verfügung stehenden Zeit nicht möglich waren. Schließlich handelt es sich um ein wichtiges Gesetzesvorhaben, welches unmittelbar die zukünftige Arbeit der ISB betrifft und beeinflusst. So wurde ein gemeinsames Antwortschreiben an den CISO des Landes formuliert, dass die Übersendung als Beginn der fachlichen Diskussion des Entwurfs, mit dem verbindlichen Ziel der Schaffung angemessener rechtlicher Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit in der unmittelbaren Landesverwaltung Sachsen-Anhalt, angesehen wird. Auf bereits festgestellte Defizite hinsichtlich der Kompatibilität mit der Landesleitlinie Informationssicherheit wurde hingewiesen.

In den späteren Sitzungen der AG InfoSic (Land) wurden der immense Umfang und die Komplexität des Vorhabens deutlich. Immer mehr Punkte, fast alle aus der NIS-2-Richtlinie resultierend, mussten geregelt und im Gesetz abgedeckt werden. Der CISO informierte stetig und transparent über den Stand des Entwurfs des Informationssicherheitsgesetzes (des Landes)

und wies immer wieder auf die Möglichkeit der Übersendung von fachlichen Stellungnahmen und Anmerkungen an das CISO-Team hin. Nach der Bereitstellung eines aktualisierten Entwurfes im Spätsommer 2023 sollte die Ressortbeteiligung erfolgen. Zu klärende Problemfelder und Themen wurden nach und nach durch das MID und den CISO herausgearbeitet. Hinderlich war insbesondere das noch ausstehende und somit fehlende Umsetzungsgesetz des Bundes. Die Umsetzung der aufgrund der NIS-2-Richtlinie geplanten Maßnahmen sollte bis Oktober 2024 erfolgen.

Der Landesbeauftragte unterstützte von Anfang an das Anliegen des CISO, ein handwerklich gutes Gesetz mit sinnvollen Regelungen für das Land vorlegen zu wollen, wissend, dass nicht alle Forderungen Bestand haben werden und erwartend, dass vieles noch geändert oder gestrichen werden wird. Die Landesregierung wird sich an dem, was übrigbleibt, messen lassen müssen.

Im Dezember wurden die ISB der Ressorts zu einem Austausch im Zuge der Erstellung des Informationssicherheitsgesetzes Sachsen-Anhalt allerdings erst im Jahr 2024 eingeladen. Nun sollen die Anforderungen, Wünsche und Empfehlungen zeitnah erörtert und einbezogen werden.

Nach weiteren Abstimmungen fand im Oktober die lange erwartete Unterzeichnung der „Kooperationsvereinbarung im Bereich Cyber- und Informationssicherheit“ zwischen dem Land Sachsen-Anhalt vertreten durch das MID und dem BSI statt. Für das nächste Jahr soll etwa ein IT-Grundschutztag in Sachsen-Anhalt organisiert werden.

32.3 Pilotphase „Mein Justizpostfach“

Gerade noch im Berichtszeitraum wurde der Internetdienst „Mein Justizpostfach“ (MJP) in den Pilotbetrieb überführt.[53] Er soll eine sichere und kostenlose elektronische Kommunikation insbesondere mit der Justiz erlauben. Es ist explizit kein Elektronisches Bürger- und Organisationenpostfach (eBO), sondern nutzt ein OZG-Nutzerkonto Bund mit einer BundID[54] und dem Vertrauensniveau hoch, was den elektronischen Personalausweis voraussetzt. Das MJP dient der rechtswirksamen Einreichung elektronischer Dokumente mit nur einer einfachen Signatur durch Angabe des vollen Namens am Ende des Dokuments. Damit muss keine qualifizierte elektronische Signatur beschafft und verwendet werden. Dennoch ist dies einer der sogenannten „sicheren Übermittlungswege“ (§ 130a Abs. 4 Nr. 5 ZPO). Das MJP ergänzt damit das bestehende Angebot des eBO und bietet damit all jenen einen Zugang zur Justiz, die nicht über ein besonderes elektronisches Postfach verfügen und auch nicht die monatlichen Kosten eines eBO tragen wollen.

Wie bereits beim eBO (siehe Nr. 17.2), gibt es Einschränkungen, die eine allgemeine Verwendung verhindern und den Nutzerkreis auf den der besonderen Postfächer der EGVP-Infrastruktur (ohne eBO) beschränken. So können MJP-Nutzer zwar mit den elektronischen Postfächern des EGVP (beA, beN, beSt und beBPo), aber nicht untereinander und auch nicht mit eBO-Nutzern kommunizieren.

Offenbar ist die Nutzung des MJP mit einer Einwilligung zur Bekanntgabe von Verwaltungsakten über das Postfach des Nutzerkontos (§ 9 Abs. 1 OZG) und den ggf. damit verbundenen Fristen verbunden.

Nutzende des MJP sollten wissen, dass ihre vollständige Privatanschrift für alle EGVP-Teilnehmer, die ein MJP adressieren können, einsehbar ist. Das betrifft auch Personengruppen, die vielleicht eher keine privaten Besuche von unzufriedenen Verfahrensbeteiligten möchten (Schiedspersonen, Gutachter, Sachverständige), aber das MJP zur sicheren Kommunikation mit Anwälten nutzen werden.

Personen, für die im Melderegister eine Auskunftssperre nach dem BMG eingetragen ist, sollten beachten, dass die Daten des MJP aus der BundID und damit dem Melderegister stammen und andere Teilnehmende am elektronischen Rechtsverkehr (Gerichte, Rechtsanwälte, Steuerberater, Behörden, ...) in der Lage sind, diese – etwa die Meldeanschrift – einzusehen. Laut FAQ wird daran gearbeitet, dass Sperrvermerke im Melderegister zukünftig beachtet werden und etwa SAFE-Einträge ohne Anschrift möglich werden. Erst im Zuge der Weiterentwicklung des MJP soll die Einrichtung eines Postfachs auch ohne Veröffentlichung der Anschrift ermöglicht werden.

Es ist wichtig, dass der elektronische Rechtsverkehr DS-GVO-konform realisiert wird. Es sollte technisch möglich sein, in einer Identitätsdatenbank auch solche ohne Postanschrift mitzuführen, zumal deren Sinn ja darin besteht, mit diesen Personen elektronisch Kontakt aufnehmen zu können. Einzig die Prüfung auf zusammengehörige Daten (SAFE-Identität und vorhandene personenbezogene Daten) müsste passend ausgestaltet werden – entweder ohne Anschriften (Name, Geburtsdatum, ...) oder mit Anschriften-Matching, aber auch dafür gibt es bereits erprobte Verfahren.

32.4 Angemessene Reaktionen auf gängige Cyberangriffe

Ein Cyberangriff ist ein vorsätzlicher unbefugter Versuch, durch Zugriff auf IT-Systeme Daten zu stehlen oder zu manipulieren oder IT-Systeme zu stören. Die beim Landesbeauftragten am häufigsten gemeldeten Cyberangriffe sind Ransomware-Attacken, Virenbefall und Identitätsdiebstahl durch unbefugten E-Mail-Versand. Cyberangriffe müssen gem. Art. 33 DS-GVO immer dann an die Datenschutzaufsichtsbehörde gemeldet werden, wenn personenbezogene Daten betroffen sind und der Angriff voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Bei Ransomware handelt es sich um spezielle Schadsoftware, die jegliche Daten auf Festplatten und Netzwerkfreigaben verschlüsseln und oft mit einer Lösegeldforderung einhergehen. Nach einem Befall mit Schadsoftware oder Viren ist die Neuinstallation der Systeme und die Wiederherstellung der Daten aus Backups unerlässlich, denn Ransomware und andere Viren laden evtl. weiteren Schadcode aus dem Internet nach. Dieser Schadcode kann sich zunächst unbemerkt und ohne weitere schädliche Auswirkung im System einnisten und später ggf. aktiv werden, obwohl die Datei mit dem ursprünglichen Virus bereits bereinigt bzw. gelöscht wurde. Daher ist es bei Virenbefall dringend geboten, alle Systeme, die mit dem Virus in Kontakt gekommen sind, neu aufzusetzen. Nur eine Neuinstallation betroffener Rechner und Server kann garantieren, dass keine Reste des Virus oder von diesem nachgeladener Schadcode, im System verbleiben und später aktiv werden. Das Bundesamt für Sicherheit in der Informationstechnik gibt umfangreiche Empfehlungen zum Schutz vor und zum Umgang mit Ransomware-Befall.[55]

Zudem sollte bereits präventiv und fortlaufend auf allen Systemen und im Vorfeld der E-Mail-Zustellung auf Viren gescannt werden, noch bevor Schadprogramme Client-PCs erreichen können. Dafür bieten die Hersteller von Antivirensoftware gesonderte Produkte sog. E-

Mail-Gateways an. Außerdem sollte das Ausführen von Makros in Office-Produkten weitgehend deaktiviert werden, um zu verhindern, dass Makros in aus E-Mails heraus geöffneten Dokumenten aktiv werden. Im aktuellen Berichtszeitraum kursieren vermehrt Viren (z. B. Emotet), die über E-Mail-Anhänge eingeschleust werden und mittels Makros das Adressbuch eines Nutzers auslesen und dessen E-Mail-Adresse und die Bestands-E-Mails nutzen, um weitere E-Mails mit schädlichen Inhalten zu verschicken. Oft werden auch E-Mail-Server selbst Ziel eines Angriffs, um aus Adressbüchern personenbezogene Daten zu erbeuten, die dann wiederum für den Versand gefälschter, schädlicher E-Mails genutzt werden. Diese Angriffe basieren meist auf Sicherheitslücken in den E-Mail-Servern, die aufgrund des Auslassens aktueller Updates noch nicht geschlossen wurden. Daher gilt es, verfügbare Updates stets unverzüglich einzuspielen.

Um Cyberangriffe zu vermeiden sollten Systeme auf dem neusten Stand gehalten, Makros eingeschränkt oder deaktiviert und die Beschäftigten über schadhafte E-Mails aufgeklärt werden. Wenn ein Cyberangriff erfolgt ist, müssen die beteiligten Systeme neu aufgesetzt werden. Das Anlegen und Wiederherstellen von Backups ist in diesem Zusammenhang unerlässlich.

40 Kommunales und Meldewesen

40.1 Live-Streams von Ratssitzungen

Der Landesbeauftragte wurde im Berichtszeitraum mehrfach mit Sachverhalten konfrontiert, die die datenschutzrechtliche Beurteilung sogenannter Live-Streams von Sitzungen eines Gemeinde-/Stadtrates oder Kreistages betreffen.

§ 52 Abs. 5 des Kommunalverfassungsgesetzes des Landes Sachsen-Anhalt (KVG LSA) eröffnet grundsätzlich diese Möglichkeit. Es bedarf aber zusätzlich noch einer entsprechenden Regelung in der Geschäftsordnung des Rates bzw. Kreistages.

Nach der Begründung zum Gesetzentwurf (Drucksache 6/2247 vom 04.07.2013) strebte der Landesgesetzgeber mit der Regelung eine ausdrückliche Öffnung über die Saalöffentlichkeit hinaus auf die Medienöffentlichkeit an. Der Landesbeauftragte für den Datenschutz hatte im Gesetzgebungsverfahren diesen gesetzgeberischen Willen anerkannt: Die Übertragung der öffentlichen Sitzungen – auch im Internet – sei ein zeitgemäßes Mittel, um Transparenz und bürgerschaftliche Kontrolle zu gewährleisten. Datenschutzrechtliche Bedenken würden unter dieser Prämisse nicht bestehen, solange das Kunsturhebergesetz (KUG) beachtet würde.

Die Regelung gewährt den Kommunen einen erheblichen Gestaltungsspielraum, schuf gleichzeitig aber auch einige Unsicherheiten. Nach früherer Rechtsprechung konnte man Mitglieder der kommunalen Vertretung als relative Personen der Zeitgeschichte ansehen, die sich ihre Darstellung in der Öffentlichkeit nach §§ 22, 23 Abs. 1 Nr. 1 und 3 KUG gefallen lassen müssten. Die Unterscheidung zwischen absoluten und relativen Personen der Zeitgeschichte musste nach einer Entscheidung des Europäischen Gerichtshofs für Menschenrechte (EGMR) aus dem Jahr 2004 allerdings aufgeben werden und wurde vom Bundesgerichtshof (BGH) durch das abgestufte Schutzkonzept ersetzt. Weil die Regelung des § 52 Abs. 5 Satz 3 KVG LSA sich hierzu nicht verhält, zwang sie das Organ der Kommune, diese Abwägung selbst vorzunehmen.

Mit Einführung der Datenschutz-Grundverordnung (DS-GVO) hat sich die Problemlage etwas aufgelöst, wenn auch beide, DS-GVO und §§ 22, 23 KUG, bis heute ein eher schwieriges Verhältnis pflegen. Problematisch ist, ob und inwieweit seit Geltung der DS-GVO noch Raum für die Anwendung der §§ 22, 23 KUG besteht, da die DS-GVO innerhalb ihres Geltungsbereichs Anwendungsvorrang vor nationalem Recht genießt. Im journalistischen Bereich beispielsweise steht nach der Rechtsprechung des BGH die DS-GVO der Anwendung der §§ 22, 23 KUG als nationale Regelung nicht entgegen. Bei diesen Normen handele es sich um nationale Ausgestaltungen der Öffnungsklausel des Art. 85 Abs. 2 DS-GVO. Für Kommunen stellt sich diese Privilegierungsfrage nicht. Hier ist also von einem Anwendungsvorrang der DS-GVO auszugehen.

Da § 52 Abs. 5 Satz 3 KVG LSA eine Regelung in der Geschäftsordnung bedingt, diese wiederum aber nur das Organ binden kann, wird für Dritte (z. B. die interessierte Öffentlichkeit) hinsichtlich des Live-Streams § 52 Abs. 5 KVG LSA nicht als Verarbeitungsgrundlage in Betracht kommen. Insoweit bedarf es also einer Einwilligung, so denn eine Aufnahme dieses Personenkreises überhaupt in Betracht kommen soll.

Der Landesgesetzgeber hat den Kommunen für einen Live -Stream der Ratsoder Kreistagssitzungen einen nicht unerheblichen Gestaltungsspielraum zur Verfügung gestellt. Dieser führt in der Praxis fast schon zwangsläufig zu einem erhöhten Beratungsbedarf, weil die Aufsichtsbehörde die behördlichen Datenschutzbeauftragten mit der Komplexität der Materie weder allein lassen kann noch möchte. Hierbei zeigte sich erfreulicherweise, dass aufgrund des Bestehens verschiedener Erfahrungsaustauschformate zwischen der Aufsichtsbehörde und den behördlichen Datenschutzbeauftragten keine Hemmschwelle besteht, Sachverhalte auch mal nur zur kurzen Bestätigung resp. Korrektur der eigenen Beurteilung an den Landesbeauftragten heranzutragen. Das versetzt die Aufsichtsbehörde in die günstige Möglichkeit, prophylaktisch agieren zu können und nicht erst im Nachhinein, z. B. im Beschwerdefall, eingreifen zu müssen.

40.2 Umfang des Auskunftsanspruches gemäß Artikel 15 Datenschutz-Grundverordnung (DS-GVO)

Kommunen werden regelmäßig mit Auskunftsansprüchen nach Art. 15 DS-GVO konfrontiert. Der Anspruch ist gemäß Art. 12 Abs. 3 Satz 1 DS-GVO im Regelfall (kann verlängert werden) binnen eines Monats nach Antragseingang zu beantworten. Neben Fristfragen stellen sich auch immer wieder Fragen zum Umfang des Anspruches. Insbesondere die Frage, ob und, wenn ja, welche Kopien an die Antragsteller herauszugeben sind, steht immer wieder zur Beantwortung an.

Der Europäische Gerichtshof (EuGH) hat in seiner Entscheidung vom 4. Mai 2023 in der Rechtssache C-487/21 nunmehr etwas Klarheit in diese bisher recht umstrittene Frage gebracht.

Der EuGH ordnet hiernach Art. 15 Abs. 3 Satz 1 DS-GVO als Rechtsfolgenbestimmung der in Abs. 1 statuierten Pflicht zur Auskunft über personenbezogene Daten ein. Im Grundsatz erteilt der EuGH der extensiven Auffassung, Abs. 3 Satz 1 verpflichte den Verantwortlichen generell zur Kopie der die Daten enthaltenen Dokumente, eine Absage.

Allerdings kann sich zum Verständnis der bereitgestellten Informationen die Reproduktion von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u. a. personenbezogene Daten enthalten, die Gegenstand der Verarbeitung sind, als unerlässlich erweisen, wenn die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten.

Was bedeutet das für die Praxis?

Künftig werden Auskunftsbegehren wohl häufig zweistufig ausfallen können. Auf der ersten Stufe kann mit dem EuGH davon ausgegangen werden, dass kein Anspruch auf eine Kopie von Dokumenten oder Dateien besteht, sondern nur auf Beauskunftung von personenbezogenen Daten des Betroffenen.

Wenn der Betroffene daraufhin allerdings geltend macht, dass der Kontext, in dem seine personenbezogenen Daten verarbeitet werden und damit eine Gesamtschau der vorliegenden Akte, Dateien und Dokumente, unerlässlich ist, um die Zulässigkeit der Verarbeitung zu überprüfen oder die Unzulässigkeit nachweisen zu können, wird man dem wohl häufig wenig entgegenzusetzen haben und auf der zweiten Stufe dann doch Daten und/oder Dokumente in Kopie herausgeben müssen.

Für die Kommunen (und auch alle anderen Auskunftspflichtigen) bleiben leider auch nach der Entscheidung des EuGH noch Fragen offen. Es bleibt zu hoffen, dass sich der vom EuGH eher als Ausnahme statuierte Fall nicht zur Regel entwickeln wird. Jedenfalls ist abzusehen, dass sich der Landesbeauftragte auch weiterhin mit entsprechenden Sachverhalten auseinanderzusetzen – sei es beratend oder auch im Rahmen der Beschwerdebearbeitung – haben wird.

42 Wirtschaft

42.7 Aushang von Hausverboten

Den Landesbeauftragten erreichen regelmäßig Beschwerden wegen des öffentlichen Aushangs von Hausverboten. Häufig geht es dabei um Streitigkeiten in Vereinen, bei denen Gespräche oder Verhandlungen zwischen den Beteiligten nicht mehr stattfinden. Manchmal sind bereits Gerichtsverfahren anhängig. Im weiteren Verlauf erteilt der Vorstand einem Vereinsmitglied ein Hausverbot für das Vereinsgelände und hängt dieses in schriftlicher Form in öffentlich zugänglichen Schaukästen aus.

Ein per Computerprogramm gedrucktes Hausverbot mit Angaben zu einer oder mehreren konkreten Personen fällt unter die DS-GVO. Es liegt jedenfalls eine teilweise automatisierte Verarbeitung personenbezogener Daten (Art. 4 Nr. 1 und 2 DS-GVO) vor.

Bei Aushängen in öffentlich zugänglichen Bereichen handelt es sich dann um eine Verarbeitung in Form der Offenlegung, also um eine einfache „Bereitstellung“ gegenüber einer unbestimmten Zahl von Dritten mit der Möglichkeit zur Kenntnisnahme.

Die Verarbeitung personenbezogener Daten nach der DS-GVO ist nur zulässig, wenn eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen erfüllt ist. Mangels Einwilligung scheidet

Art. 6 Abs. 1 lit. a DS-GVO regelmäßig aus. Art. 6 Abs. 1 lit. b DS-GVO ist hier ebenfalls nicht einschlägig. Somit verbliebe Art. 6 Abs. 1 lit. f DS-GVO.

Häufig ist schon das Bestehen eines berechtigten Interesses i. S. v. Art. 6 Abs. 1 lit. f DS-GVO zu verneinen, da Streitfragen um eine eventuelle Räumung noch nicht gerichtlich geklärt sind und somit auch ein Räumungsurteil noch nicht vollstreckt wurde.

Die durch den öffentlichen Aushang des Hausverbots regelmäßig erzeugte Pranger-wirkung führt aber jedenfalls dazu, dass diese Art der Verarbeitung „nicht erforderlich“ i. S. v. Art. 6 Abs. 1 lit. f DS-GVO ist, um etwaige berechtigte Interessen wahrzunehmen. Eine persönliche oder postalische Bekanntgabe dürfte in der Regel ausreichen. Außerdem überwiegen grundsätzlich die Interessen der Betroffenen am Unterbleiben einer Bloßstellung.

Der öffentliche Aushang eines für ein Vereinsgelände erteilten Hausverbots ist nicht zulässig.

42.8 Länderübergreifendes Glückspielaufsichtssystem (LUGAS)

Ein Unternehmen aus dem europäischen Ausland beabsichtigte, virtuelles Automatenspiel in Deutschland online gegenüber Spielern in Deutschland anzubieten. Die hierfür erforderliche glückspielrechtliche Erlaubnis setzte einen Anschluss an das LUGAS-System voraus (§ 4 Abs. 5 Nr. 6 GlüStV 2021).

Das Unternehmen sah eine gemeinsame Verantwortlichkeit i. S. v. Art. 26 DS-GVO zwischen der GGL und sich für den Betrieb und die Nutzung der LUGAS-Dateien.

Der Landesbeauftragte verneinte die gemeinsame Verantwortlichkeit. Das Unternehmen hatte keinen rechtlichen oder tatsächlichen Einfluss auf die Datenverarbeitung im Rahmen des LUGAS-Systems. Es hatte lediglich einige gesetzliche Verpflichtungen in Form der Übermittlung bestimmter personenbezogener Daten an die GGL zu erfüllen. Für die Richtigkeit dieser zu übermittelnden Daten bejahte der Landesbeauftragte eine eigene Verantwortlichkeit (Art. 4 Nr. 7 DS-GVO) des Unternehmens. Im Übrigen bejahte er eine eigene Verantwortlichkeit der GGL.

Werden personenbezogene Daten zur Erfüllung einer gesetzlichen Verpflichtung an eine öffentliche Stelle übermittelt, begründet dies für Datenübermittler und Datenempfänger in aller Regel keine gemeinsame Verantwortlichkeit i. S. v. Art. 26 DS-GVO.

42.9 Verarbeitung der Daten von Berufsbetreuern bei Banken

Beim Landesbeauftragten wurde angefragt, ob Berufsbetreuer mit dem Aufgabenkreis der Vermögenssorge sich bei einer Bank durch Vorlage ihres Betreuerausweises legitimieren können. Laut „Handbuch“ einer Bank sollte es erforderlich sein, zusätzlich zum Betreuerausweis den Beschluss des zuständigen Amtsgerichts (§ 286 FamFG) vorzulegen, mit dem der Betreuer bestellt worden war.

Der Landesbeauftragte teilte hierzu mit, dass die Vorlage des Betreuerausweis genügt. Zwar unterliegen Kreditinstitute gesetzlichen Verpflichtungen zur Identitätsprüfung, beispielsweise nach dem GwG und der ZIdPrüfV. Enthält der Betreuerausweis aber die Angaben nach § 290 FamFG, ist dies als Legitimation in Verbindung mit einem Personalausweis in aller Regel ausreichend. Dabei hat der Landesbeauftragte berücksichtigt, dass Kreditinstitute nur vereinfachte Sorgfaltspflichten erfüllen, soweit sie ein lediglich geringes Risiko der Geldwäsche oder Terrorismusfinanzierung feststellen, was im Betreuungsbereich regelmäßig der Fall sein dürfte.

43 Videoüberwachung und Fotoaufnahmen

43.1 Herausgabe von Aufnahmen von Überwachungskameras an private Dritte

In den letzten Jahren hatten sich im Zuständigkeitsbereich der Aufsichtsbehörde mehrmals Fälle zugetragen, in denen Aufnahmen von Überwachungskameras, die auch die Anwesenheit und das Tun von betroffenen Personen abbildeten, auf Verlangen an Dritte herausgegeben worden waren. Ein besonders dramatisches Ereignis trug sich in einem Supermarkt zu. Dort war einer jungen Kundin durch eine unbekannte Person ihr Mobiltelefon gestohlen worden. Die herbeigeeilte Mutter des Opfers hatte sodann bei der Marktleitung Einsicht in die Aufnahmen der zahlreichen Überwachungskameras begehrt und auch erhalten. Ihr Ziel war, die Diebstahlshandlung zu beobachten und an Aufnahmen des vermeintlichen Täters zu gelangen. Solche Aufnahmen sind dadurch herausgegeben worden, dass die Marktleitung zuließ, dass durch die Familie des Diebstahlsopfers Fotografien von den Bildern auf dem Kontrollmonitor gemacht wurden. Diese Aufnahmen wurden dann zu einer privat motivierten Öffentlichkeitsfahndung in Sozialen Netzen verwendet und weit verbreitet, was auch ungewollte schwere Folgen und einen nachhaltigen Ansehensverlust für die ganze Familie des schnell identifizierten Beschuldigten hatte, welcher auch durch das ca. 6 Monate nach dem Fahndungsaufruf erfolgte Dementi durch das Diebstahlsopfer nicht mehr ungeschehen gemacht werden konnte (zu Fragen der privat motivierten Öffentlichkeitsfahndung in Sozialen Netzen vgl. XIII./XIV. Tätigkeitsbericht (Nr. 14.1.11)).

Die Betroffenenfamilie wandte sich im Rahmen von Beschwerdeverfahren wegen der Herausgabe der Aufnahmen und deren Verwendung zur Öffentlichkeitsfahndung an die Aufsichtsbehörde. Zumindest das wegen der freizügigen Herausgabe von Überwachungsaufnahmen durch das beteiligte Handelsunternehmen durch die Aufsichtsbehörde eingeleitete Verwaltungsverfahren blieb allerdings fruchtlos, da das Handelsunternehmen kurz nach dem fraglichen Vorfall seinen Geschäftsbetrieb aufgegeben hatte.

Gleichwohl sieht die Aufsichtsbehörde Anlass, auf datenschutzrechtliche Fragen einzugehen, die mit der Gewähr der Einsichtnahme in Überwachungsaufnahmen gegenüber Dritten, der Bereitstellung von Kopien dieser Aufnahmen und dem Zulassen von Fotos, die von Aufnahmen eines Kontrollmonitors gemacht werden, im Zusammenhang stehen.

Wie auch die Videoüberwachung selbst stellt die Einblickgewährung und die Herausgabe von Aufnahmen der Überwachungskameras Vorgänge (oder Phasen oder Arten?) der Verarbeitung personenbezogener Daten dar. Auch bei einer Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung handelt es sich bekanntermaßen um eine Verarbeitung im datenschutzrechtlichen Sinne (vgl. Art. 4 Nr. 2 DS-GVO). Folglich bedurften die Einblickgewährung und die Herausgabe von Aufnahmen der Überwachungskameras als Ver-

arbeitung i. S. v. Art. 6 Abs. 1 DS-GVO einer gesetzlichen Erlaubnisnorm oder der Einwilligung der Betroffenen, wobei im vorliegenden Fall eine Einwilligung i. S. v. Art. 6 Abs. 1 lit. a i. V. m. Art. 7 DS-GVO wegen der Abwesenheit des vermuteten Täters nicht in Frage kam.

Die Aufsichtsbehörde hatte durchgreifende Zweifel daran, ob als gesetzliche Erlaubnisnorm für die Offenlegung der gespeicherten Aufnahmen gegenüber der Familie der geschädigten Kundin Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Frage kam. Zwar heißt es dort, dass die Verarbeitung u. a. dann rechtmäßig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Ob diese Erforderlichkeit allerdings tatsächlich gegeben war, blieb höchst zweifelhaft. Die Familie der geschädigten Kundin hätte durchaus die Möglichkeit gehabt, bei einer Anzeige des Diebstahles bei der Polizei gegen Unbekannt auf die in dem Markt vorhandene Videoüberwachung hinzuweisen. Allerdings hätte die Gefahr bestanden, dass bis zum zeitlich nicht einzuschätzenden Tätigwerden der Polizei die Videodaten bereits automatisch gelöscht gewesen wären.

Auch das Bestreben der Marktleiterin als Geschäftsfrau und Händlerin, möglichst zufriedene Kunden zu haben und diesen in einer angenommenen Notlage unterstützend zur Seite zu stehen, mag zwar menschlich nachvollziehbar sein, eine Rechtsgrundlage für die Einblickgewährung in die Videoaufzeichnungen gegenüber der Familie der geschädigten Kundin und die damit einhergehende Übermittlung personenbezogener Daten von Dritten vermochte die Aufsichtsbehörde darin jedoch nicht zu erkennen. Anderes gilt im Übrigen, wenn die Polizei im Rahmen von Ermittlungen, z. B. zu einem Diebstahl i. S. v. § 242 StGB, Einsicht in die Videoaufzeichnungen begehrt, um damit den Sachverhalt zu erforschen. Sie könnte sich dabei auf § 160 Abs. 1 und 2 der StPO berufen.

Die Aufsichtsbehörde empfiehlt Marktbetreibern für ähnlich gelagerte Fälle des Begehrens der Einblickgewährung in ihre Videoaufzeichnungen durch private Dritte nachdrücklich, auf die ausschließliche Zuständigkeit der Polizei zu verweisen.

Die Unterstützung eines Marktbetreibers in solchen Fällen dürfte nur so weit gehen, als dass dieser die zeitlich (z. B. 11:03 Uhr bis 11:06 Uhr) und örtlich (z. B. die Regalreihe, in der die Konservendosen stehen) begrenzten Videosequenzen, die vielleicht den Diebstahl und die beteiligten Personen zeigen, durch geeignete Maßnahmen vor dem automatischen Löschen durch sein Videoüberwachungssystem zu schützen.

Die dem Marktbetreiber als für die Videoüberwachung Verantwortlichem obliegende Pflicht, die Videodaten nach einer bestimmten Speicherdauer datenschutzgerecht zu löschen, wenn deren weitere Speicherung nicht bzw. nicht mehr erforderlich ist, bliebe davon unberührt.

Herausgabe von Aufnahmen von Überwachungskameras nur an die Polizei.

43.2 Speicherfristen bei Videoüberwachung

Bekanntermaßen dürfen personenbezogene Daten nur so lange gespeichert werden, wie es zulässig und für die Zwecke, für die sie verarbeitet werden, auch erforderlich ist. Die Grundsätze der Datenminimierung und der Speicherbegrenzung nach Art. 5 Abs. 1 lit. c und e DS-GVO sind auch bei der Frage, ob und wann Aufnahmen von Überwachungskameras gelöscht werden müssten, relevant. Allerdings wird dies, so zeigt sich in der laufenden Kontroll- und Beratungspraxis der Aufsichtsbehörde, von den Verantwortlichen oftmals nicht beachtet.

Vielmehr werden Aufnahmen von Überwachungskameras eher erst dann gelöscht, wenn das verwendete Speichermedium an seine Kapazitätsgrenzen stößt.

In den Leitlinien 3/2019 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten durch Videogeräte, enthalten im Infopaket Videoüberwachung[66] auf der Homepage der Aufsichtsbehörde, hat sich der Ausschuss eindeutig positioniert. Da einer der am häufigsten vorliegenden legitimen Zwecke der Videoüberwachung der Schutz des Eigentums oder die Sicherung von Beweismitteln ist und in der Regel eingetretene Schäden innerhalb von 72 Stunden erkannt werden können, sollte diese Frist grundsätzlich als maximale Speicherdauer für Aufnahmen von Überwachungskameras ausreichen. Soll diese Frist überschritten werden, müsste bei der Argumentation in Bezug auf die Rechtmäßigkeit des Zwecks der Verarbeitung und der Erforderlichkeit für die längere Speicherung höherer Aufwand betrieben werden. Zu hinterfragen wäre dann neben der Erforderlichkeit auch die Geeignetheit der längerfristigen Speicherung für das Erreichen des beabsichtigten Zweckes.

Die Datenschutzkonferenz hat sich der Empfehlung des Europäischen Datenschutz-ausschusses zur Löschung von nicht mehr erforderlichen Überwachungsaufnahmen innerhalb von 72 Stunden in ihrer „Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen“ angeschlossen.[67]

Soweit das Kamerabetriebssystem oder die Management-Software des Datenrekorders keine Möglichkeit bieten, eine bestimmte Löschfrist einzustellen, um dadurch das automatische zeitgesteuerte Löschen der Kameraaufnahmen zu initiieren, muss der Verantwortliche durch geeignete organisatorische Maßnahmen die manuelle Löschung der Aufnahmen in dieser Frist veranlassen bzw. dies schlicht selbst tun.

Eher nicht oder höchstens sehr ungenau funktionieren wird ein häufig anzutreffendes Verfahren, bei dem die Kamera bzw. der Datenrekorder so konfiguriert sind, dass die ältesten gespeicherten Bilddaten durch die neuesten überschrieben werden (First In – First Out), wenn Platzbedarf besteht, was nach einer angenommenen Zeit von ca. 72 Stunden vielleicht der Fall sein könnte. Dies genügt aber für einen datenschutz-gerechten Betrieb der Videoüberwachung in der Regel nicht. Bliebe bei Kameras, die nur bei erkannter Bewegung im Beobachtungsbereich aufzeichnen, der Bildernach-schub wegen schlechten Wetters, eines erneuten Pandemie-Lockdowns oder aus anderen Gründen aus, verhinderte dies die rechtzeitige Löschung der ältesten Bilddaten. Die maximale Speicherfrist könnte dadurch weit überschritten werden, was eine Videoüberwachung in dieser Betriebsweise datenschutzrechtlich zumindest zweifelhaft erscheinen ließe.

Die Speicherfrist von Videoüberwachungsaufnahmen hat in der Regel nach 72 Stunden zu enden.

43.3 Kameradummys – datenschutzgerechte Nichtüberwachung

Es bedarf sicherlich keiner vertieften Betrachtung, dass mit Attrappen von Überwachungskameras, sog. Kameradummys, keine personenbezogenen Daten verarbeitet werden können. Folglich sind auf sie die DS-GVO und auch das BDSG nicht anzuwenden. Damit entfällt bei Attrappen für die Aufsichtsbehörde, soweit die Eigenschaft als Kameraattrappe glaubhaft gemacht worden ist, das Recht, nach Art. 58 Abs. 1 lit. b DS-GVO Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen, und es entfällt für den Eigentümer eines solchen

kameraähnlichen Gegenstandes z. B. auch die Informationspflicht nach Art. 13 DS-GVO gegenüber den Betroffenen.

Allerdings, und das sind Sinn und Zweck derartiger „Geräte“, erwecken Kameradummys durchaus den Eindruck, dass durch eine echte Überwachung tatsächlich personenbezogene Daten verarbeitet werden. Es entsteht eine Art angenommener Überwachungsdruck, der durch die provozierte Verhaltenssteuerung und -anpassung durchaus zu einer Beeinträchtigung der Persönlichkeitsrechte der Betroffenen führen kann. Hiergegen sind die Betroffenen mitnichten schutzlos: Sie haben, unabhängig von ihrem Beschwerderecht bei einer Aufsichtsbehörde nach Art. 77 DS-GVO, auch die Möglichkeit, sich auf zivilrechtlichem Wege nach §§ 1004, 823 des BGB gegen eine Videoüberwachung bzw. eine Verletzung des allgemeinen Persönlichkeitsrechts zu wehren. Diese Möglichkeit besteht selbst dann, wenn es sich bei einer wahrgenommenen Überwachungskamera lediglich um eine Attrappe oder eine nicht funktionsfähige bzw. nicht aktivierte Kamera handeln sollte oder soweit die Kamera öffentlich zugängliche Flächen oder Nachbargrundstücke nicht wirklich beobachtet. Dies wird von den Nutzern von Kameradummys häufig übersehen.

Für öffentliche Stellen des Landes Sachsen-Anhalt gibt es allerdings eine durchaus wichtige Einschränkung bei der Verwendung von Kameradummys: Sie findet sich in § 8 Abs. 4 DSAG LSA. Nach jener Vorschrift nämlich ist der Einsatz von Kameraattrappen nur unter entsprechender Anwendung von § 8 Abs. 1 und 2 DSAG LSA zulässig. Der Gesetzgeber meint damit, dass nur, wenn auch eine echte Videoüberwachung datenschutzrechtlich erlaubt wäre, durch die öffentliche Stelle auch Kameraattrappen eingesetzt werden dürften.

Auch von Überwachungskamera-Dummys kann eine Beeinträchtigung des allgemeinen Persönlichkeitsrechts ausgehen, was einen Abwehranspruch des Betroffenen zur Folge haben kann.

43.4 Ordnungsamt als „Datenschutzaufsicht“

Der Aufsichtsbehörde ging ein Schreiben eines Ordnungsamtes zu, in dem davon berichtet wurde, dass die dortigen Mitarbeiter mit geübtem Auge auf einem privaten Grundstück eine Überwachungskamera festgestellt hatten. Diese Kamera erwecke aufgrund ihrer Ausrichtung den Eindruck, öffentlich zugängliche Bereiche zu erfassen. Das Ordnungsamt leitete gegen den Grundstückseigentümer prompt ein Bußgeldverfahren ein, weil dieser sich trotz deutlicher Aufforderung durch das Amt weigerte, die Kamera, die nach seinen Angaben nur eine Attrappe sei, zu entfernen. Die Aufsichtsbehörde, von der Gemeinde um Fortsetzung des Verfahrens gebeten, äußerte sich nicht gegenüber dem Grundstückseigentümer, sondern im Rahmen einer Beratung nach § 24 Abs. 4 DSAG LSA gegenüber der Gemeinde, und teilte ihr das Folgende mit:

Im Rahmen der der Aufsichtsbehörde durch die DS-GVO sowie durch nationales Recht zugewiesenen Aufgaben ist nach § 23 Abs. 5 DSAG LSA ausschließlich der Landesbeauftragte zuständige Behörde für die Feststellung und die Verfolgung bzw. Ahndung von Ordnungswidrigkeiten nach dem Datenschutzrecht. Nach Art. 57 Abs. 1 lit. d DS-GVO obliegt es ihm, die Verantwortlichen für die ihnen aus der DS-GVO entstehenden Pflichten zu sensibilisieren und nach Art. 58 Abs. 1 lit. b DS-GVO, Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen.

Adressat aufsichtsbehördlicher Tätigkeiten in Bezug auf die Feststellung und die Verfolgung bzw. Ahndung von Ordnungswidrigkeiten nach dem Datenschutzrecht wäre primär der für die Verarbeitung personenbezogener Daten durch eine vermutete Videoüberwachung datenschutzrechtlich Verantwortliche, der zunächst festgestellt werden müsste. Nicht per se sei dies der Grundstücks- oder Gebäudeeigentümer. Infrage kämen ggf. neben der vom Eigentümer bestellten Verwaltungsgesellschaft auch die Mieter oder Pächter selbst und ferner die sonst an der Liegenschaft Nutzungsberechtigten.

Sodann hätte die Aufsichtsbehörde festzustellen, ob tatsächlich keine funktionsfähige Videoüberwachung vorliegt und andernfalls, in welchem Umfang mittels der Videoüberwachung doch personenbezogene Daten verarbeitet werden. Eine Einschränkung der Betriebszeiten der Kamera, des Erfassungsbereiches oder der Bildqualität oder auch ein teilweises Unkenntlichmachen von Bildbereichen durch Privatzonenmaskierung oder auf anderem Wege, könnte dazu führen, dass die Kamera durch ihre Ausrichtung zwar den äußeren Anschein erweckt, unbeschränkt Daten zu erheben, dass diese Datenerhebung in der Praxis aber durch die technische Ausgestaltung oder die Betriebsart der Kamera beschränkt ist. Nur dieser eingeschränkte Umfang wäre dann für die aufsichtsbehördliche Bewertung relevant.

Auch in Fällen, in denen mit einer Videoüberwachung öffentlich zugängliche Bereiche beobachtet oder mitbeobachtet werden, wäre diese Videoüberwachung nicht immer rechtswidrig, jedoch bedarf die mit einer solchen Überwachung verbundene Verarbeitung der personenbezogenen Daten der Betroffenen einer Rechtsgrundlage. Gemäß Art. 6 Abs. 1 DS-GVO ist eine Datenverarbeitung nur zulässig, wenn die betroffene Person eingewilligt hat oder eine gesetzliche Erlaubnisnorm erfüllt ist. Während eine Einwilligung im Fall einer Videoüberwachung von öffentlich zugänglichen Bereichen eher nicht in Betracht kommt, da allein das Betreten oder Befahren eines videoüberwachten Bereiches keine „eindeutig bestätigende Handlung“ und keine informierte Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO (vgl. Erwägungsgrund 32 DS-GVO) darstellt, könnte für eine Datenverarbeitung mittels Überwachungskamera Art. 6 Abs. 1 Satz 1 lit. f DS-GVO durchaus eine zutreffende Rechtsgrundlage darstellen, soweit diese Videoüberwachung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Das Ergebnis dieser gewissenhaften Interessenabwägung wäre u. U. ein Indiz für die Annahme, ob eine bestimmte Videoüberwachung rechtswidrig sein könnte.

Selbst die gesetzlich geregelten aufsichtsbehördlichen Kompetenzen der Aufsichtsbehörde bei einer Datenschutzüberprüfung nach Art. 58 Abs. 1 lit. b DS-GVO gehen im Fall einer festgestellten rechtswidrigen Videoüberwachung nicht so weit, als dass er als Aufsichtsbehörde letztlich auch den Abbau der Kamera verlangen könnte. Sofern ein Verstoß gegen Datenschutzrecht vorliegen sollte, der zunächst verbindlich festgestellt werden müsste und der nicht bereits durch eine Neuausrichtung der Kamera oder anderweitige Änderungen der Datenverarbeitung beseitigt werden kann, könnte die Aufsichtsbehörde allenfalls eine Beschränkung erwirken bzw. ein Verbot der Nutzung der Videoüberwachungstechnik verhängen. Die Beseitigung der Kamera, also der Hardware selbst, könnte die Aufsichtsbehörde jedoch nach Art. 58 Abs. 2 DS-GVO nicht anweisen.

In Bezug auf die Angabe des Grundstückseigentümers, die Kamera sei nicht funktionsfähig und diene lediglich präventiven Zwecken, hatte die Aufsichtsbehörde ggü. der Kommune außerdem das Folgende mitgeteilt: Mit einer nicht funktionsfähigen Überwachungskamera, also

einer Art Attrappe, oder einer doch funktionsfähigen aber nicht aktivierten Überwachungskamera, oder soweit eine Kamera öffentlich zugängliche Flächen oder Nachbargrundstücke tatsächlich nicht beobachtet, findet keine datenschutzrechtlich relevante Verarbeitung personenbezogener Daten möglicher Betroffener statt. Das habe zur Folge, dass der Anwendungsbereich der DS-GVO in diesem Fall nicht eröffnet sei, dass kein Raum für die Aufsichtsbehörde bestünde, aufsichtsbehördliche Abhilfemaßnahmen zu ergreifen, soweit die Wahrhaftigkeit entsprechender Angaben über den „Nicht-Betrieb“ angenommen werden könne.

Bei dieser Einschätzung unbeachtet bliebe, da eine tatsächliche Verarbeitung personenbezogener Daten nicht vorliege, die Tatsache, dass auch von einer Kameraattrappe ein gefühlter Überwachungsdruck auf die von der vermuteten Videoüberwachung Betroffenen ausgeübt und dadurch in deren Persönlichkeitsrechte eingegriffen werde. Sich dessen zu erwehren bliebe möglichen Betroffenen die Äußerung eines Unterlassungsverlangens nach §§ 1004, 823 BGB ggü. dem „Betreiber“ der Überwachungskamera und, bliebe dies erfolglos, letztendlich auch der Zivilrechtsweg.

Anlass, wegen der vermuteten Videoüberwachung des öffentlich zugänglichen Bereiches ein Verwaltungsverfahren einzuleiten, hatte die Aufsichtsbehörde in jenem Fall zunächst nicht gesehen. Gegenüber dem Ordnungsamt wurde durch die Aufsichtsbehörde lediglich die Überprüfung angeregt, ob nicht das wegen der vermuteten Videoüberwachung des öffentlich zugänglichen Bereiches und der Weigerung des Grundstückseigentümers, die „Kamera“ zurückzubauen, eingeleitete Bußgeldverfahren eingestellt werden sollte.

Ausschließlich die Datenschutz-Aufsichtsbehörde ist zuständige Behörde für die Feststellung und die Verfolgung bzw. Ahndung von Ordnungswidrigkeiten nach dem Datenschutzrecht.

43.5 Klingelkameras

Während der an der Haus- oder Wohnungstür läutende und sicherlich willkommene Geldbriefträger einer eher selten anzutreffenden Spezies angehören dürfte, könnte es in bestimmten Situationen doch wünschenswert sein, bei einem Läuten zunächst zu schauen, wer da Einlass begehrt, um dann die Entscheidung darüber zu treffen, ob die Person eingelassen werden soll. Am Markt wird eine Fülle diesen Wunsch erfüllender Geräte angeboten. Sie werden Klingelkamera, Video-Türsprechanlage, Video-Türklingel oder Video-Doorbell genannt.

Diese Geräte haben gemeinsam, dass ihr Betrieb eine datenschutzrechtliche Komponente hat. Durch die optische und akustische Erfassung des Besuchers und seiner unmittelbaren Umgebung kommt es zur Verarbeitung seiner personenbezogenen Daten, was zur Folge hat, dass sich der Betrieb einer solchen Klingelkamera an den Grundsätzen der DS-GVO auszurichten hat. Nach Art. 5 DS-GVO sind die Datenverarbeitung und die Auswahl und Gestaltung der Technik an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten (Grundsätze der Datenminimierung und der Speicherbegrenzung).

Klingelkameras sind nicht per se unzulässig. Folgende Bedingungen müssten aber erfüllt sein, um ein solches Gerät datenschutzrechtlich zulässig zu betreiben:

- Mildere Mittel, wie die Einlasskontrolle durch Öffnen der Tür oder durch einen handelsüblichen Türspion kommen aufgrund einer besonderen baulichen Situation und/oder weiterer Umstände eher nicht in Betracht.

- Die Klingelkamera wird ausschließlich durch das Betätigen des Klingeltasters in Betrieb gesetzt und schaltet sich kurz danach selbstständig wieder aus. Keinesfalls darf eine Klingelkamera in permanent eingeschaltetem Zustand betrieben werden. Die abstrakte allgemeine Befürchtung von Straftaten reicht nicht zur Rechtfertigung des Eingriffs in Persönlichkeitsrechte. (Urteil des VG Oldenburg vom 12. März 2013, 1 A 3850/12 Rn. 14, juris)

- Es ist nur eine Live-Beobachtung möglich, eine Aufzeichnung der Kamerabilder darf nicht stattfinden, nicht auf einer Speicherkarte, nicht auf einem verbundenen Mobilgerät und auch nicht bei einem Cloud-Anbieter.

- Die Kamera darf zur Identifikation der Besucher nur den Bereich direkt vor der Tür beobachten. Sie darf dazu neben dem Hauseingang nur insoweit Teile des öffentlichen Verkehrsraumes mitbeobachten, als dies unvermeidlich ist.

- Den Personen, die eine solche Türklingel betätigen, werden durch ein geeignetes Hinweisschild die in Art. 13 DS-GVO genannten Informationen mitgeteilt, soweit diese zutreffen. Auf der Internetseite der Aufsichtsbehörde werden Empfehlungen gegeben, wie den Betroffenen mittels Hinweisschildes die erforderlichen Informationen zur Verfügung gestellt werden können.[68]

  Das Hinweisschild müsste folgende Angaben enthalten:

  - den Namen und die Kontaktdaten des für die Kamera Verantwortlichen,

  - die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen,

  - die Rechtsgrundlage für die Verarbeitung,

  - die berechtigten Interessen, die von dem Verantwortlichen verfolgt werden.

  Hinzu kommen einige weitere in Art. 13 DS-GVO genannte Angaben.

Bei Klingelkameras an Mehrfamilienhäusern kommt noch die Bedingung dazu, dass das Bild des Besuchers allein in die Wohnung übertragen werden darf, bei der geläutet wurde. Auch nur zu dieser Wohnung darf eine Sprechverbindung aufgebaut werden. Das Zuschalten von Wohnungen, bei denen nicht geläutet wurde, muss ausgeschlossen sein.

Eine permanent eingeschaltete Klingelkamera, die regelmäßig auch mit einem Mikrofon ausgestattet ist, könnte schnell auch strafrechtlich relevant werden. Ein Straftatbestand wäre verwirklicht, wenn jemand unbefugt das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt (§ 201 Abs. 1 Nr. 1 StGB) oder unbefugt das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen auch nur mit- oder abhört (§ 201 Abs. 2 Nr. 1 StGB). Opfer einer solchen Straftat könnte der Briefträger beim Einlegen einer Sendung in einen Hausbriefkasten in der Nähe der Klingelkamera sein, wenn er sich wäh-

renddessen, in der Annahme, unbeobachtet zu sein, mit einem Dritten unterhält oder telefoniert. Dazu muss er sich nicht einmal im optischen Beobachtungsbereich der Kamera aufhalten, Hörentfernung zur Kamera genügt bereits.

Für die Verfolgung eines solchen mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe sanktionierten Vergehens wäre dann nicht die Datenschutz-Aufsichtsbehörde zuständig, sondern die Staatsanwaltschaft.

Klingelkameras dürfen nicht zur dauerhaften Ausforschung der in den Beobachtungsbereich geratenen Dritten missbraucht werden.